Copyright

All rights reserved by the authors

To view our privacy policy, click the link below:

Privacy Policy
Table of Contents

Copyright ............................................................................................................. 2
Introduction ......................................................................................................... 11
Ground Breaking Ideas ................................................................................... 13
   Edward Ingram reveals some ground breaking ideas in
   Risk Management for Mortgage Finance ................................................... 13
   Business model to change the Economy ....................................................... 23
   The rok-a-meter ......................................................................................... 25
Key Risk trends ............................................................................................... 26
   What do you think are the key risk trends for 2013? ................................. 26
Interviews .......................................................................................................... 27
   Interview with Mr. Khalid Sheikh, international
   consultant and former SVP at ABN AMRO ............................................. 27
   Interview with Mr. Rohan Douglas, the CEO of
   Quantifi about the future of the OTC derivatives market ....................... 36
   Interview with Michael Thomsett - a world's renowned
   author and introduction to a special Options Trading
   Course .......................................................................................................... 41
   Developing and Implementing Strategy for Managing
   Risks in the Supply Chain - Interview with John Brown,
   Director, Risk Management, Supply Chain & Technical
   at Coca-Cola ................................................................................................ 49
   What it Takes to be a Better CFO .............................................................. 53
What is Risk and Risk Management? ......................................................... 55
   The expanded definition of "risk" .............................................................. 55
   Planning for the "unthinkable" risk ............................................................ 57
   Taking another look at resiliency ............................................................... 59
   How do you define risk? .......................................................................... 61
Strategy and Risk Leadership ......................................................................... 64
   Linking Corporate Strategy to Risk Management .................................... 64
   Risk Leadership: Risk Reporting - The Need to Know ......................... 66
Regulatory transparency – the holistic approach? ..................68
What is Strategic Risk Management? ..................................70
Leadership in the Convergence of Governance, Risk and Compliance .................................................................72
Risk Leadership: How to be Heard .....................................74
Risk Leadership: Knowledge is Power ...............................76
Risk Leadership: Facing Extreme Contractual Liability Risk ..................................................................................78
Risk Leadership - Creating Risk Champions ......................80
Risk Leadership? Think Rescorla, Boisjoly & LeMessurier .................................................................82

General; HR, Crisis Management, Travels Risks, Catastrophes ........................................................................84
Pareto’s Law-20% of your assets will be exposed to 80% of threats. Do you know which ones? .........................84
Volcano Lessons: Preparing for future events .....................88
The Law of the Few: World Class Corporate Crisis and Communications Teams ..............................................93
Human Capital Risk Management-What’s Missing? ..........97
Travel Safe: Top 10 iPhone and iPod Touch Travel Apps for Business Travellers ..............................................99
Crisis Leadership is better than Crisis Management ..........103
Japanese Nuclear Crisis: lessons for risk managers ..........108

Compliance & Reputation Risk ...........................................111
Are Your Company at Risk of Damaging its Reputation due to Noncompliance? ...........................................111
Personnel Compliance and Business Valuation - Due Diligence during an acquisition ...................................114
Have you adequately defined Reputation Risk in your Business? .................................................................116
Getting Real About Reputation Risk ....................................119
Can you Risk your reputation? ..............................................123
Whistleblowing- The Psychological Paradox ....................125
Insulating your organization against reputation risk .......130
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloudy issues: Can we reconcile efficiency and security?</td>
<td>133</td>
</tr>
<tr>
<td>Reputation Risk: Beyond Solution Provider Hype and Now a Core Enterprise Risk?</td>
<td>134</td>
</tr>
<tr>
<td><strong>GRC vs ERM</strong></td>
<td>137</td>
</tr>
<tr>
<td>Governance, Risk Management &amp; Compliance</td>
<td>137</td>
</tr>
<tr>
<td>different entities which work as Silos: Misconception</td>
<td>137</td>
</tr>
<tr>
<td>Is your GRC program overly focused on compliance?</td>
<td>141</td>
</tr>
<tr>
<td>5 Reasons to put ERM tools on your GRC shortlist</td>
<td>143</td>
</tr>
<tr>
<td>Risk Managers: Why Spreadsheets are Failing You</td>
<td>145</td>
</tr>
<tr>
<td>Risk Appetite Process and Enterprise Risk Management</td>
<td>147</td>
</tr>
<tr>
<td>Meeting Your Challenge of Setting Risk Appetite</td>
<td>150</td>
</tr>
<tr>
<td>Governance, Risk &amp; Compliance</td>
<td>152</td>
</tr>
<tr>
<td>5 ERM Steps to Prevent a Costa Concordia at Your Organization</td>
<td>155</td>
</tr>
<tr>
<td>How to measure your Enterprise Risk Management effectiveness</td>
<td>158</td>
</tr>
<tr>
<td>Poor Risk Management and Stinky Diapers</td>
<td>160</td>
</tr>
<tr>
<td>Risk Leadership - What is GRC?</td>
<td>162</td>
</tr>
<tr>
<td><strong>Economics, Taxes, Rules &amp; Regulations</strong></td>
<td>164</td>
</tr>
<tr>
<td>Cash flow versus net profits - the dangers of economic ignorance risk</td>
<td>164</td>
</tr>
<tr>
<td>DFA Reform: With 30% of rules in place will regulators be ready to prevent another financial crisis</td>
<td>167</td>
</tr>
<tr>
<td>Five Ways to Create More Jobs</td>
<td>169</td>
</tr>
<tr>
<td>Global Finance and Economy: a Hot Summer Indeed</td>
<td>171</td>
</tr>
<tr>
<td>Ending unemployment and increasing tax revenues</td>
<td>175</td>
</tr>
<tr>
<td>Regulation – overcoming the challenge</td>
<td>177</td>
</tr>
<tr>
<td>Davos 2012 – should everyone bank on innovation?</td>
<td>179</td>
</tr>
<tr>
<td>How to conquer PPACA/OBAMACARE - a battle plan</td>
<td>181</td>
</tr>
<tr>
<td>for brokers, employers and carriers - part 1</td>
<td>181</td>
</tr>
<tr>
<td>Brokers and carriers - profiting from the PPACA/OBAMACARE disruptive changes!</td>
<td>186</td>
</tr>
<tr>
<td>Feedback mechanisms</td>
<td>189</td>
</tr>
</tbody>
</table>
Financial Risks ................................................................. 192
Intermission on the Stage of World Finance ...................... 192
Managing Counterparty Risk key to restoring confidence in finance industry ........................................... 197
Death By Liquidity .......................................................... 200
Are banks ready for Counterparty Credit Risk under Basel III? .................................................................... 202
Visibility and control: the liquidity management mantra ............................................................................. 204
Financial Risk Management - 5 Misleading Criticisms ....... 206

Risk Management best practices, know-how and how to’s ............................................................................. 209
How to set up a successful Risk consultancy? ..................... 209
How to measure performance of Risk department? ............ 210
Brand Building of Risk Management Department .............. 211
Creating a risk-focused organisation ................................ 216
Understanding Risk .......................................................... 219
Preparing Annual Risk Management Strategy .................. 220
It’s all about good governance at the core ......................... 225
How do you audit a risk management program? ................ 227
5 Ways to put Risk Appetite into action ............................. 229
Japanese Nuclear Crisis: lessons for risk managers ............ 232
When risk management is all risk, and no management ....... 235
Best practices for managing & protecting corporate reputation ....................................................................... 236
Developing a risk-conscious point of view in the organization ..................................................................... 239
Risk Managers: What should you report to the Board? ....... 241
What is the risk awareness in your organization? ............... 243
Risk evaluation - getting around the budget issues ............. 245
Breaking Down Assumptions in Risk Workshops ............... 247
5 Steps for Better Risk Assessments .................................. 249
Risk Assessment Template Best Practices ......................... 251
Paint Draw Pick... to Implement Risk Management Across Your Organisation .................................................. 253
Using Risk Assessment Templates to Prioritize Business Measures ................................................................. 254
How to measure your Enterprise Risk Management effectiveness ........................................................................ 257
Building a Risk Taxonomy: Finding What Matters .......................................................... 259
Risk Taxonomy Step 2: Connecting What Matters .................................................................................. 261
Risk Taxonomy Step 3: Managing Cross-Silo Dependencies .............................................................................. 263
Top 5 Project Risk Management Practices ................................................................................................. 266
Presenting Risk Management to the Board ...................................................................................................... 270
How do you Explain Risk Appetite? ................................................................................................................. 273

Information Risk .............................................................................................................................................. 274
Can a computer virus make you ill? ................................................................................................................. 274
Striking the balance in data governance .......................................................................................................... 276
Identity and Access Management (IAM) ........................................................................................................... 278
Cloud Computing – Chief Security Officers (CSO) Concerns ........................................................................... 281
Security Risks of Web 2.0 .................................................................................................................................. 284
Importance of Patch Management in effective IT Risk Management ................................................................. 289
A hidden risk to cloud computing ................................................................................................................. 291
Security issues of cloud computing ............................................................................................................... 294
Entering the Cloud ............................................................................................................................................ 296

Trading And Derivatives ................................................................................................................................ 299
Transparency for High Frequency Trading Regulators, an Introduction. Contributed by Walter Hendriks ........... 299
The amazing power of candlesticks - reduce the timing risk of trading ............................................................ 302
A quick and easy way to master the world of candlestick charting ................................................................... 304
Candlestick reversal signal over 80% reliable -- How's that for risk reduction? ................................................ 305
Best of Global Risk Community Reports

OTC Clearing: part 1 - Are financial institutions prepared for central OTC clearing? ......................................................... 307

OTC Clearing: part 2 - OTC regulatory complexity fosters clearing insecurity ................................................................. 309

Extraterritoriality (try saying that quickly, three times over!) ......................................................................................... 311

OTC Clearing: part 4 - OTC clearing and its impact on collateral management ............................................................... 313

OTC Clearing: part 5 - Trade repository reporting: The regulation of unintended consequences ........................................ 315

OTC Clearing: part 6 - The LEItmotif the OTC bUSIness is preoccUPled with: data integrity and consistency .................... 317

Derivatives regulation - a corporate treasurer’s nightmare .............................................................................................. 319

Operational Risk ......................................................................................................................................................... 322

Getting your data ship-shape to weather the buy-side perfect storm ............................................................................. 322

Fraud, Business Risks, Law ......................................................................................................................................... 324

Deception--Proof Fraud .................................................................................................................................................. 324

Russian Amateur 'Web Detective' Interviewed on Successes in Finding Criminals ............................................................... 326

Regulation E: Using It To Our Best Advantage To Reduce Our Client Based ATM Fraud Risk Without Affecting The Legitimate Client ...................................................................................................................... 330

Trade secret law - an oddity exposing you to danger .................................................................................................. 335

Competition Law in Bulgaria ............................................................................................................................................ 337

Fraud ............................................................................................................................................................................. 341

Political Risk ......................................................................................................................................................... 345

Who won the Egypt referendum .................................................................................................................................... 345

The prospects for the israeli-palestinian dialogue ........................................................................................................ 348

Best questions, Debate & Opinions .................................................................................................................................. 351

Clarity in discussions of risk ............................................................................................................................................. 351

The value of healthy debate to risk managers ............................................................................................................. 352
What skills are most in demand in Risk Management now, either because they are in short supply, or there is excess demand? ................................................................. 354

**Most Engaging discussions .................................................. 355**

How to identify Business Model Risk & Weaknesses? .......... 355

The effect on cultural adoption, of risk management, of production control ................................................................. 356

Risk Management Maturity Model ........................................ 358

What are "Safety statistics & Safety planning control" ........ 359

Difference between Elimination and Substitution in Risk reduction ................................................................. 360

What is the recommended "fundamental" Risk Management training? ................................................................. 361

**Supply chain ................................................................. 362**

Finding those weakest links .................................................. 362

Managing the supply chain via tax policy - a controversial topic ................................................................. 363

Logistics, the monkey wrench in the supply chain machine ................................................................. 366

Rules for diversifying your supply chain .................................. 368

Is your trade disruption insurance good enough? .............. 369

How do you identify a supply chain's weak links? .............. 370

**Insurance ................................................................. 372**

Insurance in perspective – part of a bigger risk management program ................................................................. 372

Financing risk: points for evaluation insurance (or, have you read your company's policy?) ................................................................. 374

Seen on the Tube: How do Insurance Firms Justify Prices? ............................................................................ 376

Survival of the Fittest - For Benefit Brokers and Employer Based Benefits! ................................................................. 379

The death of an industry? - four insurance and benefits industry problems and solutions! ................................................................. 386

**Investment Risk ................................................................. 389**

Risks in accounting rules for less-informed investors .......... 389
The risk of accounting manipulation........................................390
How will the GAAP and IFRS merger affect trend
analysis..................................................................................392
GAAP conversion to IFRS - the biggest risk is in IT ...............393
Hidden opportunities in the investment market: safe
risk reduction strategies..........................................................395
Risks of trusting "special" or pro forma accounting
estimates..................................................................................397
Are you really conservative? – 5 reasons you might not
be ..........................................................................................399

Banking, Credit Risk.................................................................401

What can be done to seal the cracks in the lending
landscape?..............................................................................401
Making the most of commercial lending – how do
banks get there?.................................................................403

Real stories .............................................................................405

Icesave the Real Story. Gerard van Vliet deposited his
savings in an Icesave account and lost it within 6
weeks! It made him a risk expert and an angry 'wasp'
for all authorities......................................................................405
Things To Not Say To A Risk Manager ..................................408
From Marketmaker to Risk searcconsultant .........................409
Introduction

Dear GlobalRisk Community member,

It has been 3 years since the launch of the GlobalRisk Community site in February 2010 and now is a good time to share our best content with you, presented in the form of an Almanac.

After reaching the mark of over 14,000 members, 1000 blog posts and discussions, I’m proud to present the GlobalRisk Community Almanac containing the very best of our content.

Is our current economic crisis just an accident on the road to prosperity and was it impossible to prevent by ordinary people and professionals? Many say yes. I say no!

I believe that this is the right time to get serious about preventing the next crisis and start participating, networking, sharing and contributing to better understanding of the complex world of risk.

Selecting the material for the Almanac was a very daunting task. Unfortunately we were not able to select all articles for that would have made the e-book over 1,000 pages long.

We only selected those articles that have been placed entirely on our platform without linking to other source. Nonetheless we ended up with many hundreds of suitable pages.

The almanac is divided into chapters that present the most important topics affecting our community.

I believe that more specialized reports will follow on each of the important topics.

Special thanks go to members who contributed to this report:

Michael Thomsett, Bryan Whitefield, Edward Ingram, Tim Brew, Tony Ridley, Randy Park, Steven Minsky, Deon Binneman, Gerard van Vliet, Tom Riesack, Thomas Adair, Michele Westergaard, James E. Lawrence, Jennifer Keljik, Nagesh Bharadwaj, Sonia Jaspal, John Farrell, Sourabh Arya, Steven...

I encourage you to share this Almanac with your friends and colleagues and continue contributing to our site so that the next almanac may feature your articles.

Boris Agranovich,
Founder of GlobalRisk Community
Saturday, January 26, 2013
Edward Ingram reveals some ground breaking ideas in Risk Management for Mortgage Finance

Posted by Edward C D Ingram on January 12, 2013

A comprehensive round-up of some of Mr. Ingram’s work (of IngramSure (UK) Ltd) on investigating the instability and risk that is built into the foundations of the world’s economies. Edward thinks that this is where Risk Managers need to assert themselves by getting involved in the design of the products that they are risk managing.

BORIS - Edward you have been telling me and much of the world on your blogs about your researches.

It seems that your approach to risk management is somewhat unique. Can you tell us about that?

Edward – Yes Boris it is very different because I am not employed to manage risk. I am free to say, “This is not something that we should be managing the risk of.”

BORIS – Can you give an example of that?

Edward – Yes the prime example of something that is not correctly structured is mortgage finance. The way it is repaid is just asking for trouble and the way it decides how much should be lent / is costed is asking for trouble.

The fact is that mortgage finance and property price values and the budgets of borrowers are all at risk.

BORIS – Yes you have explained that before and I have to agree that risk managers frequently say that interest rate risk is virtually impossible to manage. You once told me that it has even been said that adding reserves to the lenders’ bank balances will not work “Because the waves are bigger than the ship.”
But before you go into that, can you name anything else that is creating insuperable problems for risk managers?

Edward – Government debt is another one which is important because it is so big. And on the opposite side of that government borrowing are investors who are trying desperately to create a retirement plan which does not put their hard earned investments at risk.

BORIS – What you are saying is that there are no investments out there that are AAA rated to protect the investments that people are putting aside for their retirement. Is that right?

Edward – That is absolutely right.

It is all sourced basically from the one common thread that we have put close to our hearts and around which we have constructed almost everything financial.

“What is that?” I hear you asking.

Let me put it this way – I think I am right when I say that for most people, interest and capital are two different things - right?

If you take away the interest what you are left with is the capital. This is a commonly accepted theorem or definition of interest and capital.

But then everyone also knows that money is constantly changing its value. Where does that fit in? It is not fully recognised by any of the financial structures that are on offer. And it is that inbuilt kind of structure, that insistence that all of the interest must be paid on a mortgage or a government bond, which makes the whole foundation upon which our economies are built, unsafe and unstable.

So the outcome is that we have nothing that is safe either in terms of its investment value or in terms of a safe budget that repays a safely affordable amount of value so that the borrower is not put at risk of default by the lender.

BORIS – What about index-linked investments and mortgages?
Edward – In principle this is a much better idea but there are some objections.

HYBRIDS

One is that the public are not educated into them, so to overcome that one I have created a hybrid mortgage in which it appears to be and starts out as the usual level payments thing, but if the interest rate rises then the borrower has a safety net which in effect turns the mortgage into a rent-to-buy model with the payments rising less quickly than incomes. This ongoing easement in the cost of payments has the effect of preventing what is called Payments Fatigue and it helps to keep all of the borrowers on board because not everyone’s income rises as fast as the average - at least not all the time. Most incomes rise faster at times and slower at other times. It may also be argued that younger people may be on a promotion path, leaving older borrowers income increases lagging behind the average.

So for various reasons the lender has to take care about what index is used for this exercise. Defining the average has its own issues. If in doubt, use the national average index but make sure that the payments fall away fairly fast relative to that index. I think that around 4% p.a. will do the trick. This means that every three years the cost burden in value or average income terms eases by almost 12%. It means that if incomes are standing still payments will be falling every year by 4% p.a. It means that you have to repay more value at first and less later on. I have been asked to illustrate that which I have now done in FIG 0 below.

FIG 0 – 3.55 times income (near mid-range) mortgage repayment table with zero income increases, and falling payments.

Source: Edward C D Ingram Spreadsheets.
### GROUND BREAKING IDEAS

**Best of Global Risk Community Reports**

<table>
<thead>
<tr>
<th>Yr</th>
<th>LOAN</th>
<th>ADD INTEREST</th>
<th>SUBTRACT PAYMENT</th>
<th>BALANCE</th>
<th>Average Income</th>
<th>Average % of income</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100 000</td>
<td>3 000</td>
<td>8 455</td>
<td>95 545</td>
<td>28 185</td>
<td>30.00%</td>
</tr>
<tr>
<td>2</td>
<td>94 545</td>
<td>2 836</td>
<td>8 117</td>
<td>89 264</td>
<td>28 185</td>
<td>28.80%</td>
</tr>
<tr>
<td>3</td>
<td>89 264</td>
<td>2 678</td>
<td>7 793</td>
<td>84 149</td>
<td>28 185</td>
<td>27.65%</td>
</tr>
<tr>
<td>4</td>
<td>84 149</td>
<td>2 524</td>
<td>7 481</td>
<td>79 193</td>
<td>28 185</td>
<td>26.54%</td>
</tr>
<tr>
<td>5</td>
<td>79 193</td>
<td>2 376</td>
<td>7 182</td>
<td>74 389</td>
<td>28 185</td>
<td>25.48%</td>
</tr>
<tr>
<td>6</td>
<td>74 387</td>
<td>2 232</td>
<td>6 894</td>
<td>69 724</td>
<td>28 185</td>
<td>24.46%</td>
</tr>
<tr>
<td>7</td>
<td>69 724</td>
<td>2 092</td>
<td>6 619</td>
<td>65 198</td>
<td>28 185</td>
<td>23.48%</td>
</tr>
<tr>
<td>8</td>
<td>65 198</td>
<td>1 956</td>
<td>6 354</td>
<td>60 800</td>
<td>28 185</td>
<td>22.54%</td>
</tr>
<tr>
<td>9</td>
<td>60 800</td>
<td>1 824</td>
<td>6 100</td>
<td>56 524</td>
<td>28 185</td>
<td>21.64%</td>
</tr>
<tr>
<td>10</td>
<td>56 524</td>
<td>1 696</td>
<td>5 856</td>
<td>52 364</td>
<td>28 185</td>
<td>20.78%</td>
</tr>
<tr>
<td>11</td>
<td>52 364</td>
<td>1 571</td>
<td>5 621</td>
<td>48 314</td>
<td>28 185</td>
<td>19.94%</td>
</tr>
<tr>
<td>12</td>
<td>48 314</td>
<td>1 449</td>
<td>5 397</td>
<td>44 366</td>
<td>28 185</td>
<td>19.15%</td>
</tr>
<tr>
<td>13</td>
<td>44 366</td>
<td>1 331</td>
<td>5 181</td>
<td>40 517</td>
<td>28 185</td>
<td>18.38%</td>
</tr>
<tr>
<td>14</td>
<td>40 517</td>
<td>1 216</td>
<td>4 973</td>
<td>36 759</td>
<td>28 185</td>
<td>17.65%</td>
</tr>
<tr>
<td>15</td>
<td>36 759</td>
<td>1 103</td>
<td>4 775</td>
<td>33 087</td>
<td>28 185</td>
<td>16.94%</td>
</tr>
<tr>
<td>16</td>
<td>33 087</td>
<td>993</td>
<td>4 584</td>
<td>29 496</td>
<td>28 185</td>
<td>16.26%</td>
</tr>
<tr>
<td>17</td>
<td>29 496</td>
<td>885</td>
<td>4 400</td>
<td>25 981</td>
<td>28 185</td>
<td>15.61%</td>
</tr>
<tr>
<td>18</td>
<td>25 981</td>
<td>779</td>
<td>4 224</td>
<td>22 536</td>
<td>28 185</td>
<td>14.99%</td>
</tr>
<tr>
<td>19</td>
<td>22 536</td>
<td>676</td>
<td>4 055</td>
<td>19 157</td>
<td>28 185</td>
<td>14.39%</td>
</tr>
<tr>
<td>20</td>
<td>19 157</td>
<td>575</td>
<td>3 893</td>
<td>15 838</td>
<td>28 185</td>
<td>13.81%</td>
</tr>
<tr>
<td>21</td>
<td>15 838</td>
<td>475</td>
<td>3 737</td>
<td>12 576</td>
<td>28 185</td>
<td>13.26%</td>
</tr>
<tr>
<td>22</td>
<td>12 576</td>
<td>377</td>
<td>3 588</td>
<td>9 366</td>
<td>28 185</td>
<td>12.73%</td>
</tr>
<tr>
<td>23</td>
<td>9 366</td>
<td>281</td>
<td>3 444</td>
<td>6 202</td>
<td>28 185</td>
<td>12.22%</td>
</tr>
<tr>
<td>24</td>
<td>6 202</td>
<td>186</td>
<td>3 307</td>
<td>3 082</td>
<td>28 185</td>
<td>11.73%</td>
</tr>
<tr>
<td>25</td>
<td>3 082</td>
<td>92</td>
<td>3 174</td>
<td>0</td>
<td>28 185</td>
<td>11.26%</td>
</tr>
</tbody>
</table>

**NOTES**

The total amount of income repaid in this table for this 3.55 times income mortgage, if you add up all of the ‘% of income’ data is around 35.2% more than was borrowed at 4.8 years’ income, which is about the normal additional cost-to-income based on average rates for the UK 1970 – 2002.

This model even works when incomes are falling. As long as interest rates are lower or mortgages are smaller, the payments will fall even faster in that case.

In the same conditions, (3% interest and zero income increases), the Level Payments Model would lend the same amount on an income of 19,143 p.a. compared to this ILS mortgage needing 28,185 p.a. That amounts to lending 5.2 years’ income (inflating property prices because all income groups can borrow more).
traditional model will cost 30% of income p.a. every year for 25 years, if incomes are not rising, a total cost of 7.5 years' income. The IMF July 2012 UK Country Report estimates that UK House Prices are normally 3.5 times income on average, based on past data, and currently they are 4.5 times income on average due to lowered interest rates.

BORIS – That kind of thinking rather puts use of the prices index outside the realm of mortgage finance.

Edward – Yes it does. In fact all of the experiments done by lenders using the prices index have fallen into the dustbin of history. The nearest anyone has got to my mortgage model as far as I know, is in Turkey where they have a model that increases the payments at the same rate as the wages index of Civil Servants. The mortgages are then offered to Civil Servants. I understand it is not popular. I am sure that must be because it creates Payments Fatigue. The advantage, which also applies to my mortgage model by the way, is that more can be lent at high interest and inflation rates.

If you ignore some of the more practical issues that can arise, in theory, my model can lend the same amount in any economy, provided that... quite a long list of things are well managed.

BORIS – How does the risk management work? You say it should not only eliminate most of the arrears cases but it also stabilises property values.

Edward – I have developed some equations and a chart for risk management which are named after myself – Ingram’s Risk Management Charts. There is the related Safe Entry Cost Equation, which is really just an equation that breaks down the state of any kind of mortgage or other regular payments debt structure into three elements which added together make up the current level of payments. They are the current capital payment element, the current rate of easement of the payments cost relative to income, called the rate of Payments Depreciation, and the current rate at which value is being added to the mortgage. I will come back to this later.
I am also preparing a follow-on paper for this discussion which I would like readers to see when it is ready.

TRAINING RISK MANAGERS AND PRODUCT DESIGNERS

In fact much of that has already been done in much greater details in LESSONS 3 to 8 at:

http://ingram-school.blogspot.com, but it needs to be done more professionally sometime. I am also creating a new, hopefully better written version of all that to be sold with an interactive spreadsheet so that every kind of test imaginable can be done on the various mortgage models by risk managers and product designers world-wide.

What the equation shows is that if you start with too large a mortgage you then find that you are charging too little in entry cost (the early monthly payments) because the borrowers usually cannot afford to pay more for a larger mortgage. This means that you, the lender, are at huge risk of arrears and default when interest rates rise. Later on, the interest rate and the payments rise because they have to. The mortgage you started with was too big because interest rates were too low to stay low. Interest rates always revert to mean, just like share prices and P/Es tend to do.

STABILISING PROPERTY VALUES AS RISK MANAGERS TAKE OVER

The outcome if all lenders over-lend in this way, is that property values get pushed sky high and when interest rates revert to mean, the collateral security has gone and the arrears jump through the roof. You don’t need any sub-prime idiocy to make that happen.

So the amount that it is safe to lend does not enlarge a lot if interest rates fall, and vice versa, it does not reduce a lot if interest rates rise above the mean value. What counts for affordability is the income multiple originally lent and the longer term averages for interest rates relative to incomes growth rate. This approach to risk management should make property values much more stable and it should preserve the collateral security that is needed.
Edward Ingram reveals some ground breaking ideas in Risk Management for Mortgage Finance

BORIS – You gave an example of what happened in America – the Fed tried to raise what had been 3.5% interest up past the mean to around the 8% mark at which point the inference was that mortgage payments would cost over 50% more.

Edward – That is correct, and that is why property prices came tumbling down. It was not just because of forced sales and sub prime.

BORIS – On that basis are not property prices still over-valued?

Edward – Yes I believe they are. When QE finishes and interest rates have to rise, there will be a repeat of the same dilemma. In fact many people are strongly opposed to QE because it is robbing the elderly of their wealth and it may be robbing lenders of some future lending capacity. Certainly it is distorting the economy, for which there is always a price to pay.

THE PROBLEMS FOR ECONOMIC RECOVERY

BORIS – You said that there is a solution to this dilemma – a way to keep property values high even as interest rates return to normal, which means that QE may be not necessary. Please tell us about it.

Edward – Basically my risk management chart shows that only if you stick to the middle ground of mortgage sizes and entry costs can you manage the interest rate risk and the payments fatigue.

As I said earlier, the **Safe Entry Cost Equation** (the one that gives a breakdown into component parts of any current level of payments including the proposed entry cost), says that any regular mortgage / debt repayment level has three basic elements as follows:

- The current Capital Repayment content C% p.a.
- The current Mortgage Fatigue avoidance element called Payments Depreciation (relative to incomes), D% p.a.
- The current True Cost element which is the part of the interest rate that makes a borrower have to repay more value than the value that was borrowed, I% p.a.
Just add these together and you get the current level of Payments, P% p.a. of the amount borrowed.

\[ P\% = C\% + D\% + I\% \] (all p.a.)

This equation applies to ALL mortgage repayment models. They only differ in how they manage the elements - the Payments Depreciation D%, and the Capital Repayment Content C%. How these components are allowed or forced to behave by the particular mortgage repayments model determines how the total repayments behave at any given time and how safe from arrears they will be.

If you stick close to the middle ground in mortgage sizes (income multiples) you can probably lend around 3.5 years’ income repayable over 25 years in the UK. In the USA they go for 30 years but that is a bit more risky in my opinion, so I stick with 25 years.

The rate of easement – the Payments Depreciation, D% p.a. - can then be around 4% p.a. or a fraction more if the third element in the Safe Entry Cost Equation, I%, is currently low – below what I think is the average, or median, level.

Now in order to support the kind of property values that are around today, many lenders are offering mortgages as much as five times income. QE is being used to keep the interest rate low for this reason – to support the collateral security of lenders and to boost the confidence of borrowers and home owners. It is claimed that this helps with economic recovery, which in the short term is true. But there is no clear plan about what to do when QE ceases and interest rates have to rise.

My equations and spreadsheets show that this support for property values can be done by lending the same amount, around five times income, even as interest rates are rising towards the median rate of interest of say 7% interest if Payments Depreciation, D% p.a., then falls towards 2% p.a. That is stretching things a bit and is not for the longer term. Some borrowers will get stressed but they will not all crash out at the same time and they may move on before their arrears grow much
and their property value may be still safe. And the mortgage money sizes will not actually start rising at these rates. So borrowers may want to opt for this route as interest rates rise.

AN INTERVENTION

But it does mean that if Lenders / Risk Managers are directed to lend this much, then property prices can stay high to protect those assets and balance sheets, whilst incomes do the catching up to reduce that five times income multiple back to the norm of say 3.5 times income, as the economy recovers. This removes one distortion at least - that of low interest rates caused by QE (or any other intervention measures), and both borrowers and bankers will survive the recovery which the current alternative plan using the traditional mortgages, may not do so easily.

BORIS – Thank you Edward. I am sure that your full paper on this will be absolutely fascinating. It appears that you have shown that if the risk management is done correctly then property values will stabilise and that going forward to a new era after economic recovery, mortgages will almost always be affordable for almost everyone with an ongoing income.

GOVERNMENT BONDS TOO

I understand that you wanted to tell us about a similar and very costly misunderstanding involving government debt. You told me that investors in government debt have been reaping very high returns that have cost tax payers huge amounts in terms of value, and that this is largely due to the wealth risk exposure that the fixed interest rate model imposes. Unfortunately we have run out of time, but maybe another time we can go into that.

Edward – Yes Boris it is a great shame because if a value-protecting, index-linked bond structure was used, linking the value of bonds to national average incomes, or to GDP even, then that would revolutionise retirement planning. Then, all kinds of other things that are troubling the governments of the world would come right. From the data I have seen it could also save tax payers a great deal of money. Some of the most costly things that both people and an economy can face is insecure wealth and
uncertain costs. I can show that the outcome of these instabilities is enlarged business cycles in place of relatively shallow ones, and lots of personal financial problems at every level. I believe that the instability of government debt value also considerably complicates and worsens austerity measures when they have to be applied.

BORIS – I understand that you are preparing another paper to illustrate and explain more of all this. Please let us know when and where we can see that. Thank you for being with us today.

Edward – Yes I will and Thank You, it has been my pleasure.

Read this article on the website Click Here
Developed multiple financial arbitrages that allowed me to invest in the financial markets without risk. Produced a business model for the arbitrage, that is ready to be implemented. This model applies to all business sectors.

The model allows the buyer to purchase any product or service and receive a 100% rebate, and possible to have all their financed payment's made for them.

The model allows the buyer to purchase any product or service and receive a 100% rebate, and possible to have all their financed payment's made for them.

Based on the production of approx. 40% return from arbitrage. Based on What I produced over 7yrs.

Need to mark up any total cost of product/service, a minimum of 100%. I take half of (or 20% of the $ amount of arbitrage) produced every year, from arbitrage over 5yrs. That produced over time period (with original arbitrage amount) equals the original cost to the buyer. The additional 20% a year is profit/expenses.

Example:

I am selling a computer that cost me $500, for $1000. The buyer gives me the funds of $1000, and I take $500 for the cost of the product, and $500 I use for arbitrage. Producing $200 a year, I take and set aside $100 a year for 5yrs. I take the original $500, match it up with the $500 produce, and return as a rebate the $1000. The additional $100/yr goes for expenses and profit.

To model this for a financed product/service, a higher markup is needed. Finance can be molded many ways. One could be, just to reduce the cost of purchase, if the buyer pays the interest while the business pays the principle. Another way, is to finance for an extended period, then 100% of the payments can be made by the business, for the buyer. Another would be to increase the mark up to pay for the principle and interest, in whatever financed time period.
This model can be used for all business. Can be used in all situations. There is no economic activity it can't be used for.

Though it may seem that the model I developed is a Socialist dream. It actually is Capitalism at its best.

The model is scalable. Instead of producing the profit up front, it is spread over the time period of the rebate.

Read this article on the website [Click Here](#)
what if you could check your internal organs without going to a clinic, waiting in line, and wasting energy of any sort, I present to you the rok-a-meter.

**Phase 1**

Is a vest which uses new algorithms to get in touch with the internal organs such as liver, kidney, heart, vertebrate, etc.

**Phase 2**

This information is sent to cyber space where it is compared to already existing data posted by the medical units associated with that sector hence a network provider is relevant if the result is negative a red light blinks else a green light blinks e.g. the American cancer society says balbalbal about the lungs this machine checks a user's health rate, what percent is damaged, any important information, compares with the data posted and gives you sense of what is needed in your body or from you. More so, information such as location of the organ at a given time is highlighted, time the organ spent in a position, what is happening to the organ during such a period, etc.

**Phase 3**

Is a keypad which has symbols of all the internal organs like the ones mentioned above when a user wants to have a vivid idea of what is wrong with the kidney for instance the user press “LK” which stands for left kidney. There is a text box on the keypad which displays data both numerical and alphabetically which are called rok-o-graphy, these info may be shared on the net so as potential suitors may be aware of a person’s health statues.

Read this article on the website [Click Here](#)
Key Risk trends

What do you think are the key risk trends for 2013?

Posted by Boris Agranovich on December 20, 2012

Is this Cyber Crime, Fraud management, AML (anti-money laundering) or regulatory compliance and implementing new legislation such as Basel III and the Foreign Account Tax Compliance Act (Fatca) or else?

Please provide your opinion in the comments field below.

Read this article on the website Click Here
Could you please describe your career, especially in risk management?

I started on the credit risk side and more specifically on country risk matters and the frontrunner of Basel II. The essence was to being prepared to a new world, which was more dynamic and as a consequence more uncertain. This was a time of growth and expansion into new territories and in some cases unchartered territories. One principle focus was to liaise with the business to support them where necessary to be successful in closing the right project. This meant that we had to look across the countries borders as globalization and financial intermediation were getting canvassed. Hence, cross border risk and country risk became more important especially understanding what it was about and which risk classified as such.

It is an obvious statement but risk is an opportunity and foremost is not static (even though the triggers of an event are).

This meant a change in thinking from deal based to portfolio-based to strategic. And consequently, changing your infrastructure and policies. I started to work on building a country-risk/sovereign rating system and later on a social ethical risk rating system. The challenge here was to build a tool that reflected the DNA of the corporate and a system that was reliable in its forecast. This was an exiting period because it demanded a change in mindset as well.

The model is just a tool. To get a good understanding of the impact of the different types of risks I developed a scenario model and some stress test to understand the economics behind the risk triggers. This helped me to predict crisis events.
The Russian, Turkey and Argentinean crisis meant stronger concerted action. I was involved in the discussions with the IMF and FED to develop a crisis prevention and resolution framework. In a joint effort led by the International Institute of Finance a framework was developed, which to date is still in place. Strategic alliances were built with the Paris Club.

During the consultation rounds of the Basel II recommendations it became clear that there was no clear view on sovereign risk. More importantly, the consequences of the proposed recommendations would limit business to emerging markets. This during a time where international trade was growing double digit and globalization was at its height. This led us to develop a roadmap for emerging economies on how to deal with Basel II. This was the spark to develop a risk advisory group on enterprise wide risk management.

Corporate Social Responsibility was put on the agenda. This required a new turn in our mindset as we needed to develop a risk framework in which our policies were embedded. This led to the development of a social ethical risk rating, which in my humble opinion is unique!

You have been described by your peers as a strategic thinker. What are the major trends in the International trade and capital flows which will play role in the coming years from your point of view?

1. South-south trade will become more important and within the south-south part intra-regional trade will grow. Hence, traditional political risk elements will arise. Also the problem will arise that more trade will be done, due strategic resources, with conflict countries. This will put more emphasis on the trade related risk component of non-payment. A relate disuse here is that many of the countries do not live up to international standards yet so documentation risk will also rise.

Connected to this is security risk. The obvious is still terrorism but also securing scarce resources will bring in some new features in our risk mind set.
We have witnessed this in the last years with the China’s soft policy towards Africa.

2. Massive currency devaluation risk has been away for some years but with growing pressure on China and India to open up their regimes I would not exclude this risk to arise again. Especially for the satellite countries around these two centers.

   When countries stop protecting their currency it will be devaluated before it will start depreciating again. We saw it in the past with Rub and thai Bath. The more than 10% in a short timespan fall in the exchange rate is harmful for business especially in trade finance.

   We are moving to countries (Africa) which are not fit yet to be integrated and the will become vulnerable because they are exposed.

3. Climate changes

   Physical damage when mines are polluted, thunderstone which blow away nuclear factories.

   The Number of floods in the last 5 years are much higher than statistically possible.

   The issue is to understand what type of risk is it? Whether this is a Political or credit?

4. Institutional risk and sovereign risk is rising again. The critical issue is when will markets accept that US has to be downgraded? When will the market be ready to accept that triple AAA ratings are not risk free! The Southern Europe crisis may be a wake up call, but as long as policymakers are hiding their inability to cope in orderly way with the issue and let markets do their job. They only make matters worse. As a consequence institutional risk will arise where the traditional safety nets like the IMF will not be in a strong position to step in.
Example: couple of years ago we struggled with the principle what is the sub-sovereign. If the State of Florida defaults who will step in?

In Europe. Who is the sovereign? ECB has the emergency fund under their control. The ECB is in essence now is the sovereign.

All the member states send money to ECB. Who is the sovereign Greece or Europe or ECB. Everybody who has claims on Greece comes to the ECB

Some institutions are becoming quasi sovereigns. Will ECB default if members state stop payments? It will change the landscape of risk and understanding how to deal with the risk.

5. Connected to institutional risk is Policy risk: All defined policies without defined SMART objectives will not fly but create more havoc and uncertainty and consequently undermine an orderly resolution. This may sound bold but we all have witnessed this recently. There is no one fits it all solution and also no silver bullet. We have also witnessed that a principles based crisis management package is more effective than a rules-based package. It is important that market participants are involved in drawing policies and support the implementation of these. This will create an environment of timely and adequate response to short-circuit huge losses. I need only to mention the Greece case. Do we really think that the EC package will work out positively? No, look how much value already has evaporated due to poor PR and defined policies.

Markets are too much controlled or curtailed by a lot of policies and new rules, so business become penalized. They are introducing mechanisms, which are not working. New institutions, which are created to control banks, we don’t know how they will work in the next crisis or we know only theoretically.
Interview with Mr. Khalid Sheikh, international consultant and former SVP at ABN AMRO

There will be an implosion in China and India. These countries cannot be new World’s locomotives. The domestic problems both socially and economically are so huge so that they can’t continue with the same growth. The only country, which is doing a good job, is Brasil So we will have protectionism and regional powers will assert power, so we might come back to the 30th of previous millennium.

Coming back to the main source of my concern is S-S trade. We need to address issue of Export credit agencies. They all look to protect theirs own currencies. So if you say that there are strategic countries in World Trade but they don’t have yet the level of guarantees, then you have to extend the insurance coverage from NL to Bangladesh, thereby creating international coordination. By doing this we are securing and mitigating political part.

What are the main principles of Sustainable development and how does it relate to risk management?

Corporate Social Responsibility has to be in the DNA of a company. So it has to be embedded in your risk philosophy and canvassed in your risk charter. All transactions should be screened against a vector of sustainability principles you as a company stand for. These criteria are a direct reflection of the policies you have defined in this respect. Stick to this as it will build a reputation and also transparency with respect to your decision making process. This will be highly valued by the business lines within your organization and also civil society. This is essence will mitigate reputational risk and protect your brand.

Also enhance your governance. So if you have policies you have to monitor them and assess transactions. You have to build number of filters. 1. Compliance to your policies, approval process criteria, KYC policies whether your client will comply to your CSR(corporate social responsible) principles. You have to get a better understanding of the value and business chains.

What are the main challenges banks face with NGO organizations and how risk management approach can solve it?

Best of Global Risk Community Reports
NGO are the voice of the people. By allowing them to look at your kitchen they get the feel how you assess the risk. By making them partner of your Risk framework they will understand more about your decision making process.

We asked couple of journalists to sit down with us on Credit recommendation process. Surprisingly they came with the same assessment as the bank.

So it more or less is creating strategic partners. Include them in the policy. Ask them,. You have to be selective, work only with 5-6 of major NGO organizations, not with the bullies and with the sharks.

Not many companies dare to publish policies that people understand. You don’t have to disclose your criterias, but you can open up transactions. We have to follow some post mortem analysis of some multi national banks. It is important because you will start understand which factors derail projects.

Why the NGO’s are so important? They see effects of your policies. You have to involve them in your impact analysis.

Is branding or Reputation risk very important? I think yes, but it is not included in the Basel framework, they still look as if in the banking sector all boils out to Credit.

You have been an Advisor to the Basle Committee on Sovereign and Country Risk. What will be the impact of Basel III and how will it change the landscape in the financial world in the years to come?

I have worked closely with my colleagues on identifying white spots in the Basel proposals with regard to country and sovereign risk. In this process we have worked with in close consultation with other institutes to define a set of criteria which in our opinion would create a level playing field.

Basel 3 will be a next step to create more awareness both with policymakers and practitioners how important it is to have a robust and sound risk management framework. And how important it is to disclose as much information as possible for
swift, prompt and corrective action in case of need and emergency. It also will help to close the gap between supervisors and financial institutions both with respect to the jargon used as to having a clear understanding of the systems and how the different systems and models relate. It will create a new breed of risk managers and also a new dictionary of financial terms. But at least we will speak one language.

But Basel 3 will not prevent any future crisis unfortunately. It is again a post mortem action. I am concerned that as long as the Basel committee does not define benchmark ratings there always will remain arbitrage opportunities. And as long there is a choice between Standardized and Advanced there will be arbitrage opportunities.

So in essence not much will change over the long haul.

**How the balance of economical power is shifting at the moment and what will be the outcome of this process? Better world or more complicated un-ruled world?**

We see the gravity is shifting to the East. China and India are complimentary to each other. These countries fit with the Ricardian model. They are too big too fail. Economically is much to be gained.

If you want to become the economical power you should become a military power. China is annexing countries in Africa, buying land. They can’t become the military power because they will have to shift resources. The Military powers will remain with USA and Russia. I think Russia will protect Asian countries to protect their economic wealth. Their resources are so important to them, so they will be the Exporters of military power. The US can not keep with their military capacity

Euro has nothing – we are competing with each other. We don’t have much specialization within the EU.

LatAm has resources and skills but they are too small compared with Asia.

This creates un-equilibrium in the world in the coming years.
India and China have their satellites and it creates tension between them.

**Which is the most important opportunity for risk specialists in the coming years?**

2 areas.

1. **Advisory role**. In the upcoming markets – we can advise them on the mistakes we made, create a level field of risk measures and policies. On the control side we need to build strong systems.

2. **Strategically setting of Risk in the organizations**. Risk is the backbone in every org. Risk has to work strongly with business and embed this in the Growth strategic of organizations and to lower risk exposure. We have to distance ourselves from quantitative and to work more on qualification of risk. People have to work on portfolio picture so that we won’t have pockets of specific types of risk.

   Example: I accept risk of 10% of my assets. More Portfolio type of approach is important.

**How can you verify that a specific risk management strategy is working?**

Stress test

Use more frequent stress test and back test – every quarter. You have to be more dynamic and create an opt-out mechanism. If you see that a project deviates from the initial assessment – you have to take actions. It is a new type of thinking, so if deviation start early in the process you can make adjustments.

**What are the main lessons from the current crisis from your point of view?**

1. Policy failures – reluctance to accept that matured countries made a mess of this.

2. Does not matter how much we talk, International coordination does not exist.
3. We do not understand the complexity of the markets. We did not implement the lessons from the past. We could have made distinction what is market driven.

4. Response time is too long

5. We don’t have instruments – is it a lack of good leadership.

US left the bankers in place. They told them if you don’t deliver you go to prison. Here in Europe and NL specifically we put policy makers in Banks. How do you deal in the crisis time?

Just imagine that an aircraft pilot was given a power to navigate a Nuclear submarine in time of crisis.

**How the GlobalRisk Community can contribute to the process and how can we improve?**

1. Organize kind of evening with a speaker. Discuss the items, follow up with the paper

2. Present the ideas to the group. – crystallize ideas, come back again.

3. Submit our proposals to policy makers looking for some agendas.

4. I sent the Questionnaire- road map. (Basel II).

IMF is struggling with financial stability.

If we write, for example, a 1-2 pager on climate change risk and how it can impact portfolio

We can send it to World bank and IMF they have meetings in Europe – to get exposure.

Dutch Gov – is going to discuss the Trade Finance and Export Credit. If we have a view on that, submit to the Minister

[Read this article on the website Click Here](#)
Interview with Mr. Rohan Douglas, the CEO of Quantifi about the future of the OTC derivatives market.

Posted by Boris Agranovich on December 19, 2011

With tons of speculation about the future of the OTC derivatives market and the need for financial reform and increased transparency, market practitioners are a great source for comments on the evolution of the market, how regulation will affect the market and what challenges reform will bring to financial institutions.

Recently we conducted an interview with Mr. Rohan Douglas, the CEO of Quantifi, a provider of valuation and risk management tools to the buy and sell-side.

Could you please briefly describe your career, especially in risk management? What is the role of your company, Quantifi, in the market place?

I started my career working for a primary bond market dealer in Australia in 1983. I joined Salomon Brothers which became part of Citi in 1990 and worked in Fulcrum and arbitrage research before running global credit derivatives and emerging markets trading research.

I founded Quantifi in 2002 with the goal to provide the same kind of advanced analytics, pricing and risk management tools used by the most sophisticated banks to the many new participants entering the OTC markets at that time. Our first products were Quantifi Toolkit (an analytics library) and Quantifi XL (XL add-ins). We introduced our trading and risk management system (Quantifi Risk) in 2005 and our counterparty solution (Quantifi Counterparty Risk) in 2010.

Since 2002, Quantifi has grown to become a leading provider of analytics, trading and risk management software for the global OTC Markets. We have a broad range of integrated pre-trade and post-trade analysis, pricing, structuring and risk management solutions, designed to enable top-tier financial institutions to
Interview with Mr. Rohan Douglas, the CEO of Quantifi about the future of the OTC derivatives market.

better value, trade and risk manage a broad range of derivatives instruments. Our solutions allow clients to rapidly and accurately manage their exposures and respond more effectively to changing market conditions.

Our clients include many of the world’s most sophisticated financial firms including 5 of the 6 largest global banks, 2 of the 3 largest asset managers, leading hedge funds, insurance companies and other financial institutions.

What will be the impact of Basel III on OTC derivatives market and how will it change the landscape in the financial world in the years to come?

Basel III is set to have a profound impact on the OTC derivatives market in almost every aspect of operations and technology. Not only will it force many banks to transform their business models, it will also require them to undertake significant process and system changes. Some of the key impacts:

New minimum capital rations will drive new methods of measuring and allocating capital as banks will be required to hold more capital and higher quality of capital to cover Credit Value Adjustment risk. There is therefore even more incentives for banks to implement CVA desks - however, there are major operational and practical challenges in setting up a CVA desk.

The introduction of central clearing will have immediate and longer term impacts as it will require significant operational and system changes for post-trade operational processes.

Increased regulatory reporting will require significant reworking of legacy risk management systems to accommodate for further data requirements, new calculations to report and increased frequency and turnaround times.

The Financial engineering term has become an almost dirty word now. Which is the most important opportunity for risk specialists in the coming years?

There has been a trend towards simpler products which is likely to continue. At face value this may indicate a trend towards less
financial engineering and simpler risk management but in reality, the current market and regulatory environment has meant that vanilla trades are now the new exotic. Valuing and risk managing even the simplest OTC products has become significantly more challenging and requires funding adjustments like OIS discounting and counterparty risk adjustments like CVA/DVA.

This significant increase in complexity for all aspects of trading and risk management raises the bar for risk specialists but presents a unique opportunity. Banks will increasingly be concerned about return on capital and as complexity widens the gap between the cost of internal builds and a vendor solution, banks will be more motivated to leverage vendor solutions that deliver the level of sophistication required while providing significantly lower capital investment and much greater business flexibility.

How can you verify that a specific risk management strategy is working?

P&L is the ultimate determinate. The key is to have the processes and systems you need in place before any market stress or unexpected event. Providing feedback as part of the process is important. This feedback should be in terms of capital cost, predicted behaviour Vs actual behaviour (with tools like P&L attribution), and historical analysis. Oversight is also important in terms of having the right corporate culture and responsibility in place.

What are the main lessons from the current crisis from your point of view and what are your projections of where we are heading to in terms of a new financial landscape?

The current crisis has spread rapidly from the financial markets to have severe and lasting impact on the real economy. One of the key lessons to be learnt is that market participants need to improve their understanding, application and management of their market and credit/counterparty risk. Having an understanding of history inevitably leads to an appreciation of the value of good management, processes, infrastructure, models and risk analysis. Having this in place takes effort and cost
Interview with Mr. Rohan Douglas, the CEO of Quantifi about the future of the OTC derivatives market.

initially but makes things easier during the good times whilst at times of market turmoil firms are better positioned to take advantage of opportunities. This is an environment where Quantifi provides even more value to our clients by providing tools that deal smoothly with these challenges and allow them to focus on and respond immediately to market opportunities as well as risks. Other main lessons from my perspective centre on macroeconomic policy, financial regulation and the global financial architecture.

Even though regulatory uncertainty and market volatility continue to dominate the markets, there is a growing consensus and direction emerging for a new OTC market landscape. Key drivers of this landscape include counterparty risk, a new valuation framework adjusting for the cost of collateral agreements called OIS discounting and central clearing. Technology is playing an increasingly important role for the OTC markets and this trend is likely to accelerate with the introduction of central clearing. The complexity of the trading, operational, and risk management system required to support OTC businesses have dramatically increased.

**How the GlobalRisk Community can contribute to the process of better understanding of complex world of risk?**

Risk management is an increasingly important discipline. As risks in the financial markets increase, the importance of risk management to all aspects of a financial firms practices increase. Managing market, funding, regulatory, liquidity, operational and other risks involves the business model and risk appetite of a firm and needs to come from the board down. This is a huge change from even a few years ago.

As an online forum for risk professionals, GlobalRisk Community is a great resource for keeping market participants informed about the rapidly changing environment and developing best practices. By connecting practitioners and researchers it helps promote sound risk management standards and practices globally.
Your comments and questions are welcome.

Read this article on the website [Click Here]
I recently interviewed Michael Thomsett who is a world renowned author with over 80 published books. He is a best-selling options author in the United States as of 2010 and he is our top blogger too. We discussed the recent trends, Michael's view on the current crisis and many other things. Michael also prepared a special option trading course for our community members which we hardly recommend to anyone wishing to effectively manage an investment portfolio.

Michael, could you please describe your career, especially how is it related to risk management?

My career began in the accounting field, where I was involved directly with risk in the financial world. At that time I did not think of accounting as risk-related, although much of my work ended up in the field of forensics accounting. The risk of financial loss is tracked through various testing and auditing, of course, and that certainly is a form of risk mitigation and prevention.

In 1978 I left accounting and began writing part-time while also consulting in the financial services industry. For seven years I consulted in systems development for insurance companies, broker-dealers, and real estate concerns. In 1985 I began writing fulltime, specializing in investing and trading topics, business management, and real estate. More recently, my focus has moved to traded, especially in options. I have written six options books published by John Wiley & Sons, FT Press, Traders Library and Amacom Books. I have also ghost written and research two books specifically on supply chain risk management. Over the past two years I have also published numerous articles involved with risk management.
Currently I have a book proposal in my agent’s hands and he has been sharing this with publishers. We have some interest in it and I am hopeful that we will be getting an offer soon. It is on the topic of the risk of a global pandemic to the global supply chain. Along the same lines, I have also had an article published in a double-blind journal this past February and I have several other articles submitted to journals for review; all are concerned with risk management in one form or another.

What are the main lessons from the current crisis from your point of view and how USA can continue its current leading role?

The current crisis goes well beyond the highly visible political infighting. One of the main lessons is that excessive spending by government is a destructive force. Another is that few can agree on how to solve the problem. A Keynesian model tells us that spending by the government moves the economy forward. Frankly, I have seen no evidence that this is true. Jobs are created in the private sector, and when government leaves businesses alone, the economy thrives.

Several steps would help to fix the current crisis. Disturbingly, the current U.S. administration is doing the exact opposite of all of these steps:

1. Lower all corporate and individual tax rates and simplify the tax code. The U.S. corporate rate is the second highest in the industrialized world, and high taxes inhibit business growth and job creation.

2. Balance the budget and enact an amendment requiring the budget to be balanced every year. This is the only way to control the spending habits of politicians.

3. Reduce spending by eliminating several cabinet departments, such as Education, Education, and Health & Human Services. Combine and consolidate Agriculture into Interior and fold Interior into Commerce.

I am not suggesting that the activities these departments perform are not important. But they all belong at the state level. The
federal government should be very, very small and should be involved in very little. Currently, it is out of control.

As an optimist, I believe that the USA will regain its role as an economic leader in the world, but this will require a massive change politically. Here in the USA many people believe that we are hated by much of the world. I don’t believe that. I think Americans are among the most generous of people, interested in helping others when disasters strike and when our friends (and even our enemies) need help. But I do believe that many outside of the USA hate the policies of the government, especially when decisions are made about foreign relations by inexperienced leaders who do not know how international policy works, or who have not articulated a clear policy.

Once the country returns its focus to being a successful trading partner, building strong alliances, and taking a strong and consistent stand with our enemies, I believe the USA will once again be a respected world leader and a good neighbor.

How the balance of economical power is shifting at the moment and what will be the outcome of this process? Better world or more complicated un-ruled world?

The balance of economic power does seem to be shifting, but this is a highly unpredictable matter. Many people believe that China is going to take over the leading economic position within a few years, but I do not. China suffers from profound problems. These include much higher unemployment and under-employment than the official numbers claim; profound poverty in the rural areas of the country; energy problems in the industrial areas; and the worst pollution in the world that will create severe health problems within the next generation.

China also has an odd jobs issue. For unskilled labor, unemployment is quite high. At the same time, skilled and technical jobs are difficult to fill because there are few training programs; so China imports many of the higher-skilled jobs from other countries.
In the long term, I believe that the USA will continue to be one of the leading economic forces in the world economy. However, everything is global and this will increase in the future. I think we will see a regional economy more so than one identified with individual countries. This is already becoming the case in the European economy, which we hear about more and more in place of the economies of the individual countries. Having a single currency for most of Europe has been an important step in consolidating the economic community regionally. This is a positive trend and I see it continuing into the new century.

Do you think stakeholders will ever value efficient risk management over potential returns on investment?

They must do so. Globalization means improved efficiency, but risk managers need to balance efficiency with security. The great threat in the future is going to be technological security. As IT moves rapidly into the mode of cloud computing, efficiency will be vastly improved and this is where great emphasis is being placed. However, in the past, the equation was simple and had two components. Greater speed and storage = Greater efficiency and Greater speed and storage = Greater risk. In the future, I think this relationship has to be changed.

The great challenge to efficient risk management is going to be creation of clouds and other venues in which efficiency and security can be competitively improved as aspects of a comprehensive method for computing. Stakeholders may not always be aware of the relationship between speed and security. Investors and top management want return on investment and as a result, pressure is put on risk managers to improve efficiency. The great lesson of the near future is that stakeholders need to be shown how better efficiency may also bring with it greater threats. In this environment, a realized threat will destroy return on investment, and ironically, the greater the efficiency, the bigger the cost will be of a realized risk.

Where do you think the next big risk crisis will occur and where should we look to strengthen core competencies over the next 12 months?
The coming year is most likely to experience a big risk crisis in the financial world. This will not be limited to trading on the markets or even to countries defaulting on their debt, although that is a big part of an emerging new world. The crisis may also extend to the safety of liquid assets, especially those vulnerable to cyber attacks.

Organizations need to enter into a defensive phase, more now than ever before. This means not maintaining liquid assets in any one economy, but diversifying among several different regions. They may also want to avoid placing too many assets with any one banking organization, given the recent history in the USA of big banks and investment houses failing unexpectedly. Finally, organizations may want to diversify by creating predetermined levels of liquidity and converting a portion of that liquidity into gold and silver holdings -- not stocks in mining companies, but direct ownership of bullion. If any major currencies “blow up” or countries default on their obligations, the economies of those countries could rapidly fail. In that case, no organization will want to have liquid holdings or any substance stuck in the monetary unit involved.

Is the efficient management of risk viewed as a competitive advantage or an unavoidable business cost by the modern business?

Currently many organizations see this as a business cost and an irritant to doing things the way they have been done for years. But those who believe this will find themselves in the same class of people investing in blacksmithing shops at the same time the automobile began to be mass produced. All methodologies may become obsolete, and this includes old-style risk management (or operating without much awareness of risk).

Today and in the near future, risk managers have to decide whether efficiency is a good enough goal by itself, or whether the necessary security has to be constructed as a crucial attribute of the more efficient system. Risk management is always going to cost money and impact the budget. The risk of failing to recognize it as a competitive advantage is the second most
dangerous threat to the organization. The most dangerous, of course, is the failure to understand the nature of risk.

How would you communicate and position risk management as a competitive advantage?

Risk management can be used to create a competitive advantage. It can be turned from a cost element into a profit center, by incorporating the risk program into the quality control and customer responsiveness that all organizations strive to improve. In this new environment, you seek to improve efficiency while also making security an efficient element of the system itself … and not an outside impediment.

What are the main challenges for the CRO in the integration of risk culture into their business?

Anyone working directly with risk management, including the Chief Risk Officer, has a great challenge. This is to educate the organization so that its culture can change. The old-style view that “it’s not my job” is very destructive in trying to build a risk-conscious culture. Toyota accomplished this with revolutionary assembly line changes and other developments in a system called jidoka and using Six Sigma in General Electric had the same kind of cultural changes.

CROs may look to programs like Six Sigma to help change the corporate culture. Simply making everyone aware of the nature of risk and internal vulnerabilities is a profound challenge. Among the most difficult insiders to change are the top executives, who are keenly focused on the bottom line and the stock price. Everything a CRO brings forward to the budget meeting will be met with two questions: “What will this cost?” and “Is it really necessary?” The challenge is to demonstrate how remaining exposed to a range of risks is likely to cost much more than doing nothing; and yes, it is necessary.

Which is the most important opportunity for risk specialists in the coming years?

As the new development of cloud computing moves at rapid pace, it presents a serious security risk. This, risk specialists need
to be aware of the need to match efficiency with security. Cloud computing is a great idea, but it also poses great threats.

I think this is the most important development because it contains amazing opportunities as well as serious threats. It will enable all companies, even the smallest and most local to become truly global in scope, communications and customer base. The cloud is a miracle that opens up possibilities we haven’t even imagined yet. But like all great opportunities, it also has to be built and controlled with great care.

**How the GlobalRisk Community can contribute to the process and how can we improve?**

The most valuable aspect to this site is that it brings together thousands of people from all around the world, sharing similar interests and concerns. We do not need to go to a seminar and pay thousands of dollars to listen to a series of speakers. We do not need to take time away from productive time to learn. Having this website available makes all risk management global on its own terms.

The importance of building membership and continuing to speak with one another cannot be emphasized too much. As a writer and businessman coming from an accounting background and with a keen interest in risk management, I have already experienced an eye-opening growth in my understanding of the “world of risk” just by being a member of the site.

I encourage all members to invite their associates to also join the site, and to become contributors to the process by communicating with one another, writing blogs, taking courses, downloading special reports, and reading what others have written. The best risk management education is going to come from working with others in the same field.

**You are announcing a new course for our members, an introductory course on options. Tell us more about it.**

Yes, the options course is aimed at risk managers who are not at all familiar with the world of options trading. Emphasis is on the basics and the course is broken down into several segments to
methodically introduce definitions and concepts. Anyone taking the course should expect to learn the essential elements of the market and how options can be used to manage and reduce risks.

Is the material suitable for those without any experience in the market?

Yes. The course is not designed to convert an individual into an experienced trader. It is intended as an exposure to the range of rules, definitions, and risk management possibilities available using options.

You can find more and book the Option Trading Course via the following link: The Options trading Course with Michael Thomsett.
The past three years have seen a number of man-made and natural disasters bring risk management demands to the forefront of executives and board directors. Fat-tail risks that have a low probability, but a very high impact to the organization, such as the Japanese tsunami, the Gulf of Mexico oil spill or the euro-zone liquidity crisis, have been front and center, creating a renewed interest in enterprise risk management (ERM) practices.

John Brown, Director, Risk Management, Supply Chain & Technical at Coca-Cola answered a series of questions written by marcus evans before the forthcoming 6th Annual Enterprise Risk Management Conference, March 19-20, 2013 in Chicago, IL. All responses represent the view of Mr. Brown and not necessarily those of Coca-Cola.

When it comes to quantifying risks within the supply chain, are there sure-fire approaches or methods to apply? Why or why not.

John Brown: The sure fire approach is to map your supply (value) chains, delineating the flow of value contribution from each node (value-adding operation) and through each link. As is normally the case, however, the sure-fire approach is not easy to implement, especially since the “map” must extent to tier 2, 3 and beyond suppliers, and downstream through customers to end consumers. The effort and resources it takes to complete this mapping is insurmountable for most companies. Some excellent work is taking place to visualize value chains by mining data in enterprise applications, such as SAP. But there are challenges...
even in this approach, which at best captures tier 1 suppliers. I am hopeful that elegant (and affordable) solutions will be developed in the next few years. What are some of the vital steps an organization must take to mitigate risks in the supply chain associated with fat-tail risks like Hurricane Sandy?

**JB:** Interesting question, and no easy answer. Risk management is essentially prevention, and few company reward structures are geared to prevention activities (as compared to reaction, such as crisis management). Part of the difficulty is that it is next to impossible to demonstrate that risk management activities prevented an uncertain event from occurring. The steps most companies can take today include understanding where they have critical dependencies, such as single-sourced materials or services, suppliers who are susceptible to external events, or vulnerable transportation/logistics links. And then establish arrangements to avoid a major disruption in the value creation chain. The challenge with this approach is that it ultimately increases your cost-of-goods, relative to a steady-state environment. Where it pays off is if you experience a disruption and are able to flex with it. A more fundamental approach is to design products and services with a view of minimizing exposure to disruptions.

**When it comes to risk buckets, how is The Coca Cola Company currently managing risks within the supply chain?**

**JB:** You would think that the beverage industry is relatively simple. Yet it is an amazingly complex system, especially for a globally diverse company. Our approach has been to develop a common methodology and tools to identify, analyze and mitigate risks at every locally relevant business entity. We then use technology to create an aggregated view of risks at successively higher organizational levels. This approach ensures that risks are identified and managed at the local level, which in itself is true risk management across the enterprise. The sweet spot is where we can identify systemic risks across multiple entities and then apply higher level resources to solve these risks once, instead of multiple times, and with sometimes different approaches. Likewise, some risks that are seen at higher organization levels
Developing and Implementing Strategy for Managing Risks in the Supply Chain -
Interview with John Brown, Director, Risk Management, Supply Chain & Technical at Coca-Cola

(which tend to be more strategic in nature) can be communicated to local entities as a watch-out. The strategies and processes we developed in the supply chain and technical areas have been adopted by the ERM team, so we have a single, unified approach to risk management across the company.

**What are some of the types of risks that are overlooked when it comes to the supply chain?**

**JB:** Supply chain organizations tend to be focused on sourcing, making, moving and selling--and as such sometimes have a blind spot relative to external events that can significantly impact value chains. Some of these risks exist in the political and social arenas, human resources, public perceptions, large-scale economic changes, and sometimes in the critical linkages in global value chains. The Fukushima earthquake (and the ensuing tsunami and nuclear power impacts), the Thailand floods, the Eyjafjalla volcanic eruption, and the Middle East unrest all exposed weaknesses that crept into value chains as we continued to find ways to increase productivity and reduce costs. It will always be a challenge to employ risk prevention in the face of constant pressures to reduce costs.

**As a speaker for the 6th Annual Enterprise Risk Management Conference, what do you look forward to most about attending this event?**

**JB:** Learning about the strategies, tools and techniques companies are using to implement risk management programs, with a focus on effectiveness and efficiency. Risk management is an evolving discipline, with many approaches and espoused best practices. Over the last few years I’ve seen a gradual move towards a common set of guiding principles, with a focus on identifying and preventing risk events. This is a critical step in my view, and ISO 31000 has provided a foundation. Too many risk management programs focus on compliance or reaction. So, the move towards a focus on prevention is welcomed.
John J. Brown, a registered professional engineer, Associate in Risk Management-ERM (ARM-E) and Certified Protection Professional (CPP), has worked directly in the risk management field for well over a decade, and indirectly most of his career. Since joining The Coca-Cola Company in April 2008, John has developed a risk management strategy and processes for the Company's global value chain, and is currently implementing that strategy.

For more information please contact Michele Westergaard, Senior Marketing Manager, Media & PR, marcus evans at 312-540-3000 ext. 6625 orMichelew@marcusevansch.com.

Read this article on the website Click Here
What it Takes to be a Better CFO

Interview with: Melanie Mailly-Demont, Chief Financial Officer, Infilco Degremont

Las Vegas, NV, September 18, 2012 - FOR IMMEDIATE RELEASE

Chief Financial Officers (CFOs) should not be afraid to ask questions to the experts in the field, advises Melanie Mailly-Demont, Chief Financial Officer, Infilco Degremont. “It is part of the CFO’s role to bring a fresh perspective. They need to be much more than what their CFO role entails,” she adds.

A speaker at the marcus evans CFO Summit XXV Fall 2012, in Las Vegas, Nevada, November 8-10, Mailly-Demont gives us her take on how CFOs can add true value to their organization.

What skills does a CFO need to bring to an organization today?

CFOs today are less technical than they used to be. They still need to know the techniques and accounting rules, but their behaviors and ethical values play a more important role. They have to be leaders and solution providers, which means they must have a good understanding of the business. Being good accountants and financial analysts is simply not enough anymore. They should proactively find solutions to different issues.

How could they better control costs?

The first thing that is required for this is a good understanding of the business, otherwise they will fail. This sounds easy, but it is not. Finance executives have to mix with people from other functions, to understand what their challenges and targets are. To be a good CFO requires one to be much more than a CFO.

What risk mitigation tips could you give?
It is not the CFO’s job to be nice, so CFOs should not be afraid of opening their mouth when they see a risk. That is the best way to mitigate risk. That means that sometimes they need to ask questions to the experts in the business at the risk of sounding stupid or naïve, but they have enough experience to offer solutions to even the experts, who might take certain things for granted. They have to approach issues fairly, but at the same time share their concerns.

**How could CFOs improve shareholder value?**

The first step for increasing shareholder value comes from measuring it. They cannot improve it if they cannot measure it. That is how CFOs can contribute. By being a naïve person in the organization, who wants to understand the basic processes that the experts no longer question. It is the CFO’s fresh perspective that will add value to the organization.

**Any final thoughts?**

CFOs have a growing role to play. Today’s measurements are mostly financial, but they also have to mean something. One cannot just value a company by the value of its share. It is also the CFO’s role to ensure that the value of the company is translated properly on the market, that people who make decisions have the right indicators to guide those decisions.

Many CFOs are just trying to be good at accounting or analyzing financial data, when they can bring much more value than that.

**Contact:** Jennifer Keljik, marketing manager, marcus evans, Summits Division

Tel: 312.540.3000 x6592

Email: summits-na@marcusevans.com

Read this article on the website [Click Here](#)
For some, risk management describes insurance only; for others, it is a process designed to mitigate known risks through various means; and for others still, it is a broader and more encompassing process moving beyond insurance and beyond known risk categories.

Everyone is attempting to deal with the same problem: reducing the cost of events through one or more means to prevent every kind of loss from small, well-known and insurable risks up to catastrophic and unexpected ones.

In addition to insurance as a means for managing risk, other methods may be incorporated into the risk management process. These methods not only address unknown or uninsured risks, but actually reduce the potential for losses, even those already insured. A risk can be transferred or shared with suppliers, manufacturers and subsidiaries. Another form of transfer is the risk pool, in which a broader base is organized to reduce the cost of insurance.

Most insurance-based risk management programs practice risk prevention as a means for reducing premiums or improving experience ratings.

The problem persists, however. Insurance can address only known risks - known both in terms of the kind of loss and its cost. But insurance does not cover unknown or unexpected risks. For these, insurance is not the sole answer, while other solutions will at least mitigate exposure. This is especially applicable for supply chain issues and most relevant for any organization involved with a global supply chain. Two methods are valuable in reducing unknown or even unimagined risks.
First is a counter-intuitive process going on today in some circles: de-globalization. By shrinking the geographic extensions of the supply chain, exposure to many types of risks are reduced as well. This is not isolationist; in fact, replacing a singular global supply chain with a series of segmented and more locally controlled ones reduces risk for all stakeholders, including manufacturers and suppliers. De-globalization may also provide greater power, control and influence to manufacturers currently limited to the supplier role. By providing remote manufacturers control over a smaller, local supply chain, these stakeholders increase their motivation to reduce and mitigate exposure to risk. For the demand side, practices like shared warehousing and just in time inventory increase risk because a single loss has greater impact. This problem is well managed with moving supply sources closer to home.

The second is diversification. Many relatively simple risks (such as unavailability of a cheap but essential part) become catastrophic if only one supplier is involved. A syringe made in one place and essential to a specific treatment may be unavailable for an extended period due to natural disaster, piracy, or strike, for example. The solution is to divide the supply chain among two or more suppliers. This not only reduces risk exposure; it also enables the demand-side of the equation to better control costs. Competition among two or more suppliers is healthy as well as a smart form of risk management.

Read this article on the website Click Here
Planning for the "unthinkable" risk

Posted by Michael C. Thomsett on May 20, 2011

This, of course, is the ever-present challenge for all risk managers. If a risk is unthinkable, how do you plan for it, mitigate it, or prevent it?

For example, a global pandemic not only causes widespread death but shuts down the supply chain and bypasses all risk management efforts and programs. To make matters worse than the mortality issues, the risks of civil unrest and shortages of food, water, and energy could lead to many more deaths than the pandemic itself. The whole problem and its scope of challenges is simply unthinkable.

Solutions are available. It's a matter of diversification and control. Anyone trying to manage risk in a global supply chain knows that a singular chain is by definition full of risk. Any number of events could and would disrupt and shut down that supply chain. Solutions include the three D's:

1. De-globalization: One of the greatest problems for SCRM is the geographical extent of the supply chain itself. By shrinking that chain and moving supplies and manufacturers closer to home, many of the inherent global risks shrink along with the size of the supply chain.

2. Diversification: Why rely on a single manufacturer or supplier? This itself is an unacceptable risk. By employing two, three or four suppliers in different regions, you avoid many of the global risks and secondary exposure, including pandemic (where borders are closed, possibly for an extended period, for example).

3. Dissemination: Open up the discussion among your own suppliers. When organizations do this, they get more intelligence that they can get elsewhere. For example, most participants in the supply chain are likely to assume that "someone else" has already planned for risk and taken the necessary steps. Secondly, you will discover more great ideas from participants in the supply chain. Finally, you will
discover aspects of the unthinkable risk that -- once opened up for dialogue -- become thinkable, and that is how solutions are developed.

This is not to suggest that solutions are easy or simple; they are not. But analyzing the problem with disciplines of business management and investment common sense are at least starting points to reduce the impact of what today is an unthinkable loss.

*Thomsett is an author and speaker specializing in business and investing topics. His paper, "Global Supply Chain Risk Management: Viewing the Past to Manage Today's Risks from an Historical Perspective" was presented in December, 2010 at the IntellectBase International Consortium. The paper was then selected for publication in the journal "Review of Management Innovation and Creativity" (February 2011 issue, Vol. 4, Issue 9)*

Read this article on the website [Click Here](#)
Aiming to create resiliency is at the heart of a risk management program, not only because it is a good attribute, but also because it defines what the program requires.

The definition for many is simply related to the financial ability to absorb loss. But resiliency means much more. It should be defined as the organization’s ability to experience loss without also losing markets or competitive position. It so often happens that organizations are not able to recover sufficiently or quickly enough and, consequently, they lose their competitive capability. In the worst case, they may even go out of business, a notable possibility for small businesses. The potential for complete loss of business is especially serious among minority- and women-owned businesses. A recent study concluded that nearly 40% of such businesses have never assessed risks that threaten disruption of service; and that only about 20% of such businesses have adequate disaster plans. ("Business Continuity Strategies: An Assessment of Planning, Preparedness, Response and Recovery Activities for Emergency Disasters," Retta Guy and Millicent Lownes-Jackson, presented December, 2010, Intellectbase Intellectual Consortium).

The vulnerability of small business is due only in part to lack of risk mitigation programs. These concerns also suffer from lack of capital and limited market area. Many cannot afford business continuity insurance or even development of a comprehensive risk program. Ironically, these limitations may ultimately protect a small business in the sense that it is not exposed to the global threats that more extensive supply chains face, from events such as piracy, terrorism, maritime losses, foreign government intervention or restrictions, labor strikes, and much more.

All small businesses may reduce risk exposure through sensible mitigation programs. But a full disaster recovery or business continuity plan must assume available resources, and this
precludes many of those newly formed businesses barely covering expenses each month.

Resiliency for the small business has to be defined in much different context than those for multinational organizations, if only due to the far smaller capitalization size alone. For small businesses, resiliency often means basic survival in business and living with chronic vulnerability even to relatively small risks. When compared to better established and capitalized organizations that can absorb losses, many small businesses are literally one monthly cycle away from going broke. A single unexpected loss could shatter the entire structure of the business. Any business that is able to survive this is, by definition, resilient.

Read this article on the website Click Here
How do you define risk?

Posted by Michael C. Thomsett on July 29, 2011

The definition of risk is obvious, right? Not necessarily. Those who work with risk all of the time may not have paused recently to consider this question. The fact is, risk means different things to different people, depending on their industry, position, experience and knowledge.

During the 1950s and 1960s a revolutionary change began taking place. Rapid advances in technology were taking place, and at the same time businesses began operating internationally. This naturally led to greater focus on risk and risk management. However, it was only in recent years that risk managers have acknowledged two important attributes to risk. First is the form of risk based on possible future outcomes, and second is the probability of a risk materializing.

This is an important distinction. In the budget meeting, non-risk managers are constantly asking the second question: "What are the odds of this really happening?" The point raised with this question is that if the probability is low, why finance a risk management effort? Perhaps the more relevant question is the first one: "What form does this risk take as a possible future outcome?"

The choice to take action and fund that action to mitigate, transfer or eliminate specific risks contains an unknown number of variables, which explains at least partially why it often is difficult to get budget approval for risk initiatives. If you cannot articulate the cost of risk materializing, and if you cannot say it is likely to occur at all, how does management know whether funding your program is a worthwhile effort?

Of course, management at this point may decide to take no action. This is also a choice, of course, and the startling realization is that the choice to do nothing might contain the same risk variables as choosing a different course. Risk is a factor in analyzing how to make decisions and it is unavoidable. Thus, managers generally want to decide on the most profitable, but
WHAT IS RISK AND RISK MANAGEMENT?

safest course. The reality is that to maximize profits, greater risks must be taken; and to maximize safety, the organization has to settle for smaller profits.

If you accept the definition of risk as expectation of loss, with the likelihood of occurrence at a high level, so then is the potential cost of the risk. But still, risk cannot be measured in probabilities nor in financial terms, in any manner other than an educated guess.

Risk and uncertainty are not the same thing, however. This is where the definition often crosses over and gets confused. Risk exists on a band ranging from low to high levels of certainty or uncertainty, and this is where the definition can be focused and management given a likely financial impact if the choice is made to simply ignore the risk. A high-probability, high-cost threat requires attention, whereas a low-probability, low-cost threat can more rationally be ignored.

One book (1) concluded that by definition, risk must include some degree of uncertainty. However, under this argument, if the probability of outcomes can be defined specifically, then there is no actual risk involved.

An example of this "absence of risk" is found in life insurance and the provision of policies to insured individuals. Death is going to occur for all insured policyholders and its timing can be calculated quite precisely based on actuarial probability. Thus, a group of people of a specific age are going to experience mortality on a predetermined schedule. With a known probability, the exposure can be quantified actuarially. Among people of age 'x', there will by 'y' deaths in year 'z', until all have died. There is no risk of death occurring because all policyholders will die; the timing is not known for any one person, but for the group as a whole, the timing is well known and the calculation of the number of deaths each year for any given age group is quite precise. According to the definition of risk based on the question of whether or not the event is going to occur at all, life insurance contains no risk based on the overall population of policyholders.
This question of how to define risk raises interesting questions, and challenges our assumptions about the nature of risk as a factor in decisions, whether in business, investing or personal lives.


Read this article on the website Click Here
Communicating corporate objectives and the strategic plan is a key consideration in the governance of an organization. Promoting effective communication throughout the organization is essential as it establishes a “Tone from the Top” that is consistent with good governance.

Communicating corporate objectives is easily facilitated through enterprise risk management processes. Most companies have a succinct statement of corporate strategy that includes a statement of objectives. Objectives emanate from or are included within a statement of mission (the company purpose) and/or a statement of vision (where the organization wants to be within one to five years). When risk management embraces corporate objectives, the objectives themselves become a starting point for the determination of risk. No matter what level of the company where risks are contemplated, once objectives are defined it is a natural follow-on to think in terms of what are the risks to meeting each objective in terms of an employee’s role and level within the company.

When risks are aligned with corporate objectives, organizations ensure that each risk (along with its treatment costs and related process costs) is in line with corporate revenue and profit expectations. It also ensures that no risk or related treatment activity is in opposition to corporate strategy and therefore that no risk is in opposition to revenue and profit expectations.

The benefits of linking corporate strategy to risk management include:

1. The costs of risk treatments (whether mitigated, transferred, accepted or avoided) are always in alignment with revenue and profit expectations.
2. The cost of risks and risk exposure is measured and compared in a way that supports the strategic plan.

3. The communication of corporate strategy is inherent in the risk management process and serves to enhance the maturity of corporate governance.

4. Each level of the company that participates in risk management thinks in terms of how their processes and risks align with corporate objectives.

5. The risk assessment and analysis process addresses operational and compliance considerations (and their associated risks) to ensure alignment with corporate strategy.

6. Determining risks is often easier when first considering an objective, such as “What are the risks that will prevent me from achieving [fill in the blank]?”

When the risk determination process starts with company objectives and is associated with operational risks and compliance risks, risk determination is naturally aligned with corporate strategy. Once defined, all risks are assured to be associated with a corporate objective and therefore all risk treatment plans and associated costs are directly measurable to corporate strategic planning and revenue and profit expectations.

Linking corporate strategy to risk management is simple: Create an assessment that captures corporate objectives in your risk management software system, and then link it to the associated risks. For more information on how Cura Software can help you connect corporate strategy to risk management.

*Posted by Steve Money, Professional Services, Cura Software*

Read this article on the website [Click Here](#)
A question often asked is how broadly or how deeply do we need to design risk reporting in our risk management frameworks. Of course there is no easy answer. Let me give you a short anecdote before I give you my usual few dot points on the topic.

I was at a UNSW Australian School of Business "Meet the CEO" forum featuring David Thodey, CEO of Telstra late last year. David was asked what his greatest issue was in managing such a large organisation and he answered with words to the effect: Ensuring that I hear the issues I need to know about from the extremities of the organisation through all the other issues that are being raised with me. He went on to say: "You have to create a culture where it's okay to tell the truth, good and bad. Unless you create that culture of greater transparency, you can't fix issues". I wanted to yell out from the crowd of 400+ that risk management and, in particular, risk reporting should be in his mix to create that culture.

It is a fundamentally important question in risk management to ask how best to ensure a culture where the people with "the need to know" are "in the know".

Here are my tips:

*Business Planning - If you don't do anything else, ensure that managers that report regularly against budgets or business plans also report on risk to their budgets or plans using risk terminology.

*ERM or Operational Risk Committees - A fantastic way for emerging risks to surface in an organisation is via operational risk committees. OHS Risk Committees worked for safety issues, so why not ERM or Operational Risk Committees for organisational risk reporting? So, either broaden the responsibilities of the Safety Risk Committee or form an ERM or Operational Risk Committee
and have them report on risks identified, progress on risk treatments and any newly identified risks.

*Risk and Opportunity Hotline - I have not seen this explicitly anywhere, however, the concept has forerunners in "whistleblower" and "idea" hotlines. Put simply, advertise to staff there is a hotline for general staff to inform us of their thoughts, without prejudice, on the emerging risks and opportunities of the organisation. Move it from "whistleblower", which is more akin to staff alerting you to shut the barn door just after the horse has bolted, to a respected avenue for staff to alert us about "risky behaviour". Move it from "ideas" to identification of opportunities that fit within our advertised risk appetite.

Bryan Whitefield

Director, Risk Management Partners

bwhitefield@rmpartners.com.au

www.rmpartners.com.au

Read this article on the website Click Here
In my recent blog, I pointed out that regulations are constantly changing, becoming more complex. Global banks will find that proving transparency across multiple products to the regulators is a big challenge. All tier one banks operate with at least some legacy systems and some manual data sources, and can’t deliver all the required information in real time.

But transparency is key. Post-2008 liquidity crisis, global regulators are prescribing a series of new, more in-depth, regulatory returns. They clearly feel that the information would help banks operate more effectively, and are unwilling to relent on the new requirements.

The point of these new regulatory returns is to offer a more holistic view of the risks undertaken by institutions, not just to disclose positions. Banks need be able to prove two things:

1. That the decisions and investments they have made are prudent
2. That they understand the regulatory impact at the time of making trades

Banks will have to closely work with regulators, building trust and helping them understand how they run their business. To help overcome these challenges and become more transparent, banks will need to harmonise their data collection and where possible automate manual processes.

**Benefits from regulation**

There is a real positive side to this too. In moving towards a fully global, transparent data framework, banks will find opportunities. What banks need is a comprehensive view of their business situation, on a national and global scale. They will have to make sure that all data is clean, traceable and available in real time – this can be done by implementing a single platform, where they can collect all data.
If banks invest in an open architecture with an intelligent data model for regulatory reporting, they will find that they will be able to meet the challenges outlined here – and the impact will be to regain the public’s trust and, ultimately, secure more clients. They will be able to use the regulatory data they produce to better manage risk and improve their business decisions. And they will, of course, future proof their business against new regulations.

As a recent commenter on my post on the Global Risk Community noted, there are many difficulties and challenges for banks that report across multiple jurisdictions. He also noted, though, that by moving towards full Basel II (Pillar II and Pillar III) compliancy, many will find the transparency that they’re looking for – and I agree. Just in trying to achieve total compliance and transparency, banks will find real benefits.

Read this article on the website Click Here
Risk Management is all about managing the uncertainty around achievement of objectives. So all risk assessments should start with the objectives of the organisation, business unit, program, project, process or system that is the subject of the risk assessment. Strategic Risk Management is the management of uncertainty around the strategic objectives of the organisation. Doing this well requires skill, experience and commitment of the most senior people in the organisation.

When I recently read “RIMS Defines an Emerging Discipline – RIMS releases definition for…”, I did so with mixed feelings. In the article RIMS described Strategic Risk Management (SRM) as a “growing discipline” and RIMS “emphasizes that SRM represents an important evolution in enterprise risk management”.

I hate to be too critical of an organisation promoting ways to improve managing risk, but I don’t see SRM as an “important evolution in enterprise risk management”. It has been a fundamental element of Enterprise Risk Management (ERM) as long as I have been practicing in the area. ERM is management of risk across, up and down all of the enterprise. How can it not include management of uncertainty of the strategic objectives of the enterprise?

Where I do support RIMS is in their assertion that doing it well does require some degree of specialisation. Yes, the risk management process is the same for all risk assessments, however, gaining the insight and knowledge to assess risk effectively differs from risk assessment to risk assessment. So assessing risk for an IT project requires a different approach to a risk assessment of the strategic objectives of a large multinational.

When I conduct strategic risk workshops the first issue I explore with participants is whether the strategic objectives they already have are the right ones for the organisation in the first place. We
then move on to assessing risk to the agreed objectives. The key tools I use are:

1. Stakeholder analysis

2. PEST (Political, Economic, Social and Technology) Analysis for external environment scanning.

3. Porter’s Five Forces for assessing the competitive threats and opportunities within the industry my client is operating in.

4. Risk Management Partners Building Blocks Analysis which is an internal assessment of the quality of an organisation’s key building blocks, laying the basis for the Risk Management Partners Healthcheck risk management maturity model:
   a. Strategy and Performance
   b. People and Knowledge
   c. Processes and Systems
   d. Assets and Liabilities
   e. Culture

In my experience these four tools provide a very good understanding of the strategic imperatives for the organisation and reveal whether the strategic objectives already defined are the right ones. They are also excellent for identifying many of the sources of risk (uncertainty) to the achievement of the agreed objectives.

Bryan Whitefield

“demystifying risk”

www.rmpartners.com.au

Read this article on the website Click Here
Leadership in the Convergence of Governance, Risk and Compliance

Posted by Bryan Whitefield on November 9, 2011

It is inevitable for governance, risk and compliance (GRC) to converge. They are all about achieving the objectives of the organisation. For me, the greater debate is what role should an individual take as a leader in the convergence of the GRC space in an organisation?

It was no surprise that the International Federation of Accountants (IFAC) Survey, which assesses the need to align risk management and internal control guidelines internationally, found the need for an alignment is strong and that "both elements are integral parts of an effective governance framework".

IFAC goes on to call for international collaboration of standard-setting bodies, professional associations and relevant regulators to achieve this goal. A long road, but we will all be better off if we have one set of guidelines to compare ourselves to.

In thinking about all the stakeholders involved from governance, risk and compliance specialists, to accountants, career auditors, lawyers, actuaries and chartered secretaries it made me ask the question, who should or will own this space in another ten years?

What I do know is that the GRC space is multi-disciplinary. It requires someone with an MBA on steroids to be across it all. Hence I can see a need for specialists. That means no one profession will own the space. I can see the space remaining much as it is now with the GRC leader in an organisation coming from any one of a range of management or professional disciplines with a personal bent towards their professional background.

The takeout for a leader in the GRC space is:

1. Manage your own personal bent and ensure you give all aspects of the challenge adequate weighting. Where you have a weakness you will need to supplement with skills from one of the specialist disciplines.
2. Resist segregation of governance, risk and compliance. They are integral parts.

3. Insist on segregation of GRC from audit. The role of audit is to provide confidence that the GRC arrangements are appropriate and effective.

www.rmpartners.com.au

Read this article on the website Click Here
Risk Leadership: How to be Heard

Posted by Bryan Whitefield on November 7, 2011

Being a risk leader in your organisation is always a challenge. More than once I have been asked "How do you get a blustering, super confident CEO to slow down and listen to what we are trying to achieve in the risk function?" Unfortunately I don't have the silver bullet, however, here are a few tips which are explored in more depth in RMP's Whitepaper titled "Risk Leadership: How to be Heard".

1. Target - Identify all the stakeholders you need to influence. Identify the order in which you wish to tackle them. It is always best to get senior management buy-in first, however, sometimes that just isn't possible and you have to win over their key influencers before you can tackle them. Make sure you have a clear strategy.

2. Analyse - Identify their main motivators, their hobbies and interests. Your best opportunity for engaging someone that does not already know you and trust you is to ignite their interest through something they are already passionate about.

3. Tangibilise - Risk management has so many intangibles. You need to do your best to make what you want to achieve seem tangible to your target audience. People comprehend best when you provide them with both visual and verbal descriptions. So draw a picture and tell them a story. Choose examples that are most likely to relate to their motivators, hobbies and interests you have identified.

4. Translate - Speak their language. I call it moving from "risk speak" to "c-suite speak" when engaging senior executives. Too often we simply blurt out what we know is needed in what we might consider to be simple risk language, however, it means almost nothing to our audience. Try talking "inherent risk" to a CEO. You know, the world without controls. You would agree, a better approach would be discussing the need to identify where we may be able to save some compliance costs by understanding which of our current controls are most...
important and which are not. You can then inch towards using risk speak as you gain their attention and then understanding.

Bryan Whitefield
Director, Risk Management Partners
Ph: +61(0)2 9400 9702
Mob: + 61 (0) 403 625 143
Web: www.rmpartners.com.au

Read this article on the website Click Here
Risk Leadership: Knowledge is Power

Posted by Bryan Whitefield on March 13, 2012

When we conduct risk assessments we are often satisfied with the outcomes based on our existing knowledge. Our knowledge however is usually based on some facts and a whole lot of assumptions, perceptions and theories.

As human beings we use our five senses of sight, smell, taste, touch and hearing to maximise our knowledge about our environment. During a risk assessment we need to find similar tools to make sure we maximise our knowledge to help ensure we identify and appropriately analyse risks, opportunities and design effective risk treatments. **Here are a few tips to consider when conducting or participating in your next risk assessment:**

**Assumptions** - A first point of call is to make sure you identify key assumptions and validate them as well as you can. Beware of senior people pulling rank because they believe this is what worked best for them - it may no longer be valid in our fast changing world. Similarly we can have assumptions that everyone is aware of, but no one in the room can identify where the assumption originated from - you will need to do some digging.

**Perceptions** - Perceptions can vary between people for a myriad of reasons. Our socio-economic, ethnic and geographic backgrounds, just to name a few. A big issue in risk assessment is when we all have a common perception of a subject matter or issue that is wrong because we all have the same underlying drivers of perception. The best way to combat this is to make sure you involve a variety of people in a risk assessment. Don't limit participants to those intimately involved with the subject. Invite "outsiders" that are likely to have different perspectives such as inviting a sales rep into a risk assessment of a back office function.

**Theories** - I advocate a scientific approach to analysing the theories present in a risk assessment. Scientists establish theories and then try to disprove them. They design a multitude of
experiments that should, if successful, disprove the theory. If they can't disprove it they become increasingly comfortable with the theory as being a fact, without ever being able to prove their theory 100%. Similarly in business, we can never guarantee the success of a new product, for example, but we can certainly increase our knowledge and hence our comfort levels by challenging the original theory with a few well designed "experiments".

www.rmpartners.com.au

Read this article on the website Click Here
"Who is to blame?" How often do we read that line in a newsletter or magazine article about a legal dispute when it all went wrong? Too often, we ignore those little clauses in contracts called indemnities. A slight change in wording in an indemnity can vastly change the circumstances of who pays how much if it does all go horribly wrong. Sometimes the contract gets signed without proper legal review and when we do have legal review, we often suffer from either the Optimism Effect or the Pessimism Effect.

**Optimism Effect**

The optimism effect is the "It won't happen to me!" attitude. Even worse, it may be the extreme "Don't be absurd. Get on with your job!" attitude. The result is often exposure to events that can shatter an organisation leaving the optimists ashen faced saying "I can't believe it!".

**Pessimism Effect**

The pessimism effect is where commercial reality meets intransigence. Some principals simply will not budge on their insistence to transfer unreasonable levels of risk onto the contractor. Pessimistically, managers may say to themselves "Someone is going to take on this risk which they could never manage or afford to fund if the event occurs. We can't cut ourselves out of the market completely. We have to agree to the indemnity".

As a Risk Leader in your organisation you need to be aware of the optimism and pessimism effects. You need to help decision makers consider the certainty of the upside the sales people are predicting vs the remote but potentially company-destroying risk of a one-sided indemnity clause. As a Risk Leader your most valuable tools in these instances are a well articulated risk
Risk Leadership: Facing Extreme Contractual Liability Risk

appetite for the organisation, signed off by the CEO/Board, along with some statistics about issues in similar contracts.

www.rmpartners.com.au

Read this article on the website Click Here
One approach for embedding a risk management culture across your enterprise is to develop a team of risk champions within your business. What should you expect of them and how should you equip them?

The answers to these questions are not straightforward. When you are dealing with cultural change the strategies that work best will depend on a myriad of elements that have occurred or will be occurring in your organisation. Here are some practical questions to ask yourself that will help you to decide how to develop your team of risk champions:

**Quality - How skilled and resourceful in risk management do you want your champions to be?**

Do you expect them to conduct top quality risk assessments in their sphere of influence or do you want them to be aware of when a top quality risk assessment is needed and where to find the assistance to get one done? Do you want them to be well versed in articulating risks in their risk reporting to management or do you simply want them to be aware of the requirements for risk reporting? How skilled are they now and how skilled do you want them to be in 3 months, 6 months, 12 months and 2 years from now?

**Quantity - How far do you want your champions to roam?**

Is the frontline culture of your organisation strong on managing risk associated with day-to-day tasks or is there an urgent need to change the culture of frontline staff? If the frontline is not the problem, perhaps it is middle management and their lack of application of risk-based decision making that you want to tackle. Cultural change at the frontline will require potentially many more champions than if your challenge is with middle management.

---

**Risk Leadership - Creating Risk Champions**

Posted by Bryan Whitefield on May 23, 2012

Bryan Whitefield
Performance - Are you planning an informal relationship or is the need so great you need to include specific elements of accountability?

How does this fit with the culture of your organisation? Do you have the skills and resources available to you to "win over" your champions through an informal relationship that will result in a strong performance by them?

Leadership - How are you going to lead your team of champions?

Will you form a key operational group that has strong input into the risk reporting process of the business or will you leave them to operate within their businesses and only bring them together periodically for communication and consultation on developments in the risk management space?

www.rmpartners.com.au

Read this article on the website Click Here
Rescorla, Boisjoly and LeMessurier - These names may not be familiar to you, however they all have a prominent position in James Chiles book "Inviting Disaster".

Rescorla was the head of security at Morgan Stanley in the South Tower of the World Trade Centre at the time of the 9/11 terrorist attack. After the bombing of the underground car park of the World Trade Centre in 1993, he warned the firm of a possible terrorist attack from the air and that the firm should consider moving to another building. Because the lease was not up until 2006 no action had been taken by 2001. When the first plane hit the North Tower he acted on his earlier concerns and immediately started evacuating his staff in the South Tower while other firms delayed. Only 7 staff were lost, including Rescorla who was personally checking floor by floor that staff had been evacuated when the tower collapsed.

Boisjoly was an engineer at Morton Thiokol, the firm responsible for the design of the space shuttle rocket booster that sent the shuttle into orbit. Their design included the "O-ring" that failed on the Challenger shuttle in 1986. In a telecon with NASA the evening before the launch he had convinced his manager to refuse to sign off on the launch approval due to problems associated with inflexibility of the "O-ring" under cold temperatures. After much harassment from NASA, due to pressures of public image after several delayed launches, objections were withdrawn and sign off on the launch was given at a higher level. Boisjoly watched the launch the next morning at the behest of his manager only to be shattered by the resultant mid-air explosion. "Boisjoly spent the rest of the day in his office, not even able to speak when people stopped by to ask how he was doing."

LeMessurier was a structural engineer who designed the Citicorp tower erected in Manhattan in 1978. After the building was
occupied he became aware of a number of construction issues and after investigation he discovered there was a 50/50 chance of the building collapsing due to wind stress that is experienced in Manhattan roughly every 15 years. He could have kept quiet as his firm was partially to blame, however, he spoke out. The building was retrofitted and made safe. His admission lead to praise, not ridicule.

These Risk Leaders, although not one was fully successful in their original quest, show what is required of a strong Risk Leader:

1. Commitment to their firm and staff
2. A mind attuned to identifying and analysing risk
3. A willingness to take the difficult course of action

There are many more Risk Leaders who have not been written about in a book - because their message was heard. When you know something is wrong in your organisation, how far are you willing to push the issue? Do you have the knowledge, understanding and skill to deliver the message? Are you heard?

www.rmpartners.com.au

Read this article on the website Click Here
Pareto’s Law: 20% of your assets will be exposed to 80% of threats. Do you know which ones?

Posted by Tony Ridley on June 28, 2010

Bad weather or even natural calamities do not affect every city in the world nor every resident of the affected area. Accidents, an inevitable part of some environments, do not affect all your people or totally devalue all your assets. Terrorist do not consider everyone a viable target nor are their actions likely to impact everyone over the course of their lives. The facts remain that only a small percentage of events or incidents resulting in loss of value or productivity will affect your business but conversely a smaller part of your overall assets are likely to succumb to these events; possibly even repeatedly. If this is the reality, why are there so many singular strategies for organizations, one-size-fits-all policy, uniformity in the approach when greater economy could be achieved by focusing on the priority areas? Most of the threats (80%) will only likely place at risk a smaller percentage (20%) of your assets. Do you know which ones?

Too much time and deliberation is spent perfecting the process of identifying and qualifying the threat. While it remains a valid and useful phase the process becomes unexplainably weaker or less popular once value and measurable impact are introduced. This is in part possibly due to the skill and experience of those conducting the analysis/assessment who typical originate from a
Pareto’s Law-20% of your assets will be exposed to 80% of threats. Do you know which ones?

weak financial background. Even for those with little resources, training or even time, a qualifying exercise to determine what the impact of service failure, disruption or other stressors will provide you with a workable project plan for applying solutions, counter measures or treatment options. This should have financial implications, tangible and intangible. The higher the number, the greater the priority and easier to be presented to business leaders or collaborators. The easier you make the measurement or driver, in a format most commonly used, the greater adherence and buy-in you will get. Abstract terms, ratings, scientific pontification or just made up data will only erode the objective and almost all will lose interest. No single person ever saved an entire organization, it takes systems and team work that follows a plan.

Many conventions are derived from habit or transferred from what others believe to be comparable models. Take fire sprinklers and suppression systems for example. A worthwhile investment and certainly mandated in some jurisdictions to prevent loss of life, undue stress on public services or even making local authorities look bad. Whatever the driver they are common place. However, not every square meter of a building is at risk of having a fire originate in that locale. Much of the planning and installation works on the assumption it could start anywhere, spread anywhere so lets just cover the entire structure. Not necessarily an efficient or effective process but wide spread practice none-the-less. Transferring this methodology to all/any other part of the business would have questionable benefits or make financial sense. These kind of general applications of similar strategies discredit the validity of risk management and force undue cost onto organizations that quite reasonably at times will forego the entire solution because the bulk of the concept is unnecessary, leaving the critical minority (20%) unprotected.

Vision and direction begins with policy. However, this policy is a guiding principle with brevity and clarity not a standalone document. It should include the priority of care or concern such as people, brand, buildings, etc. Priority of response along with the objective of the efforts should be made clear to all. Any and all measures, outlined in subsequent procedural documents and
training, should be measurable (financially, operationally and even brand integrity) and constantly reviewed. While policy is unlikely to change for longer periods of time, the process and even certain objectives may as the business changes in both culture and nature. The most effective policies are a single paragraph that encompasses all the aforementioned elements and does not dictate tactics for execution but ensures everyone at least moves forward in the same direction.

Data is a great tool for creating foundation analysis but it should originate from both objective and subjective sources. Single minded collection, measurement and review lead to much bigger falls. No company knows everything about itself or everything else around it, no matter what some may think. Comparative information, data, review and even assessments ensure greater transparency in the final outcome. Care needs to be applied to ensure it is not a popularity contest or management by consensus, a final impartial decision maker is still required. Companies of all sizes can apply this approach cost effectively and expediently while enjoying maximum return on investment not just plain old return on investment (ROI).

The clock is ticking, the world moves on and the business you had an hour ago is not the one you operate now. The process needs to be renewable, adaptive but above all constantly applied by monitoring and surveillance. Monitoring is required of the business, its actions, its impact, resources, threats, disruption impact potential and relevance to the overall business concerns. Many events that arrive on the doorsteps of your business first visited your neighbor or the business down the street. Just because you weren’t watching will not get you a leave pass on the impact your lack of preparation may bring to your organization. Larger companies have internal resources for this purpose, but the smartest have both internal and external for the reasons of effectiveness previously mentioned. Smaller companies, increasingly thanks to technology and a global market, can enjoy all the benefits of outsourced support that the larger companies
Pareto’s Law- 20% of your assets will be exposed to 80% of threats. Do you know which ones?

Do without the cost of ownership or inefficiency but with all the benefits.

Only a fraction of your workforce are at risk; a percentage of your travelers too. Not all your fixed assets are of equal value nor will they be exposed to the same single loss expectancy (SLE) or annual loss expectancy (ALE). Only some markets need heightened levels of support and protection as much as only some markets are the most valuable to your overall financial health. Every single email piece of information your company possesses shares the same value. A single piece of code could be worth thousands but a warehouse of files could be nothing more than an administrative cost and operational burden. The problem with this all is that most companies simply don’t know which end is which. The one-size-fits-all approach is cheap, easily understood and been around for years. Secretly the more profitable, efficient and even safer companies have dispensed with the rule-of-thumb and focus their 80% resourcing on the most valuable 20% assets. Do you know your most valuable assets and are they better preserved than the lesser value assets? Or are you just applying the same approach for everyone, thing, process or bit because that is the way it has always been done?

Read this article on the website Click Here
Volcano Lessons: Preparing for future events

Posted by Randy Park on June 22, 2010

Note: This was posted on my blog a couple of months ago, but I just joined here, and I think the message still applies...

Randy Park

The Issue

If you've heard me speak at a conference or another event recently, you likely heard me say that in many important areas no one can predict the future.

So if you don't know what will happen, how can you prepare for it? The solution to this dilemma is that you don't have to predict future events in order to prepare for them.

We have a recent example with the Eyjafjallajokull volcano. Could anyone have foreseen the effect a single volcano could have on air travel around the world? Careful now, because that is a trick question: I am asking if anyone could have foreseen the effect, not the volcano.

The Thinking

People generally are not very good at looking to the future. There are many solid scientific studies detailing some of the failings in human thinking. Some examples: the first information we see "anchors" our expectation; we jump to conclusions; what we see is filtered by our experiences.

These characteristics of the hardware of our thinking result in several common behaviours from many people when it comes to preparing for future events. In order of increasing awareness, they are:

1. They don't look to the future at all, or
2. They look to the future, but decide future events can't be predicted so there is no point spending time on them, or
3a. They look to the future, consider some possible future events, but decide they are extremely unlikely and there is no point spending time on them, or
3b. They look to the future, consider some possible future events, and decide they can predict the future, so there is no point spending time on any other possible future events.

The problem with these approaches, even 3a and 3b, is that they are event driven. And probably the biggest failing of human thinking is that if something hasn't happened to us personally, we find it extremely difficult to conceive it will ever happen. So if you have personally never had a computer fail, or a hard drive crash, it will be tough to convince you that backing up your data is a necessary task. (Having worked with computers since the early days when they were much less reliable than they are now, I have had many such experiences, and thus am probably better than most at backing up my data.)

Instead Look at Consequences

Even the burgeoning field of risk management is often about identifying and quantifying risks, rather than looking at the consequences of the risks and most importantly how to minimize the consequences.

But if instead you look at what the effects would be if you lost some critical systems, you can prepare for future events without necessarily predicting why they might happen.

What would you do if some or all of your business or your work was disrupted? Start by asking simply "what would I need to do?" (You can look at how it might be disrupted, and how likely later on.)

Some specific examples:

**Systems:** telephone, Internet, loss of a computer, Blackberry, web site, e-commerce site, or electrical power (our power here in downtown Toronto is so reliable, I almost forgot that one!)

**People:** key personnel - what if someone was hit by the proverbial bus? And remember, almost everyone in an organization has unique knowledge. If you're working to a tight deadline on a project or a proposal, and the one person who knows where to go for the special binding is away, you may miss your deadline.
Suppliers: How vulnerable are you to a supply disruption, either short term or long term? What if a supplier shuts down for some reason? When I have designed electronic equipment, almost invariably there would be several times during the design when a decision had to be made: should we use a unique part which would enhance performance but is available from only one source, or compromise performance but have a design that wasn't dependent on a single supplier?

Customers: what if your largest, or several of your largest, customers went away (for whatever reason)?

In 2008 many financial professionals claimed "no one saw the recession coming" (though I maintain there were many warning signs.) Many investment advisors and investors were caught when they didn't examine what would happen to their investments if the stock market went down. As a result, they lost a lot of money, and some have had to delay retirement. Even without the warning signs, it was possible to prepare for the consequences of a stock market crash. I rebalanced investments in the summer of 2008 not because I predicted the stock market crash, but because I thought about the possible consequences and decided I didn't want to be worrying about which direction the market might take.

Some Examples

The Globe and Mail newspaper had an article discussing how various people who were stranded by the volcano handled the situation. For me, the most instructive example was the News Director from Corus Entertainment in Vancouver who was stranded in London. Corus had developed a process for employees to work remotely in response to the fears of a flu pandemic and disruptions from the winter Olympics. The fact that the system was already in place allowed him to be instantly productive. I'm sure no one at Corus was thinking of a volcano when they planned their remote work capability!

On a personal note, I always carry two laptop computers when going to do a presentation. It makes for a heavy bag when travelling through airports or up and down stairs. Yet after doing this for years, one time the graphic card in one of my computers...
failed. Without the backup computer, I couldn't have presented my slides.

**What Steps Should You Take?**

Identifying vulnerabilities is best done as a bottom up approach. Each employee knows their job best; asking them what is essential to the performance of their job is a good starting point. There is a worksheet at the end of this article to assist you with the process.

Sometimes having someone "interview" an employee can help them identify the equipment and tools they take for granted. This can be another employee in the organization, but be careful: unless they are from a different department they may be making the same assumptions as the interviewee.

In consolidating this information, I am a big believer in visual sharing of information. Bringing people together to jointly share their knowledge and experiences is most effective when everyone is looking at the same view.

We use tools such as Mind Mapping, Concept Mapping, and other types of diagrams to record this information. Decision making tools such as the Paired Sort tool can be used to prioritize items.

If you start at the individual level, and work up through departments to the organizational level you can consolidate the information and identify priorities. But remember not to ignore something simply because it doesn't seem likely (remember the volcano!)

Allocating a small but definite amount of time each week to creating and them maintaining these systems avoids the possibility that the effort fades as quickly as everyone's memory of the volcano.

Once the information is in place, taking it to the next level can involve Scenario Planning and System Dynamics to examine and model possible future events.
Conclusions

Back to the first question - while it is unreasonable to expect anyone to have predicted that a particular volcano would erupt in a way that would shut down European air space, it is entirely within reason to anticipate some event that might shut down air travel. (We even have a precedent with the days after 9/11.)

It is not possible to predict future events in many important areas. It is not possible to plan for every single eventuality. But you don't have to predict what will happen to be prepared, just think through the consequences of it happening.

As air travel in Europe returns to normal, I hope organizations will take away the right lesson. The obvious lesson is "no one could have predicted a volcano." The better lesson is "we must examine our vulnerabilities to unforeseen events."

Worksheet

About Randy Park

Randy Park, founder of Decision Advancement, specializes in helping organizations to get better results by making better decisions. He holds Bachelor's and Master's degrees in Physics and brings to his keynote presentations the critical thinking reflected in his study of how people think and make decisions, and the analytical thinking reflected in his physics and mathematics training.

Randy is the author of two books. In "Thinking for Results - Success Strategies" Randy explains the core aspects of how we think and make decisions. His second book "The Prediction Trap - and how to avoid it" extends the concepts to situations where we are looking to make decisions about the future or decisions involving other people. Globe & Mail columnist Eric Reguly described The Prediction Trap as a "stimulating book... a must-read for anyone who wants to confront the temptation to sacrifice long-term planning for short-term gratification."
Many companies navigate the routine complexity of business with adequate or acceptable management, however it is the truly stellar company/s that excel not only on a routine basis but especially in times of crisis. It is select skills, experience and traits that are able to applied during times of critical decision-making that separate them from the herd. Specific skills and attributes are not something that can be learnt in the minutes and seconds required in order to apply to a critical decision making process but are acquired and developed over many years and supported by advanced processes and tools.

To understand the best-in-class for corporate crisis management and decision-making we need to consider a number of things. Given that the timeliness of response is often predicated on how little time is wasted on logistical or bureaucratic processes before getting to a point of action, therefore companies with existing policy and procedure that is both rehearsed and updated, put themselves in the top 10 to 20% immediately. This element is certainly not a significant contributor to their success our outcome. Second, the quality of information on which decision-makers and leaders are basing their actions upon. This information alone does not comes from traditional sources such as television and paper it increasingly is inclusive of social media. The voices of many, albeit nonofficial, can have a significant
impact on the outcome of the overall damage/survivability of an incident faced by a company.

The best-in-class companies not only acknowledge social media but have means of tapping into influencing and monitoring all social media channels as required, not just in times of crisis but on a routine basis. Lastly and most significantly it’s the character of the individuals that fill the functions within a crisis or communications plan. It’s this area will look in more depth to determine the requirements attributes and success factors as crisis management is seldom the catalyst for success or failure but that of crisis leadership.

In Malcolm Gladwell’s groundbreaking book The Tipping Point he mentions three significant class of character that are an important influence on social trends and epidemics. These three main character traits are also vital if not pivotal in the success of corporate communications and crisis response. Companies that lack or fail to identify and leverage from these key character and personality traits fall far behind the best of class and most innovative companies. These character traits and abilities are not governed by job title position or function they are skills possessed within a person and therefore should be leveraged in accordance with the skills to the desired outcome rather than relying on a predefined job title or function within the company. These three character traits are 1. Connectors. 2. Mavens and 3. Persuaders. In very rare instances one or more of these skill sets may be founded in a single person but any one person shouldn’t be relied upon in adding depth to any team, which is always sound practice.

What makes someone a connector? The first–and most obvious–criteria is that connectors know a lot of people. They are kinds of people who know everyone

No great team has all the solutions nor knows all of the information, however is vitally important that the team have access to an individual or group of individuals that can connect to all the known and possible resources in a short-as-possible time period. Connectors as such are fantastic networkers with not only
huge personal networks but also plug into other complementary networkers or fellow connectors that maybe industry, technical, media or stakeholder orientated. They can aide immensely in benchmarking or calibrating the sentiment of particular decisions/actions or even the most appropriate channel to make sure that their message is heard clear and concisely with the required outcome.

Every company should have at least one connector in a crisis or communications team or one that can be called upon quickly and effectively. It should be painfully evident this is not the type of skill or network that is built up overnight and therefore can’t be expected to be turned on by the flick of a switch; it may take years if not decades to develop and refine.

Second of the three kinds of people who control the work of mouth epidemics are a Maven. The word Maven comes from Yiddish, and it means one who accumulates knowledge.

Mavens are active if not and borderline fanatics in their collection of information relative to a specific discipline or social scenario. Once again it’s essential that corporate decision-makers and crisis management teams include such knowledge collectors. Some companies may have them within their own organic structure or call upon them as part of their service providers or trusted advisors, in some instances even board members. Mavens may manifest in many shapes, forms, gender and age but they are very quickly identifiable by their sheer depth of knowledge and cross-referencing ability to join problems with solutions. A single conversation with an effective Maven may save corporate decision-makers hours if not weeks of procrastination and circular discussions.

Mavens are teachers, Connectors are conduits but neither may be Persuaders and the reality is that some people are actually going to have to be persuaded to do something, this is the role of the persuader. A Persuader is not a snake-oil salesman, although many very effective salesmen and communicators are Persuaders. Persuaders are able to influence through their tone of voice, their physical appearance, their social observations, their empathy.
towards listeners or just in the way and manner they use all of the skills to communicate their particular message. Many famous politicians, while drawing criticism for their lack of knowledge and other skills, have been exceptional persuaders. Not advocating the requirement for “empty vessels” but persuaders have a rare and unique talent to be able to communicate and influence people to do something, that something being consistent with your objectives. It is a very dangerous process to use any of the identified skills and characteristics in the roles in which they’re not suited, in particular the use of a persuader in a lesser role or not that of an influencer.

Many can now probably identify these key character traits and how successful they have been in routine and critical environments. However, it should be of major concern if you can not identify these traits within your own corporate crisis and communications team. Additionally if you have a total absence of any-and-all of the skill sets within your corporate crisis and communications team. You may survive the day to day routine rigors of business but survivability rate when exposed to critical incidences without these key elements is very poor. Even worse are those that assume that job titles within the company or even gender have imparted these skills upon each and every one of their senior executives is a gross oversight. The question remains can you identify these assets or can you contact them on your worst day? Your survival may very well depend on it one day.

1. The tipping point by Malcolm Gladwell chapter 1–The three rules of epidemics, page 38
2. The tipping point by Malcolm Gladwell chapter 1–The three rules of epidemics, page 60

Read this article on the website Click Here
Human Capital Risk Management-What’s Missing?

In spite of the considerable investment and development around the preservation of assets and the mitigation of risks across conventional corporate assets such as facilities, information, equipment and products, the same methodology and motivation remains far less advanced in regards to human capital.

Before any organization even explores risk management strategies for their human capital it is fundamentally important that they first determine the value at risk. Not only is it a case of valuing the contributions of the individual or groups of personnel but differentiating the value in which they contribute to the company, whether it be through the provision of specific skills and services or the commercial value they present the company. These distinctions also need to be made between job functions or management/executive levels. No two individuals are contributing to the company in the same manner, much less two diverse business functions. How many companies even know this definitive financial value of their people?

Following the basics of valuation, and any other unique considerations that the company may have (mobile work force, fixed laborers, knowledge capital, research and development) a unit cost can then be applied for prioritizing strategies or expenditure. For example, an individual that reflects a unit cost/investment per hour of $1 will be less likely to addressed as a priority when compared to an individually that presents a unit cost/investment per hour of $100. However, if there are significant numbers of the basic unit cost of $1 at risk, that group as a whole may be a greater priority than that of a single or limited $100 per unit cost individual.

Threats and residual risks associated with human capital are many and varied. Over time a detailed and thorough analysis can be conducted to determine the probability, velocity of onset and other governing factors that will provide a single or annual loss expectancy to the company. A single loss expectancy, such as
death, may cost the company significantly more than just the forecast value identified in the first stages. Conversely, an annual loss expectancy, especially in light of the fact many companies are unable to even quantify this loss, may equate to millions of dollars in lost productivity, administrative burden or opportune costs.

To truly understand or appreciate the current or potential losses to a company through their human capital it is imperative to model the disruptions and time loss (inclusive of management and departmental support) to a cellular and group level. If someone falls ill, how long are they unproductive? What does it cost the company? Should the become a victim of crime or their business activity disrupted due to a natural disaster, what is the cost to the company? When applied to our entire human capital asset base, what is our single and annual loss expectancy?

“You can’t improve what you can’t measure” If you are making a truly informed decision on where your assets are distributed, you can then make informed decisions around strategies to preserve their value. You also enjoy the benefits of comparative investment/management. Most companies are surprised to discover that despite their commitment to their people, they actually devalue their contribution by not acknowledging them as an asset and preserving it accordingly. Are you one of those companies?

Companies that have undertaken to approach the management of their human capital consistent with other corporate assets have found the process highly rewarding and very confronting. Conversely, those adverse to such strategies or behind the curve continue to loose more money than the cost of such preparation and mitigation. They too find over time that penny wise turned out to be pound foolish.

Read this article on the website Click Here
As a global business executive, I know first hand the demands of travel. I spent more than 120 days out of the year on the road, and have supported the traveling workforces of clients every day. So how do I stay connected? Here are my thoughts on the best apps for Android smart phones – a critical tool for helping me stay in touch and on top of things while traveling.

“Like most people I use my smart phone as both a communications tool and mini computer while traveling or on the road. My Apple iPhone is my primary device, because I like its exhaustive selection of applications. However, for those times when I need to travel with a second handset (to save on data roaming costs or to access local networks), I use my Android OS phone, which also offers a great range of apps.

I am constantly testing and sampling new apps to meet both my own requirements as well as those of our clients. Below is a list of my favorite travel apps – those that I find indispensible to helping me stay engaged even as I cross time zones. I selected them based on three criteria:

Provision of knowledge or data that I don’t possess myself

1. Backed up by expertise and a richer web-based content version
2. Ease, speed and functionality of the application version

Here are the key travel applications that I would recommend for iPhone and iPod Touch users:
WorldMate (Gold)

This application is the powerhouse of all my travel management requirements. I can centralize and view all my relevant travel information from flights, accommodation, meetings and various other travel support options. WorldMate (Gold) is the portable version of the online (cloud-based) application. WorldMate even helps me visually map out locations, distances and travel requirements between airports, hotels and meetings in Google maps.

TripIt

This application has some overlap with WorldMate. However, I use TripIt because it primarily allows me to share my travel location and dates with colleagues, clients and even family. My itinerary can then be synchronised to prevent conflicts, or keep select contacts informed of my travels. This application works great with social networks such as LinkedIn. It also tracks my cumulative trips, countries visited, cities, miles and nights spent on the road. Lastly, it links me to the International SOS travel group so we can see where our fellow team members are traveling or have been.

XpenseTrkr

An inevitable part of traveling is accounting for expenditure on expenses. Therefore, I find this tool excellent for keeping independent and accurate tabs on all my spending, expenses and other reimbursables. The cumulative archive of all my trips also helps in planning and future budgeting.

Tungle

I have a lot of meetings. It seems everyone in every company has a slightly different platform for managing e-mail and scheduling calendars. Additionally, I loathe endless e-mails and text messages back and forth purely to determine availability and the best time to meet.
Setting a meeting time can be complicated enough with just one person but is further compounded when multiple parties are involved! Tungle is the perfect tool, centralizing all of my meeting appointments and quickly and simply determining both my availability and that of the client, colleague or other parties. This tool is fantastic as it synchronizes my desktop calendar, mobile device and web-based applications.

**FlightTrack Pro**

Before I even commit to a trip or a meeting I like to know if there are compatible flights for the time and location required. I find FlightTrack Pro an outstanding tool to determine the reliability and flight options to and from specific locations. In addition this tool also gives me the probability of departure and arrival running according to schedule. This application is great not only for my own travel, but also for being able to track the arrival and departure flights of friends and family.

**Evernote**

This is an excellent productivity tool that I find invaluable for travel also. Evernote enables me to cut & paste, capture, drop or simply add all the information relating to a particular trip or multiple trips. This application synchronizes between desktop applications (Outlook, Word, Internet Explorer, clipboard, etc). This ensures that all the information such as itineraries, hotel bookings, restaurants, navigation guides to client offices, local or translated phrases, maps and anything else I synchronized is available in electronic format whenever I might need it. I create separate folders for each location or activity, enabling me to quickly and efficiently access the information without opening my laptop or carrying around lots of printed or duplicated sheets of paper.

**Foyage**

Because I’m constantly bouncing around from one location to another, I often find myself in locations
that I may not very familiar with. It is important to me than I make informed decisions or find locations quickly and efficiently.
I therefore use this application to help me find other people in my network, ATMs, restaurants, supermarkets or anything else I may need quickly and simply.

Dropbox

I’m constantly working on projects, information, issues or hobbies between multiple computers or formats. I use this daily to quickly share files and content between computers, colleagues, clients and myself. I can even review presentations and notes from my iPhone just before a walk on stage without having to print or open my laptop.

Worldcard Contacts

The management of information – and in particular contacts – is becoming increasingly challenging. To help me with this process I use this application to make an immediate copy or store a contact business card. The information is scanned directly into my contacts list, but I can also reference this directly on my iPhone. Built-in functions allow me to call, text, email, or navigate to a particular address directly from the electronic copy of the business card. This application has saved me hours of heartache and provided timely access to valuable contacts and details.

Convert Everything

Part of the excitement of travel is often from the challenges foreign environments bring. Everywhere is different. Different measurements, different currencies, different languages and so on. This application can help with converting pretty much anything I want transferred from one unit of measure/language into something else.

Read this article on the website Click Here
Crisis Leadership is better than Crisis Management

The Golden Hour and the First 24 Hours!

In the vast majority of cases, regardless of the duration, the end success or successful resolution to a crisis is determined by the initial actions in the first 24 hours. Often referred to as the “Golden Hour” in emergency medicine, the initial hour of the first 24 hours is the foundation upon which the primary phase is predicated. The events, information and decision making process during these two phases will place both individuals and multinational corporations upon a path that will over time will provide less opportunity for change and influence than at this juncture.

While the incidents and information injects, whether actively or passively collected, may change, the fundamental decision making methodology will remain relatively constant due to the leader or crisis management teams experience, skills and training. It is for this reason that the greatest emphasis due to the potential outcomes remains the burden of those in a position to determine the outcomes.

In broad terms, individual entities or multi-dimensional companies are classified into two categories when managing a crisis or significant event. The first of those categories is that of the Responder who is largely driven by the events and is forced to react to each and every information inject or demand due to the absence of preparation and planning joined with the lack or limitation on resources. The second of these two categories, and the most desired, is that to the Implementer who is characterized by the ability to activate resources and follow a pre-prepared and trained plan with the support of an array of supporting stakeholders, constructed responses and proactively formulated
decision making guidelines that reduce the time from event to response.

The Implementer would typically be equally experienced as they are trained with significantly more emphasis on the latter. The primary and secondary phases of the first 24 hours will see the Responder desperately attempting to understand the situation, often with limited redundancy and support, while trying to time appropriate responses and activation of resources with little understanding of the strategic goals or longer term effects of these crucial decisions. This will be further exacerbated by the lack of experience or knowledge on the time taken to implement plans and the activation of vital resources.

In contrast, the Responder during the primary and secondary phases will be aligning support plans and stakeholders with preferred outcomes and anticipating events to potentially mitigate escalation of the situation or becoming reactionary focused. Typically the Implementer will seek to maintain a rapid escalation of support elements and appropriate resources with the option to then gradually deescalate or stand-down a range of options appropriate to the incident once they have sufficient control of information that the situation does not warrant the engagement of such resources or services.

History and more contemporary times are littered with examples whereby Government Leaders, Military Commanders, Corporate Leaders, Community Leaders and the like have failed to identify the impact of the events or incidents that have ultimately lead to an apparent disproportional result. Their failure or lack of appropriate response, relative to the potential impact and not necessarily the current information or perception, has lead to dire strategic consequences. As a result, it is these initial tactile decisions and responses that can in all likelihood determine the eventual outcome, favorable or otherwise.

The Golden Hour in medical terms is the most crucial time in which to both stabilize a patient suffering from significant injury or illness and to determine the best course of action in order to
provide them with the most appropriate form of medical care supported by adequate resources. This decision making process is often done in remote locations, at the scene of an accident or within the emergency rooms of the nearest treatment facility. While this reference is centered more towards an individual or groups affected by such events the process and outcomes are indicative of the interaction it has with all the stakeholders affected and the commonalities faced by business in general.

Firstly, the affected parties may well be key elements to an organization or business that is dependant upon their contribution and will undoubtedly respond with all available resource for both the preservation of life and the continuity of business. Secondly, the process for escalation and decision making, including the activation of services and resources, will be made in the absence of a technical expert such as a doctor. As is the case with almost all business crisis in the initial stages. Even then, the measure to which any trained and experienced expert pertaining to crisis management will be limited to a large degree by the actions of the first responders and their support resources.

Tactile and spontaneous decisions made in the immediate stages of a developing incident that could lead to a crisis or disaster event have strategic consequences. These consequences may not affect an immediate impact but overtime could overshadow the incident itself. For instance, the decision to act in the absence of consultation or verification could result in legal, compliance, ethical, morale, code of conduct, medical or criminal violations to which the parent organization will be responsible, or held to account, for the actions of one or more responders. Irrespective of the fact that the decision at the time may have in fact saved lives, prevented further disasters or simply maintained business continuity the strategic consequence could be just the opposite.

While it is neither effective nor possible to script every potential incident and provide policy and processes to support such events, especially in the event of crisis, it can go a long way to mitigate many of the aforementioned issues and negative impacts. Even if during the post incident autopsy it is confirmed that a sound and consistent decision making process was employed with an
appropriate degree of accountability and supported resources but ended in a less than favorable outcome, it will hold the organization and the individuals in far greater stead to know they did their utmost at the time but the situation was not recoverable despite best efforts and planning than to have made spontaneous decisions and decrees on the fly.

Enabling first responders, supervisors and crisis management elements to draw upon the collective knowledge of their peers and industry experts, with pretreated plans, budgets and designated resources appropriate to the risk and potential impact will significantly reduce the time from incident to response and prove to be a better overall strategy for the management of limited and significant crisis events. These plans should be both comprehensive and accessible to those that require access it but also simplified for immediate reference and implementation. This is equally applicable to any support services or resources that may be required in the event of particular incidents. Should partial or full responsibility of supporting this process be apportioned to external agencies or third party providers then they in turn should be equally if not more prepared for their roles and responsibilities. Sadly, all this amounts to nothing if the plan is not widely disseminated, trained and rehearsed with a degree of regularity to account for changing circumstances and new talent and roles.

While crisis management is often discussed and held up as the benchmark of preparedness and effectiveness, this is essentially still the realm of the Responder. In order to manage a crisis there is a disproportionate amount of time spent waiting for information injects, set circumstances, triggers and qualifying actions before implementing a plan that is known to be in existence and its results determined by the measure of its application. Crisis leadership is the true virtue of theImplementer. By proactively assessing events and mobilizing resources and the means in which to act before the situation demands, reduces the timeline of impact and in most cases reduces the overall affect the event/s may have on an
organization and its personnel. It is often a far more cost effective application of resources also.

In the modern and developing business world there is simply more information and access to information than ever before. While this has lead to many efficiencies and advancements it has not advanced the capacity or effectiveness of crisis management elements at a comparable rate. If this were the case we would incur little to no crisis events and very incidents affecting organization and their personnel would ever need be reported in the media. Effective crisis leadership is learned by training and exposure with sufficient support services and resources. The critical time in which to apply this talent however remains the same, the Golden Hour and the first 24 hours. No amount of preparation and weighty plans will resolve undesirable events in the advanced stages as a direct result of poor leadership and management in the primary phases. It is therefore of paramount importance adequate depth, training and resourcing be focused on this pivotal stage.

Read this article on the website Click Here
Japanese Nuclear Crisis: lessons for risk managers

Posted by Steven Minsky on April 1, 2011

The nuclear crisis still unfolding at Fukushima Daiichi continues to threaten a meltdown as core temperatures and radiation leaks continue to fluctuate. The disaster is one of the worst nuclear disasters in history. However the vulnerabilities at the power station are not isolated to Japan or utility companies; they are common risk management shortcomings in operational practices seen in every country and every industry. Here are a few lessons for managers from this crisis.

Link controls to the assets they depend on.

Managers’ often make the mistake of assessing the effectiveness of a single control without expanding the scope of assessment to the assets that control depends on.

For example, the Fukushima plant had multiple backup cooling systems to prevent a core meltdown. However they all depended on a single diesel generator and battery backup system. When the system was discovered to be damaged, battery backup was depleted within hours and the cooling systems were rendered useless.

Managers will have better business results by expanding the scope of risk analysis beyond a control to the systems and assets it depends.

Evaluate risk impact for each business process.

It’s very typical for managers to over-invest in risk controls for one area while leaving other areas widely vulnerable. This over-focus on a single area stems from risk analysis ending at the business unit level without considering how each business process will be impacted.
Going back to the plant at Fukushima, while extreme attention had been paid to containing a potential reactor meltdown, the same level of attention was not invested to protect spent fuel. This under-investment in controls for spent fuel pools has lead to highly unstable conditions including radiation leaks and a potential meltdown outside the main containment vessel.

Managers at the business process level have the best knowledge to identify and evaluate the possible impact of a risk. At Fukushima Daiichi that means managers would assess the impact of a natural disaster on for each business process managing fuel storage, cooling systems, backup generators, all the way down to employee performance; not just the impact on reactors.

According to the RIMS State of ERM Report 98% of organization’s fail to assess risk at the front-line. This is a widespread problem for risk management programs in every sector.

**Routinely revisit risk assumptions to reveal emerging risks.**

While executives recognize the business environment is constantly changing, the State of ERM Report shows 86% of business continuity plans are based on outdated assumptions. This leads to outdated controls whose effectiveness may no longer be valid in the current environment.

For the Japanese nuclear plant this means assessing the increased probability of natural disaster stemming from global climate change and updating models based on the latest geological information. Managers need to regularly revisit risk assumptions to prevent controls from becoming outdated.

**Evaluate risk from vendor relationships.**

Every organization depends on partners to maintain key equipment and provide key services under emergency situations. Yet, according to the RIMS report, 96% of organizations today do not cover risks from their vendor partners adequately.

Examples are everywhere, whether you look at the BP disaster and it’s outsourced oil rig from Deepwater Horizon or the
Japanese nuclear crisis stemming from vulnerabilities in the original GE reactor design.

Managers must evaluate how vendor relationships impact every area of operations and what essential processes may depend on these relationships. While a process or a technology may be outsourced to a vendor, you ultimately own the risk.

Risk management isn’t about trying to predict the future, it’s about being prepared in the right places where it matters most. These practices reveal the relationships between risks and activities within processes, and allow managers to spend less time fixing preventable problems and more time reaching their strategic goals.

Read this article on the website Click Here
A company was fined a heavy penalty the other day for a workplace accident that was caused by the company managers condoning illegal actions, because that is the "way we have always done it in the past".

In this case an unlicensed driver of a forklift caused an accident. The company decided to plead guilty being negligent in terms of the Occupational Health & Safety Act, expecting a thousand rand (ZAR) fine, but the court decided a fine of R10000 would be more appropriate. The judge's words: "Do not think you can just come in here and walk away with a small fine and continue the practice. This fine will help you to take Health and Safety issues seriously".

What if the accident resulted in a death and the company had no proper safety practices in place? According to the law the CEO could then be held negligent, and he could receive a sentence of two years in jail and a fine of R100000. With that the media would have a field day! Luckily in this case, no media reporter picked up the case, so the damages were confined to R 10000, but what if they did?

Organizations have two kinds of visibility to deal with: The first is planned visibility, which is caused by day-to-day operations and actions by your organization. The second is unplanned visibility, which is caused by the vulnerabilities you face due to the very nature of your business.

These threats are caused by employees, environmental threats, safety issues and government intervention due to a company's noncompliance to a changing legal environment, and unplanned visibility often does more harm, because of its editorial value.
In this case the company caused problems for itself by not taking the law seriously. In South Africa laws are changing "thick and fast". Keeping up with all the new legal developments is difficult. Maintaining compliance is even more challenging.

Fortunately, employers can take practical, proactive steps to maintain compliance and reduce liability risks.

Here's a list of some of the steps you can take:

- Take appropriate measures to ensure that you receive timely notice of new legal developments, and that someone be instructed to evaluate its potential impact. Often in companies this is the job of the company secretary to evaluate the potential impact of for instance internet legislation and the HR department to evaluate Employee Equity legislation on company policies.

- Take note of internal developments and their impact on the company's legal obligations. Re-engineering efforts, and business expansions can have an impact on employee legislative matters.

- Conduct periodic reviews, especially of employment policies, practices and procedures. Do it on a regular basis.

The old latin maxim : "Ignorance of the law is no excuse" applies here. What is often ignored though is the reputational impact of business decisions taken. Taking a minimum legal compliance approach in your business may not be enough to avoid potential litigation and the ensuing publicity that could accompany it.

Noncompliance with changing laws can damage your reputation. How compliant are you? When last have your company conducted a reputational audit?

A Reputational audit is a systematic way of approach to identifying issues that currently affect your company or will affect it within the next 12 to 36 months. (Like it or not, your company's policies and actions are shaped and developed in anticipation of, and reaction to, political, economic, legal, social and technological forces).
Are Your Company at Risk of Damaging its Reputation due to Noncompliance?

It is also a process of casting a look internally and examining processes, procedures, policies and issues that could impact and damage the company's reputation. It involves an in depth look at the quality of management, financial soundness, use of corporate assets, community and environmental responsibility, quality of products or services, value as a long term investment, innovativeness, and the ability to attract, develop and keep talented people, etc.

Read this article on the website Click Here
In the automotive dealership space I have seen acquisitions turn into legal tribulations when after a deal is closed personnel related non-compliance issues pop-up creating huge, multi-million dollar headaches literally days after deal close.

What was found was a fundamental disregard for the human element in the valuation of a business...what have the people been up to that reinforces the business processes that helped make the business successful as well as what they have been doing on their own when no one is looking...

The due diligence process should disclose and uncover items that have a material impact on the valuation of the business. The experience above suggests that uncovering personnel related liabilities should run hand in glove with the business' valuation process...But how does an acquiring company evaluate the causes of liabilities that can adversely affect the acquired business? How indeed...

In the auto dealership space, traditional due diligence is about reviewing the books, assessing the local market attributes, following IRS Revenue Ruling 59-60, using the “comps” in the local market as well as reviewing the fun and unique OEM franchise requirements of a dealership where factory site control, image compliance or exclusivity can have material impacts in property valuation, financing flexibility, and exit...

In ADDITION, you are also buying the processes and people who make up the culture, good or bad, that helped that dealership make money over the years. How do you gauge the type and extent and importance of internal processes that build value for the dealership in question?

Comprehensive due diligence is about knowing the culture you are buying. Is the business a stickler for compliance details? Are
the people and processes in place designed to protect your investment from hungry lawyers and misguided investigators?

If your valuation consultant did the right things and you find something “not quite right,” it is obvious the risks are higher than those assessed when you could smell the new revenue stream based off the “Rules of Thumb” your consultant relied upon to get you here.

So visibility into personnel related compliance issues provides you the opportunity to offer a lower price that reflects not only the generally accurate valuation “Rules of Thumb” but also those personnel based policies and procedures that can land you in a closed room with lawyers mumbling secret somethings in their client’s ears.

Ultimately, those personnel-related risks you uncover will impact not only what is paid for a business, but how well you can expect the business to perform after the acquisition. After all is said and done, compliance with regulations and mandates, compliance with strategic partners requirements and compliance with those proprietary business processes unique to your organization all combine to support and expand your competitive advantage, which is the harbinger of valuation.

Read this article on the website Click Here
Definitions create the lenses through which we look at the world. The renowned psychologist, Abraham Maslow said that if the only thing you have is a hammer, you tend to treat everything as a nail.

I start every seminar and presentation with definitions, so that I can establish a common framework through which I can work with my audience. In particular there are a number of definitions to describe reputation and reputation risk, each serving a slightly different purpose.

These need to be further explored so that you can decide on how you will manage reputation.

The classic definition is that Reputation is all that is generally believed about your character, respectability, credit, integrity or notoriety. (Latin: reputatio – reckoning). But it is not enough to guide us.

I also use these definitions that give it more meaning:

Reputation is a state of mind – A Set of memories, perceptions and opinions that sits in your stakeholders’ consciousness.

Reputation is the net result of the interactions of all the experiences, impressions, beliefs, feelings and knowledge all stakeholders have about a company.

So what then is Reputation Management?

It is essentially a consulting discipline that realizes that Reputation is both an asset and a risk. The definition that I therefore like to work with says that Reputation Management is the building, sustaining, and protection of an organization’s good name, generating positive feedback from stakeholders and resulting in the attainment of strategic and financial objectives. It implies that there is a definite financial link between the work we do in reputation management and the bottom line.
However reputation is also the greatest risk that an organization can face. (Think of a run on a bank). As Warren Buffet have said: “It can take twenty years to build a good reputation, and only five minutes to destroy it”.

WE therefore have to consider the following definitions as part of our approach to building and protecting reputation.

**Definition 1: (Stakeholder Perspective)** - Reputational Risk emerges when the reasonable expectations of stakeholders about an organization’s performance and behavior are not met. This has been listed in some surveys as the most dangerous reputation risk of all. It essentially involves taking a look at each stakeholders needs and expectations, matching the drivers of an organization reputation and minimizing the gaps that exist.

**Definition 2: (Asset Perspective)** - Some studies show that Reputation makes up between 55 – 73% of a company’s asset value. In this instance, Reputational Risk is defined as the loss of earnings that occur in a situation of negative public opinion. It normally results in loss of sales, share value decreases and breakdown of relationships. Many a crises have led to stock price decreases and impact in other areas of the business.

**Definition 3: (Incident Perspective)** - Reputational Risk is the exposure incurred from unexpected incidents, or from unanticipated response to the institution's initiatives, actions or day-to-day activities. This definition implies that Reputation Risk is the risk that an activity, action or stance performed or taken by a company or its officials will impair its image in the community and/or the long-term trust placed in the organization by its stakeholders, resulting in the loss of business and/or legal action, and is closely linked with the asset perspective.

**Definition 4: (Compliance Perspective)** - Reputational Risk can also be defined and viewed as the loss or negative publicity that can arise from failure to meet regulatory or legal obligations.

From the above definitions it must be clear that essentially all risks and all related components of an organization potentially impact on reputation. This implies that reputation needs to be
systemically managed if an organization wants to extract maximum value from it.

Tip – It is essential that you define Reputation Risk in these four ways in your business, as each definition implies a different mitigation strategy and potential danger.

My question to you - Have you adequately defined Reputation Risk in your Business? Do you have a Reputation Risk framework that spells out how you will mitigate, treat and respond to Reputation Risk? If you don't, you have some work to do.

Read this article on the website Click Here
Getting Real About Reputation Risk

Why should organizations be concerned about Reputation Risk?

As the world become more and more networked, more and more companies are exposed to a changing set of vulnerabilities. The landscape of risk has changed. No longer can any country or organization ignore the happenings of 911, Bali and London.

In this new world, incidents can damage a good reputation purely because an organization can take too long to act decisively with problems. For instance a reputation damaging incident can become international news in a matter of seconds and destroy relationships and brand value in other countries where the incident did not even take place.

The figures and surveys are there to support the need for sensitivity about reputation. Reputation has been rated as the number one risk in Economist magazine and more than four other international surveys. It was even mentioned at Davos.

To minimize reputation risk – the way a company is viewed by its stakeholders, companies need to take a total view of the company - from operations and behaviors to policies and objectives - so that methods of securing and protecting the business can be worked out.

A very broad view of the risks faced also needs to be established: a disaster could do a lot of damage to the business, but so could a small issue that perhaps are seen to be trivial by the organization but seen as material by stakeholders.

A simple example shows the difference between normal risks and reputation related risks. Assume that the directors of a very large public company consistently incur, and do not pay personally, parking fines for their company cars. The primary risk to the company, in this case of financial loss, is probably very small in relation to its annual turnover. Accountants and auditors would say that these amounts are not material, should not be
separately disclosed in the annual report and should be ‘lost’ in general expenses. **But what would the public think of this behavior by corporate leaders?**

How would the media report it if it came to light? Indeed, what general signals of corporate trustworthiness would this give?

Herein lays the secondary or reputational risk for the organization. **Reputation has turned the concept of materiality upside down; financially immaterial events may have huge potential significance for the organization.** The management of such risks demands attention to the deepest operating assumptions of organizations. Paying attention to the things that can impact on reputation makes good business sense.

Viewed strategically, the management of perceptions offers organizations real advantages, enabling them to become more sensitive and more efficient, while also reducing the risk of failure at times of change and transformation. It is not just about enterprise wide risk management, governance or ethics, it is about understanding the perceptions, opinions and expectations that stakeholders may have.

To create a robust reputation protection framework will necessitate a holistic view of the organization. This is why using a third party can be particularly beneficial. Because they are so familiar with their own businesses, organizations can make assumptions which outside consultants will question. Consultants will look at a company from the top down and are able to bridge all the information and operational silos that a typical organization's structure generally creates. For example, management may believe that reputation can be managed by a Public Relations or Communication department. Yet the reality is that crisis do not hit in a departmental silo but impacts across boundaries.

If a company wants to protect its reputation it will need to identify those smoldering crises – the unknowns that can cause unwanted publicity and destruction long before it appears or is mentioned in a blog, on a website or in mainstream media.
Part of this reputation risk assurance framework is something called a crisis management and crisis communication response plan. Today’s knowledge market economy expects a company to react quickly and with finesse when there is a crisis of any kind. Yet many companies have never tried and tested their planned response. To complicate matters even further companies have a myriad of fragmented plans ranging from disaster recovery and emergency response to business continuity with little integration in place.

A CSO Magazine survey on business continuity in the US a few years ago showed that, while an overwhelming majority (93 per cent) of US companies had a business continuity plan in place, only 37 per cent had tested it in a real life situation. In today's world, this is no longer acceptable.

In the past three years I have had more than 350 national government and listed organizations attend my Crisis management & Communication response workshops here in South Africa. The rate for organizations that have tried and tested their plans must average out at about the 20% mark.

Delegates cite all sorts of issues:

- **Time Management.** Other priorities are more important. Unfortunately once a company has a bad name its brand can be destroyed forever.

- **We will handle it when it comes as we have a strong management team.** Sure, but we all know that different people react differently under stress. So do management teams, and many times teams become defensive when they should be open (See my Powerlines newsletter for my article on the Johari window application to organizational communication)

- **We are in the process of allocating resources.** Most companies do not even comply with the law in terms of fire drills. When a crisis strikes, companies need to be ready. The aftermath of a major incident is not the time to establish whether crisis management plans work or not. Very strict and precise information is needed, such as fast recovery check lists that make sure people know exactly what to do when disaster strikes. Look at the actions of a paramedic – he or she do not hesitate they act. Plans have to be well
coordinated and rehearsed until they become normal response. When a crisis strike there will be realities and perceptions to deal with. It's well known that even the most meticulously planned new systems and procedures do not survive their first exposure to reality intact, and the management of crisis is no exception.

To protect your company’s reputation you need to constantly think what will affect stakeholder’s perceptions. It means factoring reputation into decision making, to constantly talk about it and constantly try to impact upon it.

Read this article on the website Click Here
Can you Risk your reputation?

Posted by Nagesh Bharadwaj on October 22, 2010

Executive Summary:

Sometimes your reputation in the industry is everything for you. Reputation is sacrosanct and hence any risk to the reputation of the company is considered high.

I worked at Sony for many years. For a company such as Sony, the brand reputation is sacrosanct. Which means any incident or event which will bring bad name to the company will be considered a “high” risk event. This is much more accentuated because the company is Japanese.

For example a pharma company makes a mistake with its formulations or it gets contaminated, then it has very high risk of reputation. This is due to the nature of the product, where lives can be at stake, the consumer will not again buy their product due to lack of trust. Add to this, any liabilities they have to pay for damages and also regulatory punishments. On the other hand a company making toilet bowls may have lesser reputation risk when compared to the pharma company. Parryware will have to fix the batch of products and perhaps recall the faulty batch and not have worry of loss of life due to non performance.

The degree of reputation risk is also a cultural phenomenon where some societies attaching a huge importance to it. “Loss of face” is considered a huge loss for Japanese where it may be taken lightly in other cultures.

Sometimes mistakes do happen and how do you handle when mistakes happen at large companies and large brands?

Have a look at Johnson&Johnson (J&J) on how they handled a handled a significant crisis. In 1982 J&Js Tylenol medication
commanded a market share of 35 percent and it accounted for 15 percent of company profits. A pretty huge number for one product and for J&J which has several products.

In 1986, a individual managed to lace J&Js tylenol with cyanide and about 7 people were killed after consumption. Word got out that it is due J&Js tylenol. Even though J&J was not directly responsible for the deaths it was coping most of the blame.

Hearing the news, the stock market responded and the market cap of the company fell by about 1 billion dollars. In the same situation other companies may have responded pretty defensively. But not J&J.

J&J bit the bullet and took the sour pill (pardon the pun). It ordered *all* the Tylenol medicines off the shell. This is not only in the state affected but all the states in the US. It went to destroy all these medicines with a huge loss to the company. Also it went to prevent future incidents by designing a tamper proof medicine dispenser. By these actions it became a champion of customer cause.

The good will resulted in J&J capturing back 70 percent of market share loss pretty immediately. It was reported that many customers converted to J&J tylenol who were using other pain killers.

Now this case has become a shining piece of crisis management for other companies to benchmark.

What value do you put for reputation at your company ? Can you put a number on it ? How would you go about determining a number ? How would you respond to significant crisis ? Do you have a plan.

Appreciate your comments.

Read this article on the website [Click Here](#)
I read the recent news that Mahindra Satyam (previously known as Satyam Computers) declared its financial results after two years of working at the previous fraudulent statements and restating the same. You might recall, the fraud was alleged to be perpetuated by the previous owner Ramlinga Raju the then Chairman of the organization for an amount of Rs 7000 crore (Rs 70,000 million) or more. The CFO and External Auditor (PWC) are considered accomplices in the fraud. The new owners made a statement that the fraud may have originated as early as 1994, and the auditors were not doing their statement.

It got me thinking that since the fraudulent representation of financial statements continued for so many years, it is highly unlikely that qualified and highly trained chartered accountants were unable to identify these transactions. In this kind of a scenario where the Chairman is involved in the fraud and has so much of political and financial clout would a mere employee be in a position to whistle blow?

The whistle blower is expected to highlight to the audit committee or external legal authorities about the irregularities, fraudulent and unethical practices being adopted by the organization. The expectation is that the whistle blower will have the moral courage and character to go against the senior management of the organization for the greater good of the company and society. In the legal spirit the requirement definitely is justified.

In recent years the challenges mentioned on failure of whistle blowing procedures is that there is no protection against retaliation, socially the individual is ostracized and professionally the individual does not get another job thereby simply reaching a dead end in their careers. However, I think we are unable to see the forest from the trees.

My concern is that the basic premise of whistle blowing – “a person having a moral character to go against authority figures” -
is something to be questioned. I am bringing here the various psychological studies conducted which prove that normally a person will not undertake a whistle blowing activity. The percentages of human beings who will have this level of moral development are insignificant.

**Milligram Experiment**

In the Milligram experiment it has been proved that people comply with authority figures instructions without coercion to the point of causing another unknown innocent individual’s death. It clearly indicates that ordinary people simply doing their job can participate in tremendously destructive activities which are against their personal value system because they are temperamentally geared towards complying with authority.

Extract from Wikipedia on Milligram Experiment - “The Milligram Study indicated that intelligent individuals who thought they were administrating deadly electric shocks onto a subject, continued to administer perceived deadly shocks at the prompting of an authority figure. There was no violent coercion in this experiment. However, the presence of a person who was perceived to be in authority was sufficient for most test subjects to continue administering perceived deadly electric shocks. The test subjects first questioned the viability of the experiment only when the shocks were of 135 volts. In Millgram’s first set of experiments, 65 percent (26 of 40) of experiment participants administered the experiment's final massive 450-volt shock, though many were very uncomfortable doing so; at some point, every participant paused and questioned the experiment, some said they would refund the money they were paid for participating in the experiment. Only one participant steadfastly refused to administer shocks below the 300-volt level”

**Kohlberg’s Stages of Moral Development**

Lawrence Kohlberg, in his 1958 dissertation, established the pre-conventional, conventional and post conventional stages of moral development. In my opinion, in the present materialistic society, most of us are in pre-conventional and conventional stages of moral development. The egoistical pride which we have for
professional and financial success even if it requires bending the rules for personal gain indicates a lack of moral consciousness. Altruism and social consciousness are attributes which are not held in high regard by the society in general. Intrinsically, the assumption of whistle blowing that employee will sacrifice their self interest for the greater good of the society is questionable.

Below is an Extract of Kohlberg’s theory from a report on Organ-Cultural Deviance: Socialized Deviance in Corporate America (Authors: Christie Husted, PhD and Renée Elaine Gendron, MA) which clearly indicates that the present day attitudes and attributes are of pre-conventional stage.

“In Kohlberg’s pre-conventional stage, individuals see morality as being external to them. Kohlberg found these individuals have a sense of right and wrong; believe in reciprocal relationships, and view relationships as a means of exchanging favors, lack identification with family and societal value. What is seen as being right to an individual is what satisfies the individual’s self-interest. Thus, the individual’s desire to satisfy their needs is egoistic. In this stage, the individual is looking to satisfy their need for belongingness, safety, security and esteem through their association with the group. The group reinforces their ego, supports, justifies and encourages the individual’s behavior and provides them anonymity.

The next stage of Moral Development, the conventional stage, individuals see morality as living up to the expectations of family and community. There is a shift from unquestioning obedience to a relativistic outlook and to a concern for good motives. The individual attempts to understand the feelings and needs of others. There is a concerted effort to help others (Crain, 1985). The individual becomes altruistic.

In the last stage, the post conventional stage, individuals are attempting to determine what a society should be like. They are working toward a concept of “good society”. Kohlberg found these individuals believe just decisions can be reached by looking at a situation through one another's eyes. However, Kohlberg admitted the highest stage of post conventional development is
Kohlberg found very few individuals attain this high level of moral development”

Even while studying the six stages of Heinz dilemma: Obedience, Self-interest, Conformity, Law-and-order, Human rights and Universal human ethics, there would be very few who would respond according to stage 5 and 6. Although, we consider crime as a relation to opportunity, rewards and rationalization, if the moral development has not taken place rationalization for participation in any crime would be without any conscious dilemmas. This indicates that employees as such do not need to be coerced into illegality, and the reward of being in a favorable position with the boss would be sufficient to actively participate in illegal activities.

In the book “Moral responsibility of the holocaust- A study of ethics of character” written by David H. Jones, he has analyzed that – “while genocide is obviously immoral how people were able to actively participate in mass slaughter with seemingly a clear conscience.” He has explained the fact how humans escape individual moral responsibility by participating in group consciousness and collective thinking. If the social structure sanctions mass slaughter, the group thinking will become so. He has mentioned less than 10% Germans helped Jews although without coming forward and doing it behind the back of Nazis.

Considering the above case and the psychological studies, are we setting unrealistic expectations from employees to whistle blow and come forward to protect the society. The above studies results show that on an average less than 10% of the human population has moral development to put social needs over self and be altruistic enough to look at the greater good of humanity.

In such a situation what is the possibility of whistle blowing becoming a successful tool for identifying corporate wrong doing? Is this not just a theoretical concept with minimal practical viability? Should we be considering the psychological angle of the law to determine whether it can be effective in the long run?

Please do share your thoughts. I would like to invite you to visit my blog Sonia Jaspal’s RiskBoard
Read this article on the website Click Here (some good comments there)
Insulating your organization against reputation risk

Posted by Deon Binneman on May 3, 2011

The word "insulation" means to protect. This article is will be valuable for any Reputation manager, PR professional, Risk manager and Corporate Affairs executive.

Numerous studies including the Corporate Risk Barometer survey conducted by the Economist Intelligence Unit a few years ago; have shown that the most significant issues facing business today are; reputation risk (defined as the threat of any event that can damage a company's reputation) and regulatory risk (defined as problems caused by new or existing regulations).

These two risk categories received the highest scores in the Risk Barometer, indicating that they are seen as more significant issues than market risk, foreign exchange risk and country risk by the majority of executives in the survey.

Why should organisations protect themselves against Reputation Risk? Unfortunately many companies damage their carefully crafted reputations either inadvertently or through blatant and incredulous acts. Most of the damage occurs when there is not a clearly defined strategy for building, sustaining and protecting the organisation's biggest risk and asset - its reputation.

The new order of the day seems to be accounting principle restructuring, companies seeking to improve trust building, governance and ethics principles and practices, stakeholders seeking disclosure and shareholders becoming more and more frustrated. Yet, there still seems to be a general lack of understanding the true value and potential of an organisation’s reputation. And, as long as management do not understand how reputational risk manifests; negative articles and doubt about company practices will continue to dominate headlines.

Unwanted actions and negative publicity leads to reputation risk. And reputation risk manifests when perceptions and opinions are influenced by negative experiences, impressions, beliefs, feelings
and knowledge that stakeholders have about a company. It often results in loss of sales, share value decreases and breakdown of relationships.

Companies should be asking themselves about what actions they are taking to protect and insure their good name against all types of crisis – especially those that are sudden, smouldering and perceptual!

More and more companies are finding that their once hidden “smouldering crises” are now becoming fully-fledged combustible crises. (A smouldering crisis is any serious business problem which is not generally known within or without the organisation, which may generate negative news coverage if or when it goes “public” and could result in fines, penalties, unbudgeted expenses or unwanted scrutiny).

The damage of a reputational crisis can be direct and indirect. These costs could include penalties incurred because of a lack of legal compliance, litigation, media conferences and advertising costs and the hiring of crises communication consultants to put forward positive messages after wrongful deeds. BUT what about the indirect costs, the effects on various stakeholders? The customers that do not return or stakeholders that takes their business interests elsewhere?

I believe that managers have both a professional and a moral duty to try to protect their company’s reputation. The way to minimise their company’s reputational risk is to be vigilant and report anything, which they believe, could erupt into an issue of unwanted publicity and therefore act to rectify it. But they can only do that if they understand what reputation is all about and how it can be managed and damaged. (The importance of the what, why & how of Reputation Risk Root Cause Analysis is one of the topics that I discuss in my Reputation Risk class).

The best way to address these concerns is through the development of a best practice strategy for the organization that should address these typical questions:

- What kinds of proactive steps should companies take to augment their reputations?
- What aspects of reputation risk are unmanageable?
- Who are the key players in managing a company's reputation?
- How should a company's organization reflect its interest in preserving and enhancing its position?
- What level of risk assessment is expected and how should companies approach this task?
- How can a company identify key risks, analyze their root causes, and take proactive steps to preserve the corporate reputation?
- How can a company's regular risk assessment process help to point out particularly critical areas that could affect reputation?
- The next postputs forth further thoughts on best practice.

Read this article on the website Click Here
Cloudy issues: Can we reconcile efficiency and security?

Posted by Michael C. Thomsett on August 8, 2011

With cloud computing coming into the mainstream rapidly, the old argument has arisen once again: Do we want (fast) efficiency or (slow) security?

The big advance in the near future will be development of cloud computing technology that offers both. The combination of data efficiency and data security should be possible: Unlimited storage, easy retrieval, lightning fast processing, and ironclad security, all in one package.

This topic will not be taken seriously by many, and risk managers who are aware of this problem will continue to be frustrated by management's tendency to ignore very real risks, even to not take them seriously. Sadly, once again these risks will not be addressed by the majority until a major breach occurs and data is compromised or stolen. But it could be severe: the loss of sensitive customer and market data, exposure of sensitive trade secrets, and loss of reputation among customers, all pose very real threats unless we can operate in a secure environment.

This is not to say security does not exist. However, with all of the advertisement about the cloud we see these days, how do we know it really is secure? If your cloud provider sub-contracts its services to another, how do you know the secondary provider is as secure as the primary? This is a huge issue, too.

There is much to be discovered, worked out, and fixed. Even so, cloud computing may represent as big an evolutionary change as the Internet was not all that long ago.

This discussion is the subject of my newly published article, "Risks Related to Improved Data Efficiency and Technology," in the Journal of Information Systems Technology & Planning (JISTP), Volume 4, Issue 9.

Read this article on the website Click Here
Reputation Risk: Beyond Solution Provider Hype and Now a Core Enterprise Risk?

Posted by John Farrell on March 5, 2012

The use of the term “reputation risk” fits the pattern of hyped buzzwords, but the significant volume of money now spent managing corporate reputation risks proves it is more than hype. Reputation dynamics are forcing pivotal business decisions. Penn State increased its acceptance rate to offset a decline in out-of-state applications and an expected drop in the matriculation rate. Deutsche Bank’s CEO Josef Ackerman refused 3-year loans from the European Central Bank concerned it would damage the bank’s reputation with customers. While risk managers generally view reputation as a consequence or a secondary risk relative to other risks, is it taking a more central position in enterprise risk management programs and corporate decision making?

The digitized Google Books database reveals authors have addressed business reputation since the 1830s, but the term “reputation risk” first appeared in 1988 and its use quickly accelerated. From 2003 through 2011, Factiva’s database shows the terms “reputation risk” and “corporate reputation” in print and online news publications expanded at a compounded annual growth rate of 13%. My skepticism as an industry analyst heightens when terms are hyped to this extent, but the match of supply and demand in this case seems to justify reputation as a vital category in any risk market taxonomy.

On the supply side, hundreds of public relations firms, crisis consultants, and business consultants promise to help corporations manage, protect, and recover their reputations. Social media launched another set of suppliers with online reputation software vendors and consultants positioned to help monitor and manage reputation in the cyber world.

On the demand side, executive perception of reputation risk is evolving quickly. Here are some stats:

- A 2005 EIU survey showed 52% of senior risk managers believed reputation deserved to be a category of corporate risk on its own
with severity far surpassing natural disasters, regulatory, human capital, information technology, and market risks.

- The 950 worldwide business executives participating in a 2007 Weber Shandwick survey considered 63% of their company’s market value on average to be attributable to reputation.

- A 2011 Zurich-sponsored HBR study indicated 50% of the 1,419 business executives surveyed identified corporate brand reputation as a risk that has risen most significantly in the past 3 years.

- The 2011 EisnerAmper Board of Directors Survey revealed, after financial risks, reputational risks is the top concern for U.S. boards with 69% of the 142 respondents noting it as most important.

- Steel City Re highlights 30% of the S&P500 members identified reputation risk as material to their enterprise value in their 2010 10K report. In 2011, this percentage rose to 57%.

Does the rhetoric on both the supply and demand sides constitute a market? I’ll complete full research of total spending on risk reputation products and services at a later date, but initial analysis indicates it crosses my threshold of $5 billion to define a sustainable market segment.

Insurance companies have taken notice. Phil Ellis, chief executive of Willis’ Global Solutions Consulting Group, observes 95% of major corporations suffered at least one major reputational crisis in the last 20 years, but less than 10% of these were insurable. Ellis notes the insurance industry needs innovative products to meet this challenge.

Three companies launched such products in October. Aon’s reputational risk product, underwritten by Zurich Financial Services, provides up to $100 million in limits of coverage triggered by 19 named perils combined with financial loss and adverse publicity. Willis rejected the peril-based criteria and is developing products by industry sector starting with Hotel Reputation Protection. Chartis is taking a more general stand-alone, no named peril approach with Chartis ReputationGuard. One common element to the offerings is access to leading global public relations firms for both preventative work and crisis
support (cue the race for every PR firm to align with an insurance provider as their very own sales channel).

As a market analyst, I have to recognize, albeit with some reluctance, that demand and supply side factors justify defining reputation risk as a major risk category. Is this elevation of reputation risk justified in the eyes of risk managers and risk consultants? Is your crisis response plan the primary vehicle for managing your reputation risks or do you manage reputation proactively as a core integrated risk in your ERM program to support corporate decision making? What makes one company ignore reputation risks while another invests in extensive reputation monitoring and purchases multi-million dollar reputation insurance coverage?

Read this article on the website Click Here
Most of today’s organizations feel that if they have a “Risk department”, an “Internal Audit Team” and a “strong Legal team “they are safe against everything but is it the case. I say No, having a resource team strong in their defined skill set is only one aspect of an equation and the remaining aspect is time, budget and coordination between the 3 (Risk Management Group, Internal audit team & Legal team) because Governance, Risk Management & Compliance do not act in silos, they are very much interdependent on each other.

Before we proceed let’s have a look what GRC stands for:

Governance: Continuous Monitoring of decisions based on which an organization is trying to achieve its vision (Long term) and Goals (Short term objectives).

Compliance: Identification & adherence to set of risks described as policies & guidelines by a regulatory body, whose sole purpose is to ensure the peoples, interest (Tangible & Intangible) in an organization for ex: SOx, HIPPA, NERC, FERC etc.

Risk Management: An approach to manage a known risk (Governance (Decisions)/ Compliance (Risk associated with non compliance of compliance)) by limiting or reducing the impact/likelihood of a Risk. Risk is the common factor which correlates Governance, Risk Management & Compliance.

How & Why Risk is a common linking factor?

1. Governance means smooth functioning, Organic growth (clean account books), employee, customer & shareholder’s satisfaction to be achieved through calculated Risks and through timely response to the market.
2. Compliance is: Identification & adherence to set of risks described as policies & guidelines by a regulatory body, whose sole purpose is to ensure the peoples, interest (Tangible & Intangible) in an organization. However, not likely the case in Enron, world Tell and for Tyco electronics. In plain simple terms “Governance” failed in all the 3 examples.

But before we proceed lets understand what RISK stands for:

Risk is a deviation from a desired / calculated output when an input with respect to a process/ function is executed or “Effect of uncertainty on an objective “.

As per COSO framework risk can be broadly classified into 4 different categories for an organization:

1. Strategic Risk: Risk with respect to Vision/ Goal of an organization
2. Operational Risk: Risk associated with execution of the strategy outlined as the Vision /Goal for an organization
3. Financial Risk: Risk associated with finances to achieve the vision/ Goal of the Organization
4. Legal Risk: Risk pertaining to regulation, compliances, law suits for an organization

Basically all kind of risks can be broken and segregated into these 4 categories and an operational plan can be devised to mitigate the same but if COSO framework is so simple then why do we need 3 different teams to handle “GRC”.

Lets again take a deep dive on how” Risk Mitigation” can be done:

1. Inherent Risk: Every process/ function has a certain amount of risk associated with it for example: Driving a car; the biggest risk is “Accidents on Road”. I can kill someone or can get killed by someone but either way I am not going to stop driving.
2. Control/ Mitigants: When a control/ Mitigants is applied on a risk, deviation from the desired output can be contained to a certain extent. In our driving example Mitigants can be your Air bags, ABS systems and etc technologies to save a human life even after the impact.

3. Residual Risk: Risk which is been controlled significantly but the deviation in the output is still there for example: we may not lose a human life in an accident any more but we still can’t rule out any significant damage to human body.

Risk Handling Approaches:

1. Risk Avoidance: How can we avoid a risk? by not getting involved in it or by withdrawing from it

2. Risk Sharing: Remember the old time, when we used to be in school, Homework not done afraid of teacher scolding and then a complaint to parents and remember the geeky but business oriented boy/girl who is willing to do your work but with a cost.

3. Risk Acceptance: The bold and a smartest way to handle a risk is by acknowledging it and formulating a plan (Time, Money & Resources ) on how to handle it. But the most important question is how to be aware of risk which has a capacity to affect my business, organization, and my day to day operations:

Honestly, there is no sure way where you can get an update about new possible risks but even if we are aware about an event that has a high probability and impact. What actions to be taken under these circumstances: 7 Strep Approach towards an event which can possibly affect your business

1. Identification: Identify all the possible risks which are associated (direct and indirect) with an event

2. Assessment: Assess the identified risk based on Impact and the likelihood of occurring
3. Prioritizing Risks: Prioritize a risk based on its impact and likelihood

4. Formulating plan: Device a plan and work accordingly

5. Ownership: Train your employees and let them know what they are supposed to do in a crisis

6. Training: Train them periodically, so that they don’t get complacent or panic in a situation

7. Update: Any event which is by far not recorded or covered in any sort of risk mitigation program should be stored and recorded and steps 2 to 7 should be repeated for it

The fundamental of GRC is risk and risk is associated with almost every function/ process or business unit which runs an organization. So our focus should be more on risks and we should channelize all our resources in this direction.

Read this article on the website Click Here
Is your GRC program overly focused on compliance?

Posted by Steven Minsky on March 29, 2011

No company falls out of compliance over-night. It’s a gradual process resulting from a combination of overlooked issues, that together create a serious problem. Strangely enough, compliance issues often result from taking an overly compliance-focused approach to risk management; a common problem for Governance, Risk, and Compliance (GRC) programs.

Take for example J&J who, after a series of product recalls in 2009, has once again fallen out of compliance and now faces a permanent FDA injunction shutting down at least one plant and requiring at least five years of severe FDA oversight. So what went wrong?

While J&J undoubtedly took the 2009 recalls seriously, they focused on correcting compliance issues rather than digging down to the root causes of those problems and correcting them at the source. The result? Manufacturing plants are once again out of compliance just two years later and the public’s trust in J&J products is beginning to wane.

Focusing on compliance is akin to adding another bilge pump because your boat has taken on too much water rather than seeking out and repairing the leak. The real solution to a company’s compliance issues is to adopt an integrated approach to risk management; one that can identify risk root causes and their impact enterprise-wide, an approach that focuses on performance management not just meeting compliance goals.

These are the hallmarks of an ERM-approach to risk management. This approach means assessing risks at the operational process level and understanding the consequences of those risks enterprise-wide.

It doesn’t matter whether you sail under the flag of ERM or GRC, the difference is in the approach. Does your organization take an ERM-approach to managing risk?
Visit the **RIMS Risk Maturity Model assessment** and learn more about evaluating your program on one of the seven key attributes that drive ERM performance.

Read this article on the website [Click Here](#)
If you’re considering automating your governance, risk, and compliance (GRC) program there are dozens of choices out there and choosing the one that’s best for your program can be challenging.

While many tools out there can document controls and test compliance, managing enterprise-wide governance, risk, and compliance is about much more. It’s about adding measurable business value and contributing to the achievement of strategic goals.

To help you separate tools that have simply jumped on the buzzword bandwagon from tools that will help you deliver business value, here’s a list of five must have features required to support your GRC or ERM program.

5 Capabilities that will add value to your GRC/ERM program

Is GRC and risk management tied to strategic goals?

Senior management is concerned with where your organization is going. Without a connection between risk and strategic objectives, you’re executive team is unlikely to make risk or compliance initiatives a priority.

Does it directly link activities to business performance?

While it’s good to be in compliance and have some risks covered, your risk and compliance program should be aligned with operational goals. This means using metrics and controls that can actionably improve business performance, not just meet requirements or checking off a box.

Does it drill down to the process level?

Every day your front-line managers are making decisions about risk. Does this software give you transparency into these decisions and will your process-level managers be able to use it?

Is information shared across business silos?
Meeting several compliance standards often requires the collection of similar data. Does this software allow information to be collected once and then be reused across silos and functions to prevent double-work?

**Does it use SMART business metrics?**

S.M.A.R.T. business metrics are built at the process level, around root-causes, are comparable, and are forward looking to give you the most complete picture of your risk and compliance program.

Whether your risk management program flies under the banner of GRC or ERM you need tools that give you transparency into processes and shows relationships across your enterprise.

To learn more about these attributes, take the RIMS Risk Maturity Model Assessment today and see how your program compares to industry best-practices.

Read this article on the website [Click Here](#)
While spreadsheets are still an excellent tool for data manipulation and one-dimensional analysis, they fall significantly short of delivering the capabilities a risk manager really needs to analyze trends and see the relationships the job entails.

The limitations of spreadsheets verses ERM software are systemic and largely stem from the way they manage data, their inability to easily show relationships, and their general inaccessibility.

**Impractical**

Risk management is an iterative process that requires collecting a great deal of information to glean the necessary insights. This often results in dozens of spreadsheets and documents each with multiple versions and revisions.

Not only does this impede the process of combining data into a coherent big picture, it also means any changes to data structure becomes a great undertaking. Dependent on spreadsheets, risk managers will spend countless hours validating data, double-checking formulas, and updating values instead of spending that time on much needed evaluation and mitigation.

**Relationships**

Risk analysis is not a static process; it's dynamic and highly strategic. Assessment structure, information, and the people involved evolve over time as management's requirements and priorities change.

Spreadsheets, however, are ridged. With each change to a spreadsheet, links between information are lost making it very difficult to analyze relationships over time. Without these relationships, how will you link risks and their controls to your organization's strategic goals?

What's worse, spreadsheets can actually limit the depth of risk analysis. You can only analyze the relationships your risk tools
can uncover. Spreadsheets offer limited access to past and current data, you cannot easily aggregate and dissect information, and they require a high level of technical knowledge to compare data over time.

Simply put, spreadsheets prevent an understanding of the dependencies and consequences between departments, processes, and strategic goals. Without these connections it’s impossible to see how multiple risk can come together to create a disaster like the BP oil spill or the Japanese nuclear crisis.

**Inaccessible**

Risk management isn't something that can be done in isolation. The information risk managers collect and analyze needs to be accessible to the rest of the organization. Spreadsheets, however, aren’t accessible to business intelligence software, to management, or to other support functions that could benefit from that data.

The result is a risk management function without support from management and an organization with an abundance of duplicate tests, controls, and information. Risk managers need to be able to aggregate and access information across business silos and multiple levels in order to engage the right people with the right information.

**The Solution**

Risk management requires dynamic tools that can organize and link data automatically, analyze dependencies and consequences enterprise-wide, and be accessed by decision makers and other silos.

The solution is a robust software platform that can organize risk-information all in one place, link the relationships between data, and be accessible to the rest of the organization. Identify duplicate tests and controls, uncover the complex relationships between risks, and make that information accessible to decision-makers with one shared risk management platform.

Read this article on the website [Click Here](#)
Risk Appetite Process and Enterprise Risk Management

Posted by Steven Money on October 11, 2011

Risk Appetite is often addressed as a quantifiable number that is a guide to the nature of risk that a company will undertake. To use the 'appetite' analogy: What is the nature of your diet restrictions and how do you interpret these when ordering your next meal?

In the application of Risk Appetite, the questions become:

- How is Risk Appetite central to business decisions;
- How is Risk Appetite central to business operations; and,
- How does Risk Appetite affect Enterprise Risk Management?

(In other words, how do we easily apply our diet restrictions to any type of restaurant or to any selection of meals that we may be faced with?)

Risk Appetite Definition vs. Risk Appetite Process

A Risk Appetite definition describes our restrictions and Risk Appetite process describes how we successfully apply these restrictions.

Risk Appetite Process

Risk Appetite’s effect is best served beyond its definition to allow us to measure our restrictions as a dynamic factor in our on-going assessment of risk and, in doing so, we consider the breadth and range of our Risk Appetite definition and apply it to all risk types. Going back to our diet analogy: What and how much should we have for our appetizer, salad, meal and desert? In real terms, we look at monetary value or limit to our risk and we also include all our risk areas such as stakeholder confidence, brand image, compliance risks, etc.

Just as we try, sometimes in vain, to apply our dietary needs to a specific dining event, we need to also make the process of Risk
Appetite as easy and part of the everyday risk management process. In the Risk Appetite Process, we consider our Risk Appetite as simply a guide rather than a boundary. In this way we are not bound by a bread and water restriction but may alter and adjust our appetite based on the facts and circumstances of the risk or opportunity...as long as we don’t disregard the diet completely and stay within the philosophical boundaries of our risk plans.

*Risk Appetite* is the amount and type of risk an organization is willing to accept in pursuit of its business objectives and is defined, as such, at the strategic level. In this case, the Board should be effectively attuned to the business’ Risk Appetite.

A great example is in looking at a new opportunity. The opportunity is a risk where you see grand rewards that are contemplated in your mission or vision. By applying a decision process that includes consideration of your Risk Appetite philosophy (but not a limiting boundary of the former definition), you decide that pursuing the opportunity is within your business strategy and within tenants of your Risk Appetite definition. You decide to undertake the risk by pursuing the opportunity.

To use the appetite metaphor, we may have a perceived dietary limit for our next dinner out but find that the chef has prepared a remarkable and hard to find dish. Rather than limit ourselves to the set plan, we see the opportunity and reward and we adjust our appetite accordingly. This type of decision may be applied to each and every risk decision and in this way apply also Risk Appetite to our constantly changing risk environment.

When we utilize Risk Appetite as part of our risk decision process we find that the concept of Risk Appetite becomes much more than that of a definition that serves to bind our risk activity but is now a positive influencer that enables our management of risk in a way that truly supports the corporate strategic plan.

Where your business sees Risk Appetite as a limiter you are probably limiting your understanding of Risk Appetite to a hard and fast definition and you need to evaluate the where and how Risk Appetite impacts your risk based decisions. Once you
consider Risk Appetite not only as a definition risk limits relative to its strategy but also as an enabler managing your enterprise risk you are much more armed for successfully reaching strategic objectives and pleasing your stakeholders.

*Posted by Steve Money, Professional Services, Cura Software*

Read this article on the website [Click Here](#)
Meeting Your Challenge of Setting Risk Appetite  

Posted by Bryan Whitefield on November 2, 2011

A well defined risk appetite endorsed by Executive Management and the Board is the singular most important element for establishing the risk culture you want for your organisation. Like many things in life, the best things don't come easily though. The two greatest challenges are:

1. Dealing with disinterested Executive Management.

2. Agreeing a risk tolerance that may be viewed by many as socially unacceptable or immoral.

Disinterested Management

A disinterested Executive means they have not made the link between risk appetite and the behaviour of staff. Whether they like it or not, staff are absorbing signals from management and making their own assumptions about the organisation’s appetite for risk and they are making their judgements accordingly. In the absence of a well articulated risk appetite it is certain that some of the staff will have misinterpreted the risk appetite the Executive desire.

To win over the Executive you simply need to work backwards from the decision making of staff to the signals being sent by management. Use examples to point out how the signals flowed through the organisation.

Socially Unacceptable Tolerances

For many organisations, principally those only with office workers, it is simple to articulate any loss of life to be “catastrophic” for the organisation. However, even for these organisations, one death does not usually mean the extinction of the organisation. The real challenge comes for organisations that know they will experience events that are socially unacceptable to many such as mining, oil and construction companies where lives may be lost and environmental calamities may occur. To avoid
these at all cost would mean the organisation could not operate, yet society wishes for the organisation to exist to provide goods or services we desire.

To manage this when documenting risk appetite you can distinguish between risk events that are due to negligence versus risk events that have occurred despite the efforts expected by a “reasonable person”. As an example, you can document an acceptance of risk that there will be fatalities in your business due to the risks of international travel that a “reasonable person” would assume in their role. This might include flying with an airline that is accredited and maintained to international standards while avoiding airlines that are not.

**Bryan Whitefield**  
**Director, Risk Management Partners**  
bwhitefield@rmpartners.com.au  
www.rmpartners.com.au  

Read this article on the website [Click Here](#)
"It's not the things you are afraid of that will kill you" - Mark Twain.

I have fielded a number of calls this week from recruiters looking for someone to implement a GRC process for some company. Before I can ask about firm's board governance towards risk management and accountability, the questions turn to SQL, Java and, well you get the idea. If a firm does not set its overall risk tolerance, understand its risk profile and empower managers who take risk to manage the risk, software isn't going to improve anything.

Whether one calls it GRC, Governance, Risk and Compliance, ERM, Enterprise Risk Management, ERP, Enterprise Risk Planning, or OR, Operational Risk, understanding and managing the sources of risk created within an enterprise is a human endeavor requiring judgment. This first requires a strong tone from the top and board engagement. Management must be empowered and incentivized to continuously focus on direct and indirect sources of risk. They need to be able to articulate it to the board and proactively mitigate unproductive and unnecessary risk. Risk taken on to further value creation must be evaluated, balanced with other priorities and monitored. This requires motivation, expertise and persistence.

Risk Management systems are useful but limited to its internal algorithms and the the data it can analyze. Computers are great
for alerting people to quantitative risk metrics but not so good at identifying or evaluating qualitative risk discussions. It is these unstructured risks that have the greatest likelihood of destroying an enterprise's value. Often events that have never happened before or last occurred before the collective memory of the programmers are the ones we really care about.

Quantitative Metrics are appropriate for managing many types of risk such as credit risk, market risk and weather. Unfortunately, rare events, the identification of bubbles, binary events, and any discussion that follows the words “assuming a normal distribution” can not be properly quantified. It's human nature to tend to ignore that which can not be neatly defined or measured.

Qualitative risk discussions and evaluations are at least an equal partner with quantitative tools. Quantitative methods work well with describable probability distributions such as stock prices, interest rates or hurricane prediction. Companies often embrace quantitative measurements of risk for a number of reasons.

First they can be seductively simple. Isn't it nice if management can be presented with one or a few numbers that will tell them how much risk they are taking on to produce the performance measurements listed in the same report?

Second, employing even state of the art quantitative tools can be handed off to a committee, subordinates or a contractor. Meaningful qualitative analysis requires extensive and continuing input from management and the board. Outside contractors sell comprehensive risk management tools that primarily collect and evaluate quantitative risks. If this is what they sell, the reasoning goes, this must be what we need.

Third, the government employs quantitative measurements almost exclusively. This is not because regulators don't understand holistic risk practices and the value of qualitative tools. Rather, compliance is a legal and administrative process. In order to enforce a rule on anyone, it must be written, consistent, testable and audit-able. Unstructured risk discussions and evaluations do not easily fit within the regulatory structure. I think the best efforts to mandate qualitative risk reporting are the
requirements for form 10K which includes 3.1.2 Item 1A – Risk Factors and 3.1.8 Item 7 – Management's Discussion and Analysis. While very useful to investors, these reports can be vague, irrelevant or difficult to compare across organizations. There is simply too much leeway in their preparation and a lack of timely updates on what should be included going forward.

Governance, Risk and Compliance begins with Governance. It requires the right tone from the top, engaged (incentivized) management and a cultural shift to risk being understood as a necessary but controllable input to value creation. Without this one is left with being legally compliant but not risk intelligent.

Richard Ellis, PMP PRM

www.E-bRM.com
www.linkedin.com/in/richardellis86
www.richardellis86.blogspot.com

Read this article on the website Click Here
The Costa Concordia, a Carnival Cruise Line owned ship, ran aground resulting in at least 6 deaths. This is a 4,000-passenger, 115,000-ton cruise mega-ship, with the latest and greatest technology, as it is just 5 years old. As an Enterprise Risk Management (ERM) professional, my forecast is that we will learn over the next six weeks that this is not the first near miss for the Costa Cruises organization, nor the first questionable judgment call by one of their ship's captains. My bet is that one of the thousands of crew management have reported issues in the past and that other Carnival ships have faced similar operational risks in the past several years. The problem is each one on these issues in its silo is a one-off near miss and perhaps in isolation is not worth escalating to senior management. Put them together however, and you see a grave systemic pattern that is likely to result in disaster that would have been preventable had the systemic pattern been detected and managed as a whole rather than as one-off incidents.

To be effective, Enterprise Risk Management must be pushed out to the front-line business process activity level where decisions are made and information must aggregate up across silos and levels to be understood by senior management. Few organizations have their ERM programs functioning at the business process activity level. Typically, organizations interview the top management about their "risk worries" and boil things down to the "top ten risks". Unfortunately, these top ten risks are disconnected from the everyday operating controls at the business process activity level, so these "top ten risks" continue to be unresolved. GRC programs are no better, as they focus on heavily silo’d compliance, such as SOX, IT, and Internal Audit, and also do not link risk to operating controls and business metrics at the business process activity level.

The fact is that operational risk is all around us, typically most prevalent in the organization's area of core competence. In the last
year, I have blogged about oil discovery firm's failure to manage drilling risks, leading banks' failure to manage investment risks, power companies' failure to manage power risks and manufacturers' failure to manage product quality risks. I have heard risk managers say their bosses give the same answers too many times, "It won't happen to us," or, "Although enterprise risk management is a priority, we are not ready to take our ERM program to the business process level." Since 89% of ERM and GRC programs fail to adequately manage operational risk at the business process activity level, this dangerous game of not moving their ERM and GRC programs forward to detect and manage operational risk at the front line activity level is not only fraud, but also a form of "Russian roulette" with real consequences.

Due to SEC requirements passed in February 2010, the once widespread practice of, "Don't write it down," is no longer viable. Boards of directors are now liable for not having their risk management programs reach the front line business process activity level. Now, both management and their boards of directors are liable for what they don't know, but should have known. If you are a publically traded company or you are a supplier to a publically traded company, evaluate your risk management effectiveness with these five competencies:

1. Create a risk taxonomy by naming your business processes
2. Conduct a risk assessment in each of these business processes
3. Connect mitigation activities to each of the key risks in these processes
4. Connect your business metrics for each process to these mitigation activities
5. Connect your process risks to performance management strategic objectives

These are five of twenty five requirements outlined in this complimentary risk management maturity test available on-line: www.rims.org/rmm. If you do not score above a "managed level" of risk management maturity, it means your organization is
failing to achieve these five simple steps in a material manner at the front line business process activity level, where it matters the most. The Costa Concordia accident was preventable, and so are the risks at your organization.

Read this article on the website [Click Here](#)
How to measure your Enterprise Risk Management effectiveness

Posted by Steven Minsky on January 4, 2012

I am often asked for insight on business measures or KPIs for ERM programs to track overall progress and effectiveness.

The key question for risk managers is: how do I measure the value ERM is delivering to my organization?

The following are examples of measures that will quantify and measure the value your ERM program is providing:

**Number of systemic risks identified**

- Systemic risk identification will detect areas of upstream and downstream dependencies throughout your organization, such as when one area of the organization is unknowingly causing strain on other areas. Additionally, this method could also identify areas that would benefit from centralized controls so the extra work of maintaining separate activity level controls is eliminated, increasing organizational efficiency.

**Percentage of process areas involved in risk assessments**

- ERM is cross-functional in nature and cannot be done in silos. A business is the sum of its parts. The same is true of risk. A risk event in one functional area also affects other functional areas within the business. Process owners own the risk; risk managers own the completeness, timeliness, and accuracy of the risk information. The more process owners involved in risk assessments, the more accurate and forward-looking the information collected will be, both of which are hugely valuable to the organization.

**Percentage of key risks mitigated**

- Having a sense of your overall risk coverage is important; however, it is not nearly as valuable as knowing the coverage of your organization’s key risks. Because all risk assessments should be conducted on standardized criteria, you can determine a uniform tolerance, or cut level, throughout the organization based on the resulting assessment indexes. This will help you to prioritize resources to the risks that need stronger coverage, rather than wasting resources on risks that will have no major impact on your
organization. This gap analysis with a tolerance level will also help you to identify emerging risks as they rise out of tolerance and it becomes clear that some mitigation activities in place are no longer sufficient.

**Percentage of key risks monitored**

- Most organizations have no understanding of how the business measures that they rely on daily are tied to their risks. If a risk or activity changes, organizations have no way of knowing how, and if, these changes will affect their metrics. Through risk assessments and linking risks to activities, organizations can start prioritizing what activities need to be monitored. Regular risk assessments enable organizations to detect increased threat levels and identify new emerging risks before they materialize and bring business metrics out of tolerance.

Watch a 20 min On-Demand webinar “Streamlining Governance through ERM" to learn how to measure risk management effectiveness.

Read this article on the website [Click Here](#)
A chemical plant explosion in Japan on Sunday shows the consequences of poor risk management in a really personal way. The Nippon Shokubai Co. produces a chemical that is a critical link in the supply chain for one-fifth of all the world's diapers. A diaper shortage is expected.

One, where was the risk management program to prevent the explosion? As is always with these things, in the next 6 weeks, evidence of an employee warning their management about conditions that could result in an explosion will be uncovered. It is always the front line that detects the vulnerability, but too often organization's Enterprise Risk Management (ERM) programs do not reach the front line; and therefore, there is no effective systematic risk assessment and control evaluation mechanism in place to evaluate and allocate resources properly.

Two, how can one fifth of all the world's diaper manufacturers rely on a single factory for a core ingredient? Again, poor vendor risk management. Most organizations manage vendors from a compliance standpoint and request documentation on business continuity plans but rarely do they require these plans to be tested or validated. They are typically just nice looking gibberish documented to meet a vendor compliance regulatory requirement.
Corporate vendor managers often do not incorporate ERM in their vendor management programs so that vendors can be risk assessed from various points of view for their criticality to prioritize the level of examination beyond just checking a box. In this specific case, a risk assessment would have identified that this particular supplier is extremely risky in terms of reliance and ease substitution, perhaps among other things, and thus can be identified as a critical vendor which demands more scrutiny than the standard documentation acquired through meeting compliance requirements.

Both scenarios one and two above are easily addressed by extending ERM out to the front line with an automated ERM Software that is integrated in the functional operations and governance, risk, and compliance (GRC) areas of their institutions. It typically takes only 90 days and US$15,000 to save millions or more. ERM programs are jokingly underfunded, so when you are making your next business case for automating your ERM program, help illustrate the operational consequences on business performance, and not just compliance, to get your business case approved, as you do not want your organization to be in the news for having caused a major operational risk due to negligence—or worse be shopping your resume with the equivalent of dirty diapers on your hands!

Read this article on the website Click Here
I just returned from GRC 2012 - The inaugural industry conference bringing together the Australian Compliance Institute and the Risk Management Institution of Australasia. If you are wondering what GRC stands for, why the associations combined their conferences and what GRC really means, here are my views.

What does GRC stand for? GRC is an acronym for Governance, Risk and Compliance. It has its origins in the US, particularly post the large corporate collapses of a decade ago, where there was a mountain of compliance requirements loaded onto organisations and the software industry responded with solutions. Some offered risk only or compliance only solutions, however, before long the industry was offering solutions for both, plus various elements of governance processes. Whether it was a software vendor or someone else who first coined the phrase is irrelevant, the software industry has been pushing their wares under this banner and it has become a huge industry globally.

Why the combined conference? Because in many people's eyes, mine included, the risk and compliance professions are converging. Among my clients there is a plethora of job titles with mentions of either risk, compliance or both, along with a good proportion having governance in their title.

What does GRC Really Mean? There was a lot of discussion on this at the conference. Indeed there was often complete disdain for the term. In general people could see that risk and compliance activities are part of good governance and that good governance is a good risk and a good compliance strategy and hence they are closely linked. If you were to ask me to summarise what GRC means I would say that GRC is all about ensuring the organisation has "NO REGRETS". That although we might not have been as successful as we wanted to be, we were true to ourselves.

What is a GRC Professional? In short you are a performance coach. Athletes are coached to do their best and, other than those
at the pinnacle of their sport, they fail many, many times. Perhaps you should have the title "Chief Performance Officer" or "Chief Performance Advisor"!

www.rmpartners.com.au

Read this article on the website Click Here
Cash flow versus net profits - the dangers of economic ignorance risk

In the U.S., the individual tax rates top out at 33%. But this is only part of the picture. Not only are the tax rates potentially higher depending on where you live, but the real question should not be the net profit, but cash flow.

One of the targets of the current administration is that group known as "millionaires and billionaires" who enjoy corporate jets, yachts, and more, and are vilified as earning and keeping too much of their profits. They are not paying their fair share, according to the Obama administration.

The actual numbers contradict this claim. According to the Internal Revenue Service (www.irs.gov) the top 1% of all earners pay 38% of all income taxes; and the top 5% pay 59%. Nearly half of all American taxpayers pay zero taxes. So there is a great disparity here, with "the rich" already carrying most of the burden.

These so-called "millionaires and billionaires" is a group defined by the administration as anyone making over $250,000 per year. But this includes many small businesses, the source of most job creation. The idea is that these rich folks can easily afford to "pay their fair share" and give up their corporate jets and yachts. But if taxes were raised from the top rate of 33% up to 50%, will that hurt job creation? More to the point, would it help or hurt the economy? The issue is not net profit, but cash flow; that is what determines whether or not businesses are able to hire.

Here are some numbers. Assume a small business grew rapidly last year and netting $250,000 in profits. If this business is located in New York City and is a sole proprietorship, it has several tax liabilities:
federal tax, 33%

self-employment tax (Social Security), 13.3% on the first $106,800, or $14,204

New York state tax, 6.85%

Net York city tax, 3.7%

Out of the $250,000 net profit, the taxes reduce it to:

\begin{align*}
\text{Net profit} & \quad $250,000 \\
\text{Less: 33\% federal tax} & \quad \$82,500 \\
\text{Less: Self-employment tax} & \quad \$14,204 \\
\text{Less: New York state tax 6.85\%} & \quad \$17,125 \\
\text{Less: Net York city tax 3.7\%} & \quad \$9,250 \\
\end{align*}

This leaves an after-tax net profit of $127,101, or 49\% of net.

If the federal tax rate were increased to 50\%, the federal tax would be $125,000, decreasing net profits to $84,601. Overall tax rate would then climb to over 66\%.

So with only $84,601 left over after all taxes, what about business growth? Businesses in this situation are not sitting on a pile of cash but have to consider cash flow as well. With growth, accounts receivable and inventory levels are going to be higher, meaning some of that $84,601 is tied up in these current assets. Growth also requires investment in upgraded and newer capital assets (equipment, vehicles, etc.). That $84,601 can dwindle down to zero (or less) in no time in the business expects any more growth at all.

Given this reality, how can anyone expect the business to add jobs? An unsympathetic view might be that it's tough luck if someone earning $250,000 has nothing left after taxes and cash flow. But it all comes down to a question of jobs. Growth creates jobs unless punitive taxes take profits and cash flow away. Fewer jobs means continued economic problems.
A form of risk previously never discussed may be termed "economic ignorance risk." It is easy to use class envy to appeal to the public. Those corporate fat cats with their corporate jets and their yachts are an easy target. But it is economically ignorant to over-simplify the facts. No one can expect true recovery without enabling small business to expand in real terms, meaning keeping their cash flow for re-investment in new jobs. With higher taxes, this is going to be impossible.

This is not a political debate, but an economic one. The issue is confused when some so-called economists defend the Keyserian economics of the administration, which believes that government policy creates jobs and not the business community. As an economic reality - and with politics aside - this simply is not true. Keyserian economics is a failed system and the past 2.5 years have demonstrated this profoundly.

Read this article on the website Click Here
DFA Reform: With 30% of rules in place will regulators be ready to prevent another financial crisis

Posted by Marijana Curguz on May 19, 2011

With House Committee passing a slew of rules on May 4, 2011 to postpone the implementation of derivatives section of the DFA by 18 months, Seila Bair’s decision to leave the FDIC on July 8, Geithner’s warning of a financial crisis if the legal debt limit is not raised, many are wondering if the U.S. economy is heading back into recession and will regulators be ready to prevent it.

These and other concerns were the main focus of the Regulatory Risk conference held in New York on May 9-10, 2011. The organizer, Marcus Evans, brought together leading industry Experts and a keynote speaker Carlo V. di Florio, Head of SEC Office of Compliance Inspections and Examination, to evaluate critical Regulatory Reforms: the Dodd-Frank Act, Basel III, housing finance reforms and KYC/CIP that are drastically altering the landscape of the financial world as we know it.

Florio underlined SEC need for a big budget boost to keep up with the fast-growing markets and carry out new duties they were tasked by the DFA. SEC was handed lion’s share of work to implement DFA that requires it to write nearly 100 new rules for Wall Street by summer, manage systemic risk, oversee the $600 trillion derivatives market, regulate the unregulated (PE, HF, Credit Rating Agencies, ABS) and catch the next Bernard Madoff, and secure greater transparency and liquidity.

Regulators confirmed they asked the Congress to extend the deadline for some portions of their rulemaking as only 30% of the regulations have been enacted while 62% of 387 rules have not been proposed yet. As of April 2011, none of the deadlines of 30 DFA rule makings were met. On May 4, 2011, House Committee approved a bill to delay by 18 months or until December 31, 2012 the derivatives section of DFA. It kept the July 21, deadline for reporting of swap trades and for regulators to define who is...
covered by the law. The largest 25 bank holding companies currently have $277 trillion notional amount of swaps.

Florio said SEC is finalizing the rules on the new risk-based national exam program, consolidated audit trail and large trader reporting, that will help it better track trading across the fragmented U.S. equity markets. Some of the key risks the Exam is focusing on, broken down by participants, are: Investment Managers (valuation, portfolio management, performance), Broker Dealers (product innovation, abusive sales practices, lack of technology/system breaks), Credit Rating Agencies (conflict of interests, inadequate processes, people).

The panel of industry experts including Mark Gunton, CRO, HSBC, Scott Polakoff, Principal, Booz Allen, to name a few, shared their experiences and view on how to navigate the regulatory landscape to create an effective compliance plan, determine what compliance areas are most important for growth and managing regulatory compliance risk, evaluate the people, processes and technology necessary to facilitate compliance with new regulations, optimize compliance and risk management practices by discussing key issues: new capital and liquidity requirements, enhance transparency across the business.

The conference ended on a positive note, with participants believing the financial industry is heading for further consolidation though the worst might be over as some indicators purport it: Loss projections for FI are budgeted at $4.5 Bn down from $23 bn, a year ago, deposit insurance is profitable again, Banks downgrades declined, Banks failure cost decreased to $92bn from $170bn y-o-y, there is more transparency in the markets, Whistleblowers regulation is in place, trading and markets, in particular swap deals have improved significantly.

Read this article on the website Click Here
Five Ways to Create More Jobs

Posted by Michael C. Thomsett on July 5, 2011

1. **Reduce tax rates.** Business thrives with incentives, and everyone benefits from lower tax rates. In the 1980s when U.S. tax rates were reduced dramatically, tax revenues rose along with a robust improvement in the overall economy. High taxes harm job creation. Making matters worse, high taxes do nothing to improve the economy; the more government collects, the more it spends, so that (ironically) higher taxes do not increase revenue, but they do increase spending, making deficits worse.

2. **Balance national/federal budgets.** This is so apparent that it is amazing that so many government leaders refuse to recognize it. No one -- government nor individual -- can spend their way out of recession and no one can control deficit spending by spending more.

3. **Get rid of excessive regulation.** An overbearing government is not only expensive and unnecessary; it also prevents business from creating jobs. The money spent complying with multiple layers of regulatory red tape would be better spent creating jobs. The benefit of regulation for risk managers is minimal; the cost of compliance is not necessarily related to reduction of risk. Regulation tends to become self-justifying and to grow over time for its own benefit.

4. **Allow organizations to go where they want without penalty.** Government cannot force efficiency or profits by forcing companies to take certain steps, like demanding they operate in union-dominated states or keep all factories at home. The profit motive is not only about profits; it is also about margins of profit and a friendly operating environment.

5. **Let the free enterprise system do what it does best.** Put the politics of taxation, regulation and class envy aside and deal with a reality: free enterprise and the profit motive work, not only for top earners, but for everyone. Those earning minimum income or, more seriously, those without jobs, are...
more likely to succeed in an environment in which free enterprise is allowed to thrive. So government, even well-meaning government at any level, serves the economy best by simply getting out of the way.

Read this article on the website Click Here
Global Finance and Economy: a Hot Summer Indeed

Are we seeing ghosts everywhere or is something ugly going on indeed? Take a look to some of the current debates, concerns and questions about Greece, US and China, and imagine how it all could play out.

Greece: Austerity measures and new bailout package

Last week, Greece’s Prime Minister George Papandreou won approval to his 78 billion-euro package of budget cuts and asset sales, key to receive the fifth instalment of 110 billion-euro bailout in 2010. This despite of the boiling public anger and an UN expert’s warning that these austerity measures could violate human rights. Yet the country’s overall debt situation is not likely to improve as a result: a second rescue package for Greece of about the similar magnitude as the initial 110 billion euro bailout is already being considered.

Several questions and concerns arise, e.g.:

* How long this game around Greece can continue? When and how will it end?

* Will or should the second bailout be classified as selective default by rating agencies given that private-sector is in fact forced to participate via a “voluntary” rollover of maturing Greece’s debt by banks?

* What risks the banks are taking when rolling over Greece’s debts? Do they have better alternatives? What are the implications to banks’ lending to private sector?

US: Debt ceiling and QE3

As also pointed out by IMF in its Concluding Statement of the 2011 Article IV Mission to The United S.. (20 June 2011), US public debt is on an unsustainable trajectory. In order to avoid default, the federal debt ceiling has to be raised once again (according to IMF, this has already happened more than 70 times over the past few decades). Meanwhile real economy is picking
up very slowly if at all: housing market remains weak, unemployment stays high, credit supply conditions remain tight etc. To somehow (although temporarily) cope with the situation, the Fed is set to buy USD 300bn more Treasuries. Some say, QE3 has already started (see e.g. the post in Zero Hedge, 31 May 2011).

In relation to the above, one could (for example) think about the following:

* The absurdity of the situation where just lifting up the debt ceiling means a top grade credit rating while not doing it would result in default grade

* QE1 and QE2 ended up everywhere else than helping US real economy to recover. Where will go QE3?

* Are there any real possibilities for avoiding high inflation later on? Of course, Fed has at least some technical means for mopping up excess liquidity but can this be done given the likely consequences of reducing money supply?

**China: All at the same time**

When taking a quick look to the latest news about China, it feels that the blow up is just around the corner. Just consider these headlines and excerpts:

* “The speed at which China’s local governments are taking on debt is "terrifying"." (Business Insider, 28 June 2011)

* “After years of housing prices gone wild, China’s property bubble is starting to deflate.” (Wall Street Journal, 9 June 2011)

* “And legendary short seller, Jim Chanos, says China’s local government debt is worse than America’s subprime problem.” (The Christian Science Monitor, 14 June 2011)

* “The official public debt of the central government was only 19% of GDP at the end of 2010. Adding the debts of local governments, the non-performing loans of the banks and other liabilities, such as central-bank bills, the public debt amounts to about 80% of GDP according to Andrew Batson and Janet Zhang
of GaveKalDragonomics, a consultancy in Beijing.” (The Economist, 2 June 2011)

* “China: new lending sharply down” (Financial Times, 13 June 2011)

* “The yield on Chinese bonds are inverting at an accelerating rate. This does not portend well for the Chinese economy, and this may have negative implications globally.” (Moneynews.com, 24 June 2011)

Based on facts or just guesses, these expectations may very easily be self-fulfilling. According to the logic of finance, the real risks are extremely high too.

But that’s not all. China’s large forex reserves are not well diversified either. It is estimated that around two-thirds of the total USD 3.04 trillion is invested in US dollar-denominated assets and that US Treasury bills account for half of these assets. In addition, euro-denominated assets accounted for a large share of forex reserves -- up to 25 percent. (Source: Want China Times, 6 June 2011) What if US rating will be downgraded or Greece will default? Note that if “money game” were fair game, both of these events would have happened already.

Among others the above urges us to ask:

* What are the links between the above and the China’s current monetary policy?

* How China is planning to manage all of these risks and uncertainties at the same time? Which risks are actually manageable and which ones are not?

* What is more likely for China: soft landing and hard landing?

* What is China going to do with its foreign reserves?

* Should we fear a serious conflict between China and US?

The above presents only a fraction of all the current global financial and economic challenges – a bare top of an iceberg. Vote into which topic we should bring the clarity first or add your
own: vote, support and win! I feel that no matter how well educated and capable central bankers and policy makers may be, we cannot rely on them only. Our own ability to interpret the news is at least as important.

Read this article on the website Click Here
Here’s an idea that makes simple economic sense: reduce unemployment and increase tax revenues, ending the U.S. recession in a matter months rather than years.

It makes so much sense that it will never happen, at least not under the current administration. Why? Because Obama simply does not like business. He is so committed to his economic worldview of bigger government, and has so much distrust and dislike of business, that he would never consider the obvious fix to the problem. If he did, he could probably win a second term. But true believer that he is, it would be impossible to take these steps.

Here is the plan:

1. Eliminate the corporate tax rate. Today the U.S. rate is second-highest in the industrialized world, which has caused virtually all manufacturing and many other sectors to go elsewhere. Reducing the corporate tax rate to zero would increase tax revenues, however. The employment levels in U.S. manufacturing would boom, and so would government revenues from individual taxes.

   Is this naïve? No, in fact it simply makes sense. Higher tax rates only chase away productivity and ultimately this reduces revenues from individual taxes while increasing the burden on government spending for unemployment benefits and other costs caused by having 9.2% of the workforce idle (and another 9% or so under-employed or off the roles altogether).

2. Do away with requirements to unionize manufacturing. Why are the right-to-work states out-performing the nation on average? Because without the inhibitions and productivity negatives that come with unionization, business thrive — and so do their employees. It is impossible to imagine Obama embracing this idea, not only because it contradicts his...
philosophy, but because it would demand a level of imagination he simply lacks.

There is no case to be made for unionization as a requirement to protect workers from exploitation on the part of management. The layers of regulation to protect workers, plus an enlightened human resources culture of modern times, make unions obsolete. Today unions pretend to be all for their workers, but in practice many of the larger ones are really arms of the Democrat Party, whose primary function is to ensure election of politicians who support them.

Read this article on the website Click Here
In Europe, most banks have already implemented Basel II. The next step is complying with Basel III, which has significant add-ons compared to its predecessors – including much higher capital and liquidity requirements – specifically shining a torch on the so-called global systemically important financial institutions (GSiFis). In the US, the Basel III compliance process is further complicated by the concurrent implementation of the Dodd-Frank financial-overhaul legislation.

Regulations these days are coming in faster than in the past, some within just 15-18 months. They require more complex, frequent and granular reporting. Effectively, regulators are asking the banks to share with them the same type and level of information that they would show to their top management.

This poses a challenge for banks. They have to implement new processes in shorter timeframes, while still maintaining business as usual. Many banks are still using very old technology solutions to create and manage their regulatory reporting and compliance. As the changes get more complex and start touching whole new business areas, implementing them becomes increasingly difficult, thus increasing delivery time and costs.

We see banks suffering from data overload. Siloed data repositories, legacy systems, inflexible and hard-coded reporting programmes are the reality in most banks. Off-line spreadsheets and other manual records are still often the primary source of information, especially for liquidity risk management. This issue is particularly pertinent at smaller bank subsidiaries as many of them still rely on spreadsheets for their operations.

So is there a way for banks to report in a timely and cost-effective manner?

**A harmonised approach**

A flexible approach to support changing regulatory requirements is vital. Banks should be seeking to harmonise the data gathering
process to enable this to be done efficiently, irrespective of geography. Regulatory reporting and compliance solutions should work across jurisdictions.

Forward thinking institutions will use technology investments to their own advantage. Meaningful regulatory data can add value to management decisions, help manage risk and improve market positioning. In this way, increased information demand can also become a revenue opportunity.

Read this article on the website Click Here
Cost cutting and better risk management remained high on the European financial services agenda at the recent World Economic Forum. Institutions worldwide are facing similar concerns, because of the ongoing instability in the current economic environment. Yet cost cutting initiatives and the move to further enhance risk management are often undertaken to the detriment of what customers today are looking for – innovation.

Regulation is intended to create transparency, but if not managed efficiently, it can run the risk of stifling business. Financial institutions need to re-investigate the way they look at regulation. They must think about how they can configure their business and technology to meet the increasing need for transparency.

There are signs, however, that an industry shift is starting to take place. Institutions realize that return on equity demands that the focus on core activities and services can be spun out or procured from technology service providers. In addition, some banks are already working more closely with other banks - in some cases even with competitors - to share non-proprietary IT infrastructure and platforms, and as a result drive down costs.

Our estimate is that global financial services institutions still need to reduce total costs by at least 20% - or approximately $500 billion* as they strive to get back to the return on equity levels they were achieving before the crisis. It goes without saying that this is not an insignificant figure. Any move to further reduce costs, deliver greater shareholder value and provide the customer with the ever increasing levels of experience they continue to demand needs to be well thought through.

Regulatory reform shows no sign of waning resulting in the new normal of higher capital burden. The institutions that will survive will be ones that look at how investments in innovation and restructuring of IT infrastructure will benefit them – and their customers - now and in the future.
How to conquer PPACA/OBAMACARE - a battle plan for brokers, employers and carriers - part 1

Posted by Philip Eide on November 18, 2012

This Post is the first in a set of two Posts looking at PPACA - Sometimes referred to as Obamacare or ACA.

1. **This first Post** is to provide background on PPACA with Links to valuable information to answer questions for Brokers, Employers and Carriers.

2. **The second Post** will provide a Workable, Efficient, and Cost-Effective Strategy for Brokers and Employers to deal with PPACA/Obamacare for the 2013 Plan Year and Beyond. **The time to get started is now!** This will be Posted on Friday after your Thanksgiving! **We wish you a Happy and Joy Filled Thanksgiving!**

**A Little PPACA History** -- Since March 3, 2010 when President Obama signed PPACA, the Patient Protection and Affordability Care Act, also known as Obamacare - there has been a significant disruption change to the Group and Individual Health Insurance Markets! The Supreme Court Ruling of June 28, 2012 further fueled the concerns about disruptive change to the Industry for Carriers, Brokers, and Employers.

*Wikipedia* provides the following -- "PPACA is aimed primarily at decreasing the number of uninsured Americans and reducing the overall costs of health care. It provides a number of mechanisms— including mandates, subsidies, and tax credits— to employers and individuals in order to increase the coverage rate. Additional reforms are aimed at improving healthcare outcomes and streamlining the delivery of health care. PPACA requires insurance companies to cover all applicants and offer the same rates regardless of pre-existing conditions or gender. The Congressional Budget Office projected that PPACA will lower both future deficits and Medicare spending."

With the re-election of President Obama, the changes are now inevitable! For many reasons, most Carriers, Brokers,
Consultants, and Employers had been reluctant to prepare - or implement strategies based on the lengthy PPACA legislation that did not provide many details. Now there is no waiting! Recently the Fed. - utilizing healthcare.gov - published a timeline for the implementation of PPACA from 2010 - 2015. This is a graphically rich resource for gaining a better understanding of what needs to be done when!

Where We Are Today with PPACA -- A great deal of time, energy, and money has been spent by the Insurance and Benefits Industries trying to defeat PPACA! Unfortunately, there were only a limited number individuals and Organizations dedicating creative time, energy, expertise, and money on dealing with the realities of implementing PPACA. The focus has not been on creating compliant strategies coordinated with a set of integrated Benefit/Insurance Plans.

The good news is that some specialists focused on their specific Market Sectors, ie. Individual Plans, Voluntary Plans, Technology, Enrollment, Administration, etc. They were active creating Plans, Programs, and/or Services to take advantage of PPACA.

Healthcare Reform put a focus on only one part of the overall Benefits and Insurance needs of Employees and Individuals - the Health Insurance Component. This focus was a major set-back for Strategic Benefit Planning. A number of constituencies were directly impacted - They included:

1. **Carriers** - Were forced to expend their time and energies in deciding whether or not to produce PPACA compliant Health Plans for Groups and Individuals.

2. **Carriers** - Were forced to focus on the new Medical Loss Ratios (MLRs). The following is a Link to Federal MLR Guidelines.

3. **Brokers** - Were forced to abandon or restructure their business plans as Health Insurance Carriers dramatically reduced commissions on traditional Group Health Plans to assist in compliance with MLR. An AISHealth/Health Plan
How to conquer PPACA/OBAMACARE - a battle plan for brokers, employers and carriers - part 1

Week Article analyzed this trend. An article In Life Health Pro by Allison Bell on June 15, 2012 about Brokers and PPACA was titled "Kaiser: 73% of Brokers Dislike; 20% Like It!"

4. **Brokers** - Were forced to continually take a "Wait and See" position for the Supreme Court Ruling and then the Election in making recommendations to their Employer Groups and Individuals. While Brokers hoped to avoid the disruptive changes caused by PPACA, most new it was inevitable. The dilemma was simple - What to do? Employee Benefit Advisor described this dilemma in an article by Nelson Griswold on September 1, 2012 titled "2014: Will your agency be ready?"

5. **Smaller Employers** - Became reluctant to offer Health Insurance to their Employees or started to consider dropping their exiting plans. With the details of PPACA unclear - and with a threat of additional plan costs - Employers saw offering Benefits as a threat to staying in business. Health Reform.com addressed these issues in a study titled "Helping The Bottom Line - Health Reform And Small Business".

6. **Smaller Employers** - The original PPACA provided limited details on Exchanges, Tax Credits, and Penalties applying to a Small Business grappling with offering Health Insurance Plans to their Employees. Healthcare.gov in a news release titled "Small Business and the Affordable Care Act" provides details on how "The health care law provides tax credits and soon - the ability to shop for insurance in Exchanges...".

7. **Larger Employers** - Became equally confused about the ramifications of continuing to offer Health Insurance Benefits to Employees. The law firm of Michael Best &amp; Friedrich LLP published a lengthy outline about the effects of PPACA titled "Summary of Changes Affecting Employers Under the PPACA - Amended". While helpful - this outline demonstrates the need for a Strategic Benefit Plan.

8. **Larger Employers** - Who prefer longer-term Strategic Benefit Plans were confused by the potential penalties under PPACA with its lack of details. The Congressional Research Service
provided the following clarifications titled "Summary of Potential Employer Penalties Under PPACA (P.L. 111-148)."

What's Next? -- It's time for Carriers, Brokers, and Employers to take action! Our next Post - "PART 2 - HOW TO CONQUER PPACA/OBAMACARE - A BATTLE PLAN FOR BROKERS, EMPLOYERS AND CARRIERS" will outline Workable, Efficient, and Cost-Effective Strategies for Brokers and Employers to deal with PPACA/Obamacare for the 2013 Plan Year and Beyond. These Strategies that can be integrated or stand alone include:

1. Private Exchanges - For offering Core, Voluntary/Worksite, and Ancillary Plans, Programs, and Services!

2. Defined Contribution - For providing: Employers budgetary controls; Employees valued choices to meet their Needs and Price-Points; Brokers positioning as "Trusted Advisors" and new needed revenues; and Carriers enhanced Distribution Channels!

3. Integrated Benefit Choices - For providing Employees the capacity to meet their Individual and Family Needs and Price-Points working with qualified Brokers - Choices including: Core, Voluntary/Worksite, and Ancillary Benefits!

4. Integrated Support Technologies - For Employee Education, Communication, Enrollment and Data Distribution Management!

5. Inbound Marketing - For Shortening Selling Cycles, Reducing Marketing Costs, and Driving Revenues for Carriers, Brokers, and Service Companies leveraging the Power of the Internet, Search Engines, Social/Business Media and SEO!

Working with Strategic Partners we have developed this Integrated Five Component Strategy. Each of the above parts can be utilized on a stand alone basis or integrated to maximize the opportunities. Visit our Introductory Chart to see how the above components fit together and what we will be discussing in Part 2 next Friday!
If you would like to discuss becoming a Strategic Partner by assisting in providing one of the above components, please contact phil@benefitplace.biz.

If you have Questions, Suggestions, or Comments please Email - max@benefitplace.biz or Call 216.577.5579. We invite you to Join our LinkedIn Groups, Insurance Forum, for more discussions.

Read this article on the website Click Here
Brokers and carriers - profiting from the PPACA/Obamacare disruptive changes!

Posted by Philip Eide on December 15, 2012

Philip Eide

5 Profitable Strategies For Employers, Brokers, Wholesalers, Carriers, Service Providers For Dealing With PPACA/Obamacare! Profitable Solutions For The PPACA/Obamacare Disruptive Changes! Opportunities for 2013 and Beyond!

PPACA/Obamacare has brought many disruptive changes to the Insurance and Benefits Industries as well as to Employers! While these changes are viewed by many as foreboding Doom and Gloom, there are 5 Integrated, Profitable Strategies turning the changes into Opportunities!

The Question - With the Benefits Marketplace ready and waiting for solutions, are Plan Provider/Carriers and Trusted/Advisor/Brokers prepared to deliver solutions?

When J.D. Powers & Associates analyzed the Benefits Market in 2012, the study found that "47 percent of employers say they 'definitely will' or 'probably will' switch to a defined contribution model within a private exchange". Are Brokers informed and capable of delivering the models and private exchanges? Have the Carriers configured their plans and distribution channels to meet the demand?

Solutions and Strategies to assist Brokers and Carriers - The 5 Strategies described below will assist the Brokers while creating new Distribution Channels for Carriers and Solutions for Employers. These strategies allow Employees to select the coverage that best fits their needs and creates savings for the Employers.

A group of Affiliated Partners has been formed - and is expanding - to deliver the following 5 Valuable Strategies to Brokers and the Employer-Based Benefits Marketplace:

1. Private Exchanges - For Delivering the Entire Benefit Plan Package.
2. Defined Contribution Design - For the entire Benefits Plan Design.

3. Integrated Benefit Plans- Core & Voluntary Plan Choices.

4. Integrated Support Technologies - Back Office, Communication, Enrollment, etc.

5. Inbound Marketing Strategies - For Shortening Selling Cycles

Recent BenefitPlace.biz Blogs provide in depth information about the strategies.

Here's How They Work - The Strategies are delivered by Brokers using a unique set of tools offered to Employers - Large and Small - to better address the ramifications of PPACA/Obamacare in 2013 and Beyond.

Delivery of the 5 Strategies can be either as an integrated platform or severally. Each of the Affiliated Partners delivering their part of the strategies will profit both through their participation in the affiliated partnership and as Broker/Employer Clients utilize their specific area of expertise. While Affiliated Partners will continue their traditional business models, opportunities will be delivered to them through BenefitPlace.biz. BenefitPlace.biz is the Coordinator and Inbound Marketing Conduit. See a Chart describing this process!

The First Question generally asked by Brokers is "What's the Cost?". The Answer - While flexible, the following model was most accepted in Beta Testing and affordable for Brokers:

1. A start-up fee of ($2880) that includes the Inbound Marketing - and the set-up for the Private Exchange and Defined Contribution Strategies.

2. A Fee for the select supporting technology(s) for the Private Exchanges; Defined Contribution Strategies; and the Employee Education, Communication, Enrollment, and Data Distribution on a case-by-case basis. When implementing Defined Contribution strategies with Brokers in the past, the cost of the supporting technology was passed through to the
Employers on a case-by-case basis. In some cases BP was able to negotiate with the selected Carriers to pick-up the cost of Supporting Technology!

3. A small percentage of the Fees and Commissions generated from the Employer Groups. This percentage generally ranging from 5%-12% keeps the start-up fees low and assures that the Affiliated Partners are partnering with the Brokers and Employers for the long-haul!

In conclusion - Given the challenges created by PPACA/Obamacare and other factors, these Strategies are both effective and affordable! In the face of disruptive changes, Brokers, Carriers, and Service Companies are presented great challenges and opportunities to meet the needs of Employers, Employees, and Individuals.

BenefitPlace is a research and information center serving the Insurance and Benefits Industries! For more information - Email max@benefitplace.biz - Visit http://www.BenefitPlace.biz or Call 216.577.5579.

Read this article on the website Click Here
Feedback mechanisms

Feedback mechanisms

Posted by Robert Arvanitis on August 17, 2010

The optimist says the glass is half full. The pessimist says the glass is half empty.

The engineer says the glass is twice as big as it needs to be.

The issues of failed regulation, and failed political systems more generally is not one of left or right philosophy in particular, but rather mis-aligned feedback mechanisms.

When my house gets cold, my (properly engineered) thermostat simply turns on the furnace.

But when Congress designs the process, and the house gets cold, the Congressional thermostat turns on the lights, opens the curtains, plays loud music and starts mixing drinks, on the theory that neighbors, believing there is a party, come over, and their body heat warms the house.

Doubt that? It is in fact not a joke. Consider how Congress tries to monitor financial markets....

*****

It’s almost a toss-away line: “Politicians want to overrule the boards and shareholders who normally determine CEO salary and bonuses.”

But if boards and shareholders had in fact determined CEO salaries, if they had set up rational feedback mechanisms and enforced sound risk management, then CEOs would not have gone so far off the rails.

The real issue in capital markets is the Rube Goldberg apparatus that passes for regulation. Whatever else history records, the current financial contretemps did not result from lack of regulation. Rather, it arose from human weakness on both sides—government AND industry. The amorality of industry is widely discussed. What is too often ignored is the human weakness in government.
Consider the specifics:

- Congress delegates to SEC, which delegates to PCAOB/FASB to set rules for accountants, who then compel GAAP and SarbOx reporting to shareholders, in the vain hope that they will in turn force directors to rein in managements. 
  
  - *Perverse outcome 1* – Auditors deny blame for fraud, and get rewarded with more work under SarbOx.
  
  - *Perverse outcome 2* – Rating agencies in epic fail, and get rewarded with more work under TARP.

- Coming along after the fact, shareholder suits are too blunt a corrective. They create uncertainty, and raise D&O premiums, but have no effect on management and emphatically do not discipline boards.

- Meanwhile SEC also allows SROs and exchanges to set their own rules. As does CFTC.

- Then Labor, by way of ERISA, tries to define prudent investing, which means delegating authority (but not responsibility!) to rating agencies, who are paid to say “yes.”

- Beyond this general corporate regulation, there is special banking oversight, including the Fed, OCC, FDIC, and OTS. On top of that come the state banking regulators.

All of that ignores the fact that the sole proper role of the Fed is to make sure the Treasury does NOT cheapen the dollar and thereby rob investors by inflationary default. (cf. Bagehot vs. Hankey.)

With so many moving parts involved, no specific party can ever be called to account. No one gets blamed for failure. Being mortal, bureaucrats love power just as much as private enterprise loves money.

Even worse, it is far more profitable to game the rules than to enforce them. So the best minds are squandered on games. Witness the over-reaction of SarbOx, the waste of money on useless reporting, and the ease with which companies avoided real change.
Such a scheme is far worse than nothing at all, for it deludes us into thinking that Someone, Somewhere, is Responsible.

Free markets are great, but that’s not quite what we have now.

Read this article on the website  Click Here
The G-20 Summit is over and the US has walked away without a major commitment. From the US perspective this has been a failed summit. The remaining G-19 member’s outlook could be interpreting this as a success. Our developed and emerging nations economic partners stood up to the minimum demands of the United States. It will not be the last time this outcome occurs.

As recent calls from various interests for a return to a global gold standard, US quantitative and non-quantitative easing proposals, emergency standby EU guarantees on possible defaulting Irish debt, currency wars, protectionism, and inflation/double-dip recession concerns are washing across the globe, notwithstanding Friday’s blood-letting on Wall Street, two fundamental events are occurring concurrently that may or may not be escaping investors awareness.

The first phenomenon is the acceleration of the structural evolution occurring in international commerce. The brunt of this change falls completely on US financial shoulders. Once upon a time our successful or unsuccessful economic conditions rose or fell primarily on our own predilections.

Raw materials around the world were consumed or ignored, without regard to supply or cost, by the capricious needs and changing desires of the US. Many nations benefited from sharing their natural resources with us.

Today, the role of puissant global power is being performed by an ascending Zhongguo or People’s Republic of China (PRC). The US is controlling less and less of our own economic fate. Fears ran through global markets overnight as China’s October inflation rate of 4.4% exceeded the prior’s month 3.6%. Also, China’s Consumer Price Index in October rose to an annualize rate of 12.1% up from the previous month’s 5.2%.
As a result, Every US market was hit with selling; the DJIA fell 90.52 or .8% to 11, 192.58; the S & P 500 fell 14.33 or 1.18% to 1199.21 and NASDAQ fell 37.31 or 1.46% to 2518.21. The Bond market was hit worse; the 2-year, 10-year, and 30-year Treasury all fell on Friday, the day that Ben Bernanke started QE II by purchasing $7.23 billion in Treasuries coming due between 2014 and 2016.

In commodities, gold lost $35.00 or 2.49% to $1368.30; silver fell $1.39 or 5.07% to $26.015, oil lost $3.08 or 3.51% to $86.53.

Two things; first, global markets and their economies are concerned that China may begin a series of interest rate hikes to cool off their economy, thereby, stifling global growth and second, 15 years ago markets weren’t concerned about the Central Kingdom’s inflation rate.

As disconcerting as this may be for the US investors this is the shape of things to come. The final cost of deregulation, NAFTA, one-way free trade, access to cheap labor, and open markets, plus developed nations’ seed capital generously pouring into emerging markets stretching over the last 20 years has produced today’s critical mass for a radical realignment of global economic power and market share. International capital will proceed with this new perspective on global economics.

The second fundamental shift occurring, particular to the US economy, is the inevitable demise of the later 20th century business model in the 21st century. Corporations pursuing an endless mission of maximizing shareholders value from endless rising cash flow levels and robust Deltas on the back of an ossifying American economy will discover that that formula for success is breaking down. The formula began breaking down at the onset of a NAFTA induced globalization.

This morning I spoke with a retired senior executive from the insurance industry and a friend. He told me that this week MetLife was exiting the long-term care insurance business. This follows other insurance companies that have exited both the fixed and variable annuity business in the last year. The insurance industry is realizing that their investment portfolios are becoming
incapable of generating sufficient returns to sustain several of their traditional business lines going forward. Insurance industry mergers and acquisitions will only kick the can down the road - not solve the problem.

Moreover, medical, pharmaceutical, and technological innovation over the next decade may extend their customer’s average lifespan 5 to 10 years or greater, crimping future earnings. Corroborating this thesis, Bill Gross of Pimco made a confession about this new reality and the subsequent detriment to the future performance of his $2 trillion portfolio in his November letter to investors.

Performing objective analytical [connecting the] dot work, this is precisely the precarious position airline and automobile industry union workers and their unions found themselves, over the last decade, now facing municipal workers.

Austerity ideologues and the main stream media demonize and batter retirees and their unions who merely want their mutually agreed to benefits upon retirement. These contractual terms were earned in good-faith negotiations much like the negotiated terms of a mortgage contract. They are not the villains; the true villains are simple math and careless long-term assumptions.

Failure of the marketplace to deliver non-guaranteed but optimistic presentations of average annual assumption rates, promoted as achievable by the investment industry, revealed the limitations of the marketplace and free markets. Securing organizations asset management business was the motive. Everyone suspended disbelief.

I recently attended a Global Asset Allocation Summit and Emerging Managers Summit, both events hosted by Opal, and I was mildly shocked to hear that pensions and trusts are still clinging to 8% and 9% average annual return assumptions for their portfolios. That orthodoxy was never seriously challenged by most attendees. The predominant asset allocation still comprise of equities, fixed income, and real estate. Alternative Investment percentages are insignificant.
While such returns were obtainable during the secular bull market of the 1980’s and 1990’s, investment portfolios now are confronting a secular bear stock market, a collapsed credit market restricting liquidity, punk consumer demand, and a residential real estate market in depression. For the foreseeable future, a consistent domestic 8% - 9% average annual return in a traditional asset allocation mixture is doubtful.

Realize that the inability of the marketplace to deliver on these ring size returns is only the effect. The cause of this arrested development is the before mentioned structural change in international commerce which renders the general usage of the 20th century US business model itself unrealistic. The average American is absorbing petite returns on her principal in CDs and T-bills, flat wages, and shrinking net worth from stock market and real estate losses.

Retiring baby boomers comprise a significant portion of affluent consumers. That generation’s consumption appetite and spending patterns has forever changed. Consumers, representing 70% of today’s US economy, are also gun-shy from one too many bubbles bursting, lately, to aggressively invest anymore. Consumer sentiment surveys oscillate from month to month, a clear sign of uncertainty and anxiety.

Reconciling never ending corporate earnings increases with stunted cash flows and insecure disposable income from a matured economy captained by a constipated government, lacking a coherent industrial, fiscal and monetary policy and supposedly driven by upset and untethered voters, is unrealistic.

Once, a $.50 cup of coffee is now a $4 Starbucks Venti Iced 24 oz. Caffé Vanilla Frappuccino/Soy/Whipped Cream; a $.25 phone from a phone booth is now a $125 monthly mobile smartphone bill from Verizon; free broadcast TV is now a high-speed internet and premium $200 monthly cable bill from Comcast. Free daycare in a single paycheck home is now a $200, $300, or $400 weekly Kender Care daycare expense for both working parents.
Daily expenses that were recently considered trivial are now deemed luxuries for many. I would avoid many retail stocks whose products for consumers are totally discretionary in nature.

The dreaded disease afflicting our economy is the big C - change. There is no cure. It is inevitable. How capital is managed differently, in a new century with different parameters, is equally important as where and when to invest.

The last global intermission began shortly after the end of World War I and concluded after the end of World War II. The curtains are falling on that mid-20th century world that we inherited from the greatest generation whether or not we approve or are prepared for the aftermath.

Make no mistake; we are in another historical intermission. The datasets and impermanent financial laws of physics of the 20th century are approaching their expiration date.

Read this article on the website Click Here
Managing Counterparty Risk key to restoring confidence in finance industry

Posted by CJ Conti on August 18, 2010

Written by Xavier Bellouard, founder at Quartet FS

Monday, 16 August 2010

Most of Europe's biggest banks comfortably passed the Committee of European Banking Supervisors’ recent stress tests and the sector has breathed a visible sigh of relief. However, plenty of uncertainty remains over banks that either squeaked by with just enough capital or passed but did not fully disclose the data that went into their calculations.

The spectre of counterparty risk, last seen in dramatic form in the wake of the Lehman collapse, is not far from regulators’ and investors’ minds amid the continuing eurozone sovereign debt crisis. So, with regulation and stress tests to one side, what else can financial institutions do to convince the market that they are appropriately managing credit risk and thereby encourage more lending back into the market?

Risk is an acceptable, even a welcomed part of trading. Every trade comes with some risk attached - it is just a case of knowing what the potential problems are and being comfortable with them. But as the financial crisis showed, pinpointing where the risk lies is not always so straightforward – even big institutions didn’t always understand the full extent of their exposures. However, better understanding and management of risk, especially counterparty risk, will be key to the ongoing financial recovery and to re-injecting confidence back into the interbank lending market.

A large part of better managing credit risk will come from providing risk managers with increased access to data in order to gain a thorough view of counterparty risk exposure and calculations. The evolving regulatory landscape and greater need to monitor, measure and report, has advanced in such a way that understanding and realizing these risk exposures in real-time has become crucial to a financial institution’s ongoing stability and
success. Risk managers need to be able to provide aggregated figures quickly and accurately in order to truly establish the position the business finds itself in.

However, with a multitude of other risk facets to consider, including liquidity, market and operational, many risk managers are struggling to adequately analyze and establish their positions. No-where is this truer than in the front office, where 21 months after the collapse of Lehman Brothers, financial institutions are still struggling to properly calculate counterparty risk. Due to its interconnected nature, counterparty risk analysis must not only take into account various data, including VaR, P&L and sensitivities, but must also integrate a number of asset classes and draw together an understanding of the collective impact that they have.

Once counterparty risk is accurately established, risk managers need to gain better access to and analysis of this data so they can more effectively bridge the gap between ‘quants’ and decision makers. For example, business decision makers need information that goes beyond a single indicator or figure so that they can fit credit risk into the broader perspective for the senior management team and board.

Banks’ traditionally siloed approach however has meant that to date such a scenario is more of a pipedream than a reality. However, aggregating high volumes of data from multiple streams to produce both snapshots and the ability to drill down into the data in real-time is now possible with the right technology solutions. While technology is by no means the panacea to solving all the issues associated with risk management and indeed counterparty risk, if implemented and deployed appropriately, it can provide detailed analysis and ensure that decisions that need to be made quickly are not only well informed but also support the business. In short, the quicker a firm can realize its true counterparty positions and potential exposures in the context of the overall risk picture, the greater its overall market competitiveness and confidence will be.
Of course, implementing this kind of change through a technology refresh will take time. In the short-term, it will be the interbank lending markets that will have the answer as to whether confidence is returning to the European banks. However, in the longer term, understanding where a financial institution’s risk lies, and what would happen in a worst case scenario, through better access to, understanding and analysis of data will reduce the fear of counterparty risk that is currently stifling the market’s fledgling rebuilding of confidence.
Death By Liquidity

Posted by Richard Chapman on May 28, 2012

‘Shortage in liquidity will kill you instantly and excess liquidity will kill you over time’ is a well-known industry saying which serves as a very real warning to banks across the globe of the dangers of poor liquidity management.

These dangers are highlighted even more starkly by the waves of change that are washing over the banking world, ranging from Europe’s painfully drawn out debt issues to last month’s revelations that four major US banks failed their latest rounds of stress tests. All in all, banks’ liquidity management strategies (or lack of) are very much under the spotlight.

As emergency funding becomes ever prevalent in Europe with the hope of improved liquidity as directed by Basel III, banks face continued cost challenges and threats to long term reputational damage which are often, as we have seen, hard to recover from. With Dodd Frank on the horizon, which many believe will align with Basel III directives, pressures on bank liquidity management have never been higher.

These new market dynamics and burdening regulatory requirements are increasing operational challenges which if we look at in more detail, strongly support the business case for re-evaluation of liquidity strategies.

Historically banks have struggled with acquiring visibility of deviations on desired liquidity profiles which ultimately either result in a shortage or excess in liquidity. Without access to accurate and timely information, treasurers and cash managers struggle to identify and respond to these deviations as early as possible; this hinders the bank’s ability to capitalise on opportunities and mitigate against potential risks.

In order to improve this visibility, more and more real time, intra-day data has to be passed from the back to the middle and front office. This creates the challenge of increased back office costs,
which the bank must mitigate against in order to safeguard future profitability.

Increasing optimisation of business processes is the only real way that banks can overcome these challenges and acquire greater clarity on their ‘cost of cash’ – the precarious balance between protecting the bank and its revenue – to help ensure that coupled with achieving regulatory compliance, cash and liquidity reserve strategies support future growth objectives.

Banks that will successfully dodge ‘death by liquidity’, are those that are able to:

1. Release strategic cash by optimising their liquidity buffer calculations and determining an appropriate liquidity strategy
2. Reveal hidden cash by identifying intra-day surpluses or shortages in liquidity and rapidly responding to them
3. Refine moving cash by optimising their business processes

Despite new liquidity requirements not being fully defined, banks that do not act will simply fall victim to their own lack, or surplus, of liquidity. Those that seek new ways to optimize liquidity provision and more effectively forecast future liquidity distribution will not only survive, but will thrive in the long term through enhanced business processes. New tools which provide an agile foundation on which to ease compliance and generate more accurate and timely calculations are a game changing asset in transforming bank liquidity strategies.

How far are banks in re-evaluating their liquidity strategies? How many are equipped both culturally and operationally to successfully manage their cost of cash?

Hear how banks can successfully overcome new world liquidity challenges with our series of videos

My next blog will explore in more detail why banks need to optimise liquidity buffer calculations and determine an appropriate liquidity strategy to release strategic cash.

Read this article on the website Click Here
Are banks ready for Counterparty Credit Risk under Basel III?

Maturity across the Counterparty Credit Risk (CCR) and Credit Valuation Adjustments (CVA) space varies greatly across the industry. Our recent survey provided some interesting insights as to whether banks are ready for CCR and CVA under Basel III, thanks to detailed responses from our clients and academic participants.

We found that there are clear differences of opinion between academics and practitioners particularly when it comes to Basel III readiness for CCR. The same is reflected with regards to banks having access to the right people and the right technology to effectively calculate and manage CVA.

However, from our survey responses, most banks themselves feel they do have access to the right people and talent but struggle with technology requirements, particularly with access to data. This is very much the crux of the issue facing the industry - CCR is a hybrid product and modelling it accurately requires several data sets which have not historically been combined for use regularly. Over 70% of the survey participants are now reviewing their credit support annex (CSA) and collateral agreement data in a bid to prepare for Basel III. Speaking from personal insight, further challenges will likely arise due to restrictions created by legacy systems, organisational alignment and computing power required.

Added sophistication, be it of process, technology or people, will come at a price, and there is a trade-off to be made between precision and cost of the overall architecture. This balance must be struck for the risk managers, quants and technologists who will use it and will be vastly different for each organisation.

Indeed, while most of the big names are well on their way to building their CCR management systems, several smaller banks are still trying to understand how far they need to go to be ready.
Clearly the stakes are high. They are further compounded by uncertainty around regulatory timelines, the extent to which the OTC market can move to a central clearing model and the capital charges and P&L volatility which CCR brings. Banks certainly need to start preparing now so they are not caught out further down the line.

Read this article on the website [Click Here]
Visibility and control: the liquidity management mantra

Liquidity has moved further and further up banking executives’ agendas thanks to the growing industry focus as well as regulatory demands for more liquidity to be available in banks. Following the 2008 crash, liquidity has established itself as a risk concern for banks like never before – the failure of Northern Rock was essentially one of liquidity not funds. As a result, liquidity management strategies continue to be at the forefront of any strategic risk plan.

A fundamental challenge for banks is that increasing amounts of liquidity are needed to support clearing and settlement, customer business flows and regulatory requirements. This is happening in parallel with rising costs of cash and high quality collateral while supply remains restricted. To illustrate the extent of the issue, it’s been estimated that European banks will need approximately €2 trillion in qualifying assets to meet new regulatory requirements.

As liquidity is a key resource, banks are reforming their liquidity operating models so that systems give real-time visibility to liquidity information. Visibility and control is now the mantra for effective liquidity management. This trend for visibility and control meets its greatest challenge in the supervision and management of currencies that are cleared and settled indirectly through agents. Pressure is rising from regulators and central banks for banks with significant cash flows to be direct members of clearing and settlement systems. Changes to risk policies and pricing among leading settlement banks are also driving rationalisation of correspondent banking models and arrangements. Large networks with replicated capacity are being trimmed down and demand is growing for improved intraday information services.

As many bank departments use liquidity on a daily basis, there must be enhanced controls in place and banks must demonstrate active management, allocation and pricing of liquidity. In
addition, the payment processes that handle intraday cash flows must provide real-time control over scheduling and exposure to external accounts and counterparties. Banks must take steps to adjust their liquidity management strategies or risk being hit by expensive collateral costs or unfavourable liquidity risk profiles.

Read this article on the website [Click Here](#)
Financial Risk Management - 5 Misleading Criticisms

Posted by Cristin Riffle on April 16, 2012

Financial Risk Management, like any discipline, has its limitations. Understanding how to manage financial risk simply involves developing a proper appreciation of these limitations. Few understand this better than Wiley author Thomas Coleman, who shares 5 Misleading Criticisms of Risk Management.

Risk Models May Not Capture All Risks

The models used to measure risk will never include all risks. Nobody should be surprised. A risk system should be viewed as a tool for summarizing and aggregating a large amount of information in a concise manner. Such a system will not be perfect, and users should recognize that in using the results.

Risk Measures Such as VaR and Volatility Are Backward Looking

This is simply the way the world is: we can seek to understand the past, but we cannot know the future. Understanding the past is terribly important because understanding current exposures and how they would have behaved in the past is the first step toward managing the future. As the philosopher George Santayana said, “Those who cannot remember the past are condemned to repeat it.”

VaR Does Not Measure the Worst Case

Statistical measures will never tell us the worst case. Whatever VaR level we choose, the world can always throw something worse our way. Although VaR is often referred to as a “statistically worst-case loss”, doing so is both intellectually lazy and dangerous. It is intellectually lazy because a so-called worst case relieves us of the responsibility for thinking of the consequences and responses to yet worse outcomes. It is dangerous because it is certain that results will, at some point, be worse.
Quantitative Techniques Are Complex and Require Expertise and Experience to Use Properly

The financial business overall, not just risk measurement, is complex and is becoming more complex all the time. Managers at financial firms should take their responsibilities seriously and learn enough about the business, including risk measurement, that they can effectively use the available tools. Risk professionals have the corresponding responsibility to explain their techniques and results to nonexperts in a simple, concise, transparent manner. Simple ideas, clear presentation, and concise description must be the goals for anyone engaged in measuring risk.

Quantitative Risk Measures Do Not Properly Represent Extreme Events

Quantitative risk measures do not catch extreme events. Experience does not catch extreme events. Imagination can try, but even that fails. Extreme events are extreme and hard to predict, and that is just the way life is. We need to recognize this limitation, but it is hardly a failure of risk techniques. To criticize the field of risk measurement because we cannot represent extreme events very well is just silly, like criticizing the sky because it is blue. Anybody who does not like extreme events should not be in the financial markets. Luck, both good and bad, is part of the world. We can use quantitative tools to try to put some estimates around extreme events, but we have to learn to live with uncertainty, particularly when it comes to extreme events.

A Proper Appreciation of Risk Management Limitations

A key component of true risk management is an appreciation of not only the power but also the limitations of quantitative risk techniques. Quantitative techniques work best in the hands of those who are keenly aware of the limits and boundaries of what these techniques can provide. A deep appreciation of the limitations gives us the confidence to rely on the techniques when appropriate and the good sense to turn elsewhere when necessary.
The existence of limitations is not a problem. Failure to appreciate our limitations, however, is a serious mistake. Overconfidence in numbers and quantitative techniques and in our ability to represent risk, extreme events in particular, should be subject to severe criticism because it lulls us into a false sense of security. Understanding the limitations, however, does not mean throwing out the tools that we have at our disposal, even if they have limitations.

Keep Reading at Capital Exchange Blog for the Full Article>>

Thomas S. Coleman is the author of Quantitative Risk Management + Website: A Practical Guide to Financial Risk. He has worked in the finance industry for more than twenty years and has considerable experience in trading, risk management, and quantitative modeling. Coleman currently manages a risk advisory consulting firm. He is also the author, together with Roger Ibbotson and Larry Fisher, of Historical U.S. Treasury Yield Curves.

Download a preview chapter of Quantitative Risk Management to learn more: Risk Management vs Risk Measurement Chapter 1 Sample>>

Read this article on the website Click Here
How to set up a successful Risk consultancy?

I'm looking for some marketing intelligence regarding the best practices in setting up a Risk practice.

What constitute the value proposition of a Risk consulting services? What are the critical things to put attention on?

Can anybody share his/her knowledge & expertise in both best practices for setting up a new Risk Consulting practice and the customer perspectives on how they select a consultancy? Are there any case studies available?

What is the most important from a client perspective: previous experiences, robust methodology, tools, overall thought leadership?

What methodologies work and for what type of organization? Based on what criteria do clients select Risk consultancy? What is the best offering strategy?

Thanks.

Read this article on the website Click Here
Am in the process of enhancing performance measurement for our Risk department but would want to quantify our performance as much as possible. What are the key KPIs for Risk staff?
Brand Building of Risk Management Department

Posted by Sonia Jaspal on September 24, 2010

Your brand is created out of customer contact and the experience your customers have of you" - Stelios Haji-Ioannou, Chairman, EasyGroup

The risk management departments are sometimes perceived in negative light due to their role in the organization. The business operation teams view the risk management departments as office police, watch dogs, critics and messengers of bad news. The basic job function of the risk management departments is to:

Conduct audits and reviews of business operations and identify weaknesses, non-compliance and non-adherence issues. This generally negatively impacts the business operation teams as their work is under review and shortcomings are identified.

Ensure compliance to all statutory and legal requirements. This activity sometimes results in business operation team needing to adopt a longer process with more controls and/or sacrifice a specific strategy of earning profits because it contravenes laws. Here risk managers advise sacrificing profits to maintain ethics and laws, which again negates the activities of business operation teams.

The negative image causes a lot of damage to the department and team members. The following reactions of business operation teams are sometimes observed:

Lack of transparency or hiding facts from risk management team.

Obstructing risk management team’s participation in critical meetings and discussions.

Creating political scenarios where risk management teams credibility is put in question.

Ganging up or retaliating against the risk management team at a personal level.
These reactions are driven by emotions of the business operation teams. It is a scenario where the messenger of bad news gets shot. As one senior manager said to me when I was responsible for fraud investigations - “Sonia, your presence in my office indicates to me big time trouble, so I can’t say I am happy to see you. However, as there is trouble and I know it is you who is handling it, it gives me a level of confidence that it will be handled efficiently.” This statement basically indicates the sentiments of most professionals when they see a risk manager in their office. Sometimes the views are so clouded that a risk manager’s professional job and personal personality are considered one, and they are viewed as being critical, ruthless, rude, etc. in personal life.

These negative emotions build resistance to the risk management department and their work is made more difficult. The need of the hour is for the risk management department to focus on building a positive brand image. The following process should be adopted for building a brand of the risk management department.

Vision & Mission of Risk Management Department

The risk management department needs to position themselves such, that stakeholders and customers view them as value adding agents. The vision and mission statement should be communicated to all the stakeholders and customers to ensure that same message is received by all. This can be done by putting up on the company intranet in text and video. Mass newsletters and emails can be used to convey the message.

Understand customer requirements

The risk management department should do some internal selling to build awareness that business operation teams will benefit from associating and involving them. Organization surveys, group forums and one-to-one in-depth interviews should be conducted of the business operation teams. The purpose should be to understand their requirements from the risk management teams, and their positive/ negative emotions regarding various
aspects of risk management. The business strategies and operations should be understood along with personal aspirations of the team.

With this information the risk management team should conceptualize and discuss a method by which they can hand hold the business operation teams in achieving their goals with complete compliance to legal requirements.

Build trust and credibility

The risk management department at some level is viewed with fear and apprehension by the business operation teams. The perception is that the negative points highlighted in the reports will be used as political ammunition to harm the business operation managers. This creates an environment of distrust.

In a risk management department trust is the key component of its reputation. A risk management department perceived as unethical, political and self-serving can damage not only the department but also the organization.

The risk management team needs to first focus on building a non-political independent image which is for the benefit of the organization. Few aspects need to be ensured:

Reports issued focus on process shortcomings and are not person specific.

CXO’s and other managers do not use the reports to settle their personal political agendas.

Develop relationships at all levels of the organization to address employee concerns regarding the reports and their impact.

Ensure transparency in the process and obtain buy-in of the business operation teams on the recommendations and way forward.

In nutshell, the department should always be perceived as following the high moral ground and using ethical means to manage issues.
Focus on the bigger picture

The image of risk managers is that they are focused on nitpicking and make mountains out of mole hills. The other aspect is that they do not appear at the CXO radar since the observations are immaterial from the CXO’s standpoint of business. This image is basically formed as the risk management departments are focused on transaction audits.

The risk management department needs to develop a strategic focus and understanding of the business. They need to involve themselves at the point of strategy formation and provide viewpoints for increasing shareholder value while minimizing risks.

The present day organizational challenge is to build a healthy work culture. Risk managers can be key drivers for building an ethical and constructive work culture. They need to develop the core values of the organization and work with organization behavior change management team with human resources department to build a uniform culture throughout the organization.

Reward and recognize accomplishments

The next negative viewpoint of the risk management department is that it is viewed as a department which dishes out the punishments with a stick in hand. People suffer emotionally from the criticism and the management actions taken for implementing the recommendations.

Here the risk management department needs to bring an attitudinal shift in business operation teams. The good things about their operations and positive compliance should be recognized and rewarded.

The risk management department can initiate a formal recognition and reward system with the help of human resources department. The criteria for achieving the key performance indicators should be communicated to the operations team. In some manner a competition can also be set up to check on the
awareness of risk management practices and adherence to the same.

Last but not the least, the reports submitted should provide a balanced view. For example, if 20 internal controls checks have been done, and 5 are considered weak. The report should indicate that 15 internal controls are good and only 5 are weak.

To summarize, risk management department to build a positive image needs to ensure that the business operation team experiences with them are favorable and perceived in positive light. They should take care that they are not perceived as selling negative services.

Welcome your opinion on building a positive brand.

Visit me at http://www.soniajaspal.wordpress.com

Read this article on the website Click Here
Creating a risk-focused organisation

Posted by Peter Chisambara on September 2, 2010

The nature and type of risks facing the organisation:

One of the main challenges facing managers in today's constantly changing business environment is dealing with uncertainty and creating a risk-focused culture within their organisations. New technologies, new concepts (such as social media and web 2.0), and changing market dynamics are all presenting managers with both threats and opportunities.

This uncertainty has the possibility of creating or destroying customer value and shareholder value, strengthening or weakening brand reputation and above all increasing or decreasing the organisation's competitive advantage.

Understanding the nature and type of risks facing the organisation is the starting point to a successful creation of a risk-focused organisation. With an ever changing business environment comes an increased number of risks. Though risks can be identified separately, for example, supply chain risks, people risks, catastrophe risks, IT risks, reputation risks, country risks etc. one way of identifying these risks is by grouping them into the following sub-categories:

**Strategic Risk:** This involves analysing and evaluating the effect of competition, customer changes, industry changes, global expansion, potential mergers and acquisitions, product mix, markets and locations of operations on the business.

**Operational Risk:** This involves analysing and evaluating the ways in which the organisation achieves its goals and objectives. In other words, you are looking at the daily activities and processes and identifying whether they are still viable or they need improvement. For example, this involves looking at processes, information gathering, analysis & its storage, emergency response procedures, protection against external events such as natural catastrophes and disaster recovery policies.
Creating a risk-focused organisation

**Financial risk:** This involves analysing and identifying the effect of interest rates, inflation rates, foreign exchange rates and the availability of credit on company cash flow, return on investment, credit rating and profitability of operations.

**Legal risk:** This is risk pertaining to regulation, compliances and lawsuits for an organization. This also involves identifying all the rules and regulations that the organisation is bound to, ensure that they are being followed to avoid paying non-compliance penalties. The starting point could involve looking at your industry standards set by your industry's regulators.

**Environmental risk:** What is the impact of your organisation's activities on the environment? This involves looking at levels of your carbon footprint, pollution levels (noise, odours and light), environmental compliance in all locations, natural resources damage and ongoing monitoring and management.

**Social risk:** This looks at your organisation's impact on human beings, both from an internal and external perspective. Areas investigated may include, anti-discrimination policies, safety of products, product reliability and quality, sexual harassment concerns, training and education of employees and hiring and promotion practices. The key is developing and maintaining a positive relationship with both your internal and external stakeholders.

**Making risk management every employee's everyday business:**

The process of identifying, analysing, evaluating and managing risks within the organisation should not be solely left in the hands of senior personnel. Although senior management have the overall say in the deciding the destiny of the business, they might not possess all the knowledge about the risks facing the business. Thus they need the input of other management personnel and the employees.

In creating a risk-focused culture, managers should:

**# Move away from a silo-based thinking of managing risks:**
This means instead of making say the finance department focus only on financial risks and the IT department on IT risks only, an
integrated approach (Enterprise Risk Management) should be pursued. This avoids looking at organisational risks in silos but from a broad perspective. This also promotes co-ordination between various functions of the organisation.

# Promote ongoing monitoring and management of risks: Risk management is not a one-off process that is done say once a quarter or twice a year. As the macro-economic environment is always changing, so are the risks to the business. When risk management becomes an everyday business and its importance raised within the organisation, the whole culture is going to change and embrace risk management as a value enabler.

# Encourage training and education of employees: Both employees and managers need to be fully equipped and aware of recent developments in risk management. By sending employees on short courses or industry conferences, their knowledge of risk management is refined and they can use that acquired new knowledge for the betterment of the organisation.

How else can managers foster a culture that is risk-focused?

Read this article on the website Click Here
There's a lot of nonsense about risk and complexity at the moment, notwithstanding the good work by a few people.

Let's remember that at the heart of things there are people, experts, stakeholders, employees and communities. Everybody shares a little bit of information about what has happened, what will happen, what we need to watch out for, and for any given situation, what we need is a multi-level open discussion with everybody involved. The conversation needs to be a structured, balanced, collaborative conversation and, apart from good manners and common sense, if there are tools out there that can help manage these conversations and remember what was last talked about and how things turned out, then we've just about cracked it. If companies, organisations and communities are hierarchical and dictatorial and don't encourage conversations, then sure, use statistics, but it misses the point and wastes a phenomenal resource - the people who share the emerging story. For sure, if I'm going to be tried for a crime then please let it be a fair an unbiased jury and not a statistician controlled by a dictator.

The main way to understand and mitigate risk is to get busy listening. It's not rocket science and like good health is free to all that choose it.

Read this article on the website Click Here
Preparing Annual Risk Management Strategy

Organizations would be focusing on preparing the risk management strategy and plan for 2011 as it is the last quarter of the year. Normally, Chief Audit Executives, Chief Risk Officers, Head of Internal Audit, Chief Information Security Officers, Head of Compliance, Head of Ethics and Head of Fraud Risks are very busy in the last quarter finishing off the year-end targets, objectives and key performance indicators. The next year strategy is developed from the previous year reports, observations, balance score cards and risk dashboards. A simplistic risk management strategy focuses on the following:

1. Financials - Developing a budget and other cost indicators
2. Operations - Preparing audit and review schedules. Listing out policies, procedures and manuals to be prepared and reviewed.
3. Resources - Formulating a hiring and a training plan
4. Knowledge – Developing knowledge bases, writing research papers and upgrading risk management tools and software.

Risk management has become complex and critical in the present economic environment. Without sophisticated and skilled risk management departments the organizations may face multiple disaster scenarios. Globalization, technology, economic environment, regulators, competitors, and speed of change, all have contributed in making business operations more complex. Risk management departments need to gear up and develop annual strategy considering these aspects in mind.

Five suggestions for preparing a comprehensive annual strategy are given below:

**Break the Silo Approach**
Depending on the size of the organization, the organization may have a number of departments focusing on risk management. To name some, in respect to the department heads mentioned in the first paragraph, we have Internal Audit, Fraud Prevention & Investigation, Risk Management, Compliance, Information Security and Business Ethics. These departments generally have some overlapping functions and turf wars. Silos are formed and the senior management has difficulty in making sense of various risk dashboards and reports presented by the department heads.

Prepare individual plans for the departments and roll them upwards to have a combined one of all risk management departments. Prepare one single risk management strategy and plan for the organization as a whole to present the same to senior management. Present a plan to the management which emphasis on the top risks to the organization, with a plan to mitigate and control them. The management will have higher respect and provide greater support to the integrated approach. Various risk management departments will also be able to save cost and time on monitoring various risks by reducing duplication of work, leveraging synergies and sharing tools and information.

**Determine Risk Philosophy and Appetite of the Organization**

In some cases, the risk management departments present a risk dashboard to the senior management of the organization. If the CEO of the organization asks “Can I hold you on this? Are you sure that if these top 10 risks are mitigated, the organization will sail through the year?”; the head of the department generally cannot a say a definitive “yes”. The answer is given with a maybe, but, if etc. but not a “yes”. So the question is how should a risk manager address this concern.

Risk management department need to determine the risk philosophy and appetite of the organization. To assess the risk philosophy, understand the organization culture and environment. The way business operations are conducted daily and the organization’s strategy are good indicators to find the risk philosophy. Assess whether business has an aggressive or conservative attitude towards risks for achieving business goals.
Risk appetite is the amount of risk which the organization is willing to take to undertake business activities. A simple question to ask the board of members would be - “What amount is going to make you uncomfortable if it appears in the business newspapers?” Consolidate the risk exposures from the various risks identified by the risk departments and present it to the board. Finally, assess whether the company’s internal outlook on risk philosophy and appetite are consistent with the viewpoints of the board and other stakeholders. Realign the two where required to prepare the annual strategy.

**Understand and Integrate with Business Strategy**

In a few companies, the annual strategies and plans of business and risk management are drawn up in parallel, with neither having information of what the other is planning. The risk management strategy cannot be internally department focused. The risk management heads need to obtain information on the business strategy of the organization to understand strategic risks.

For example, obtain information on new products and services which the organization is introducing in the coming year. Identify the territories, branches, and countries which the organization is planning to expand its business operations. Determine what will be the risks of expansion and innovation. Let us say, a USA company is planning to introduce its products in India. Now India has different laws, regulations and taxes. Also, the operational risks are different. Understand these risks and integrate them in the annual strategy and plan. This way, neither the risk management departments nor the business operation departments will be surprised. The budgets and plans would be incorporated and approved before the year commences, hence there will be limited fire fighting.

**Focus on Building Relationships**

One of the grouses which risk management departments have is that they are not on CXO’s radar, do not have direct reporting to
Preparing Annual Risk Management Strategy

the top or representation at the board and are sidelined from the critical business operations due to negative perceptions.

Plan for the coming year and prepare a wish list. Include in it time required from CEO and other CXO’s, formation and membership of risk oversight committee, a new organization structure with the head directly reporting to CEO and a nomination at the board. Discuss these aspects with the CEO and senior management during plan preparation. This will ensure that the senior management schedules the requirements in their plans. Insist that the CEO puts risk management as one of the points in his/her personal balance score card. This will make sure he/she is dedicated and committed to risk management throughout the year.

Discuss the composition of the risk oversight committee and audit committee. Identify the members you wish to nominate who support risk management initiatives. Define the process of reporting to the board and the audit committee. Get their commitment for board nomination and new organization structure for risk management departments. Start the groundwork for building relationships at the planning stage itself.

Assess Competitors Strategies

The risk management departments are generally happy with what they are doing and discover information about tools and methodologies from various institutes periodicals, magazines and conferences. In a few cases there is some focus on the operations of risk management departments of competing businesses and organizations.

Determine which organizations are competition to the business in respect to products and services in various territories. Focus on finding information of the risk management department operations of these organizations. Find out which risks the organizations faced, how they were mitigated, what kind of tools and knowledge bases they are using, what are the staff strength and the skill set and the organization structure. Will some of the practices result in cost savings and better synergies within
business? Determine the similarities and differences, and assess what can be incorporated in your organization effectively. There are some lessons which can be learned from competitors success and failures. Leverage on competition knowledge to learn these lessons.

The above mentioned five points are those which can be easily incorporated to prepare a comprehensive annual strategy. There are a few other things which the risk management departments can look into. Some of them are, introducing ERM, building risk management department’s brand, applying collective intelligence etc.

A single line of advice would be to look at the bigger picture and question the status quo. Put on your thinking hats and prepare a new strategy. Wishing you all the best for preparing the annual strategy

Read this article on the website Click Here
It’s all about good governance at the core

On the surface at least, it’s hard to take away positives in the wake of the financial crisis. Yes, it taught us that we have to manage risk better, improve processes and become more transparent. But it’s the regulators globally that seem to have taken these lessons closely to heart.

With some banks still struggling to conform to Basel II requirements, Basel III is being hotly debated. It will force banks to hold more capital, and many argue that this will bring the end of ‘cheap money’. In the US, the Dodd-Frank Wall Street Reform is now signed into law and set to bring a massive overhaul of the financial system.

The regulators are also toughening up. We have seen recently some of the biggest and most public penalties for non-compliance. Société Générale was fined over $2m by the UK’s FSA for failing to hand over accurate transaction reports. It joins a long list of offenders, including Barclays, Credit Suisse, Getco, Instinet and Commerzbank.

So what’s a bank to do?

To meet these regulatory demands, a bank needs to have a centralised, global view of risk. And this requires standardisation across the board. Banks should gather, store and make sense of information from all business lines – on a daily or intra-day basis.

But this is as essential for the business as it is for the regulators because it helps the bank make better decisions. A bank needs to know exactly what its risk exposure is to a company, region or currency, so for example, when cross-selling, it can see where the opportunity lies and where not to over-commit.

To make the most of this capability, banks need to put good governance at the core. This calls for change, both in the bank’s culture and in the way it operates. It involves training staff, introducing new processes and investing in systems that monitor the entire risk process. Finally, everyone needs to think long-
term. A long-term strategy is in place not to appease the regulator, but to create good governance in a wider ecosystem.

Read this article on the website [Click Here]
How do you audit a risk management program?

Posted by Steven Minsky on April 29, 2011

With so many risk management standards and government regulations out there that require risk assessments, how should internal audit evaluate the effectiveness of your organization's risk management program? How would you apply any one of these frameworks to an audit? How do you meet the reporting requirements of so many external stakeholders from regulators to investors to customers to rating agencies?

Challenges with using risk management frameworks:

1. Many standards to choose from: COSO, ISO 31000, Solvency II, etc

2. Recommendations aren’t directly actionable and are vaguely defined

3. No concept of improvement over time

4. Standards are lengthy and abstract

None of these standards have clear auditor guidelines, review requirements, or control recommendations. Because of this, some auditors have begun using risk maturity models developed by consultants, however these models tend to be externally focused on compliance rather than centering around achieving an organization internal goals and performance.

This is where the proven framework known as the RIMS Risk Maturity Model comes into the auditing process.

The RIMS Risk Maturity Model is a collection of best-practices taken from each of the major ERM standards. For each of these criteria it provides clear and actionable activities to achieve these standards as well as risk metrics to track the effectiveness of achievement. The RIMS Risk Maturity Model has been proven to correlate with better business performance as risk maturity increases.
How does internal audit use the RIMS Risk Maturity Model to review risk management?

The RIMS Risk Maturity Model has requirements for five levels of risk maturity for each of 68 core competencies that roll up to 25 success factors, 7 underlying attributes, and one final score.

This allows auditors to quickly assess their organization’s risk management program, identify the top findings that require remediation, and make actionable and practical recommendations with the companion practitioner’s guide.

Review your organization’s enterprise risk management program with clear requirements, clear recommendations, and a focus on your organization’s strategy and achieving results.

Take a tour of the RIMS Risk Maturity Model Assessment today and see how intuitive auditing risk management can be.

Read this article on the website Click Here
An organization-wide risk appetite can be a powerful statement that gives your risk or compliance program direction. However, like any policy, risk appetite without accompanying action is nothing more than an idea.

So how do you give your risk appetite teeth? How do you make it an actionable guide for your organization?

Here are five recommendations to put your risk appetite into practice.

**Translate risk appetite to the process level.**

Every day your front-line managers are making operational decisions about risk, far from your risk appetite policies. This is where income is generated, where employees interact with customers, and where emerging liabilities are first visible.

To successfully implement your risk appetite you need to identify and set risk tolerances at this level of operations; at the front-line process level. This will allow you to connect front-line decisions with your overall risk appetite and determine which processes are out of range.

**Set and measure risk tolerances around root causes.**

Setting risk tolerances around front-line processes isn't enough to truly put your risk appetite into action. You also need to be monitoring root causes of risk at this level.

For example, say your risk appetite sets a low tolerance for customer dissatisfaction and as a goal you aim to increase customer satisfaction. You could goals for a particular customer satisfaction survey. However, this metric doesn't offer any actionable solution to improve customer service.

Instead, go to the root causes of customer dissatisfaction with metrics such as call wait time, email response time, or case
volume. Unlike the results of a survey, these metrics are actionable if they are found to be outside of their defined tolerance.

**Risk metrics need to be forward looking.**

Another problem with our customer service survey comes from the time it takes to compile responses and analyze aggregated results just to be able to make a decision. With a survey you'll always be acting on customer impressions from last month as an effect of last year's policies.

Instead, your metrics need to be looking to the future. Back to our customer service department, case volume, for example, is available as cases are created and will allow you to detect emerging trends long before they have significantly affected your organization.

**Use a risk taxonomy to standardize your risk metrics.**

Underlying risk metrics need to be comparable over time, across levels, and across silos for a risk tolerance to be meaningful.

Using our customer service metrics again, re-opened cases might a good root-cause metric, but it's not comparable over time or across products as the number of total customers will vary. Instead measuring the percent of re-opened cases may be a more meaningful metric as it's value is independent of customer volume and is thus comparable both over-time and across silos.

**Align your risk tolerances with your strategic goals and business model.**

Risk tolerances will naturally develop from your overall risk appetite, but they also need to be in line with your organization's goals. Your organization might define a very low tolerance for customer dissatisfaction, but if you're attracting lots of high cost customers, then this policy isn't in line with a discount business model.
When risk tolerances are aligned with both overall risk appetite and strategic goals, they will both improve risk mitigation effectiveness and contribute to achieving your strategic goals.

To see the power of these recommendations in action, watch this 5 minute video: "Streamlining Governance with ERM".

Read this article on the website Click Here
Japanese Nuclear Crisis: lessons for risk managers

Posted by Steven Minsky on April 1, 2011

The nuclear crisis still unfolding at Fukushima Daiichi continues to threaten a meltdown as core temperatures and radiation leaks continue to fluctuate. The disaster is one of the worst nuclear disasters in history. However the vulnerabilities at the power station are not isolated to Japan or utility companies; they are common risk management shortcomings in operational practices seen in every country and every industry. Here are a few lessons for managers from this crisis.

Link controls to the assets they depend on.

Managers’ often make the mistake of assessing the effectiveness of a single control without expanding the scope of assessment to the assets that control depends on.

For example, the Fukushima plant had multiple backup cooling systems to prevent a core meltdown. However they all depended on a single diesel generator and battery backup system. When the system was discovered to be damaged, battery backup was depleted within hours and the cooling systems were rendered useless.

Managers will have better business results by expanding the scope of risk analysis beyond a control to the systems and assets it depends.

Evaluate risk impact for each business process.

It’s very typical for managers to over-invest in risk controls for one area while leaving other areas widely vulnerable. This over-focus on a single area stems from risk analysis ending at the business unit level without considering how each business process will be impacted.
Japanese Nuclear Crisis: lessons for risk managers

Going back to the plant at Fukushima, while extreme attention had been paid to containing a potential reactor meltdown, the same level of attention was not invested to protect spent fuel. This under-investment in controls for spent fuel pools has lead to highly unstable conditions including radiation leaks and a potential meltdown outside the main containment vessel.

Managers at the business process level have the best knowledge to identify and evaluate the possible impact of a risk. At Fukushima Daiichi that means managers would assess the impact of a natural disaster on for each business process managing fuel storage, cooling systems, backup generators, all the way down to employee performance; not just the impact on reactors.

According to the RIMS State of ERM Report 98% of organization’s fail to assess risk at the front-line. This is a widespread problem for risk management programs in every sector.

**Routinely revisit risk assumptions to reveal emerging risks.**

While executives recognize the business environment is constantly changing, the State of ERM Report shows 86% of business continuity plans are based on outdated assumptions. This leads to outdated controls whose effectiveness may no longer be valid in the current environment.

For the Japanese nuclear plant this means assessing the increased probability of natural disaster stemming from global climate change and updating models based on the latest geological information. Managers need to regularly revisit risk assumptions to prevent controls from becoming outdated.

**Evaluate risk from vendor relationships.**

Every organization depends on partners to maintain key equipment and provide key services under emergency situations. Yet, according to the RIMS report, 96% of organizations today do not cover risks from their vendor partners adequately.

Examples are everywhere, whether you look at the BP disaster and it’s outsourced oil rig from Deepwater Horizon or the
Japanese nuclear crisis stemming from vulnerabilities in the original GE reactor design.

Managers must evaluate how vendor relationships impact every area of operations and what essential processes may depend on these relationships. While a process or a technology may be outsourced to a vendor, you ultimately own the risk.

Risk management isn’t about trying to predict the future, it’s about being prepared in the right places where it matters most. These practices reveal the relationships between risks and activities within processes, and allow managers to spend less time fixing preventable problems and more time reaching their strategic goals.

Read this article on the website Click Here
When risk management is all risk, and no management

Posted by Michael C. Thomsett on May 31, 2011

Most managers have heard that budgets are political documents. As true as this is, when it comes to what gets cut, nothing is politicized as much as the risk management effort.

Risk management, whether in the form of insurance or internal preventive initiatives, is easy to cut because it is not thought of as essential by so many managers. These managers consider risk as something intangible and outside of their responsibility, and probably not even likely to be a threat. Even when these managers know about risk and the need to mitigate or transfer it, they may be willing to take a chance, hoping that a disaster won't happen, at least not within the current budget year.

So what happens when a risk is realized and that all-important budget is left in shreds? What happens to the carefully trimmed budget that reduced insurance coverage, minimized internal safety protocols, and did not finance preventive programs? What happens to all of those corners so efficiently clipped? The projected net profit was promising in that rosy budget, indeed, but a single point of failure quickly destroys all the wishful thinking in the world.

This is when you hear the second part of the reaction. The first part, of course, was "We don't need to pay to prevent something that probably won't even happen."

The second part: "Why didn't you tell us this was going to happen?"

Read this article on the website Click Here
According to Wikipedia, “Best practices can also be defined as the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people.”

There are best practices for identifying and mitigating reputation risk in different types of companies as well as best practices for managing reputation as an asset. Please note that not every environment or every company is the same. Your unique environment may require different configurations in order to provide the best protection results. If you have questions about your environment and would like some guidance on mitigating reputation risk, please contact deonbin@icon.co.za

Like all of the intangible assets whose value has escalated in recent years (other examples are talent, knowledge, know-how and intellectual property), reputation has often been overlooked by organisations because it is so difficult to comprehend.

It is only when a reputation incident severely damages the credibility of an organisation or one of its brands, or its standing in the eyes of its stakeholders, that the potentially catastrophic consequences of not managing the crisis properly become apparent.

Studies of organisations that have handled crises affecting their reputation badly have identified long term and irreparable damage to share price, market share and brand value. Many organisations make the mistake of assuming that all that is needed is media training and crisis planning. However, a reputation crisis exposes to public and media scrutiny not only the organisation's competence at crisis handling, but the values, standards and shortcomings that existed beforehand.
The reputation best practice strategy should, therefore, have two simple objectives - to prevent the causes that could damage your reputation, and to minimise the impact if, despite your best endeavours, a reputation crisis should occur.

Here is a partial list of some of the best practices to consider:

- Develop ways to understand the nature of your reputation
- Design & develop a reputation risk management strategy that can act as a roadmap for strengthening risk management in particularly vulnerable areas
- Work together with PR, Risk and Compliance departments to close gaps
- Develop standards and controls for the action that the strategy places most importance on
- Learn how to proactively manage elements of reputations - Provide reputation management training, education and communication to obtain the vital support and commitment of your employees and managers
- Design analysis and monitoring mechanisms to provide early warning of problems or crises
- Develop a process of continuous crisis assessment
- Conduct regular crisis planning and testing
- Ensure regular reporting and monitoring of reputation risk, including incident analysis, issue management, environmental forecasting and online reputation monitoring.

Some organisations have attempted part of this best practices process themselves, particularly the first few stages. In my experience, they are severely disadvantaged by being too close to the issues, or by risking avoiding taboo or politically difficult areas, or by not challenging assumptions vigorously or objectively enough.

If you would like to learn more about best practices in building, managing and protecting corporate reputation, why not get me to
RISK MANAGEMENT BEST PRACTICES, KNOW-HOW AND HOW TO’S

run one of our learning interventions internally? e-mail reputationeducation@icon.co.za

Read this article on the website Click Here
Developing a risk-conscious point of view in the organization

For the organization concerning with the priorities of budgets, profitability and efficiency, it is easy to overlook the need for simple awareness about risk. The tendency within the finance-dominated organization is to focus only on known profit and loss factors, and not on what future risk truly is, a contingent liability only.

This does not make accounting-dominated organizations negative. There are many sound reasons that accounting and finance should dominate the discussion of cash flow, profits, and internal controls. However, as an ex-accountant myself, I know that most financial folks do not like anything not found in dollar values on the financials, especially if they are not explained even in footnotes. So the potential for exposure to unknown future risks -- the contingent aspect of risk management itself -- is not as compelling (or as easily understood) as revenue growth, profits, and cash flow. These are tangible and easily quantified, whereas the possibility of risk is not. For example, if the question is, What is the cost of a potential future loss? the answer must be, We don't know yet. This does not comfort the accountant, who deals in specific dollar values or at least in assumption-based dollar values.

This conflict between accounting/budgeting and risk management points out why risk-consciousness is in fact the hard sell but also the essential change in corporate culture that needs to occur. This is especially true as the global supply chain expands. Every organization is at the mercy of supply chain risk, even if the organization exists and functions in a very small geographic market. Virtually no organization can function without relying on raw materials, products or labor from elsewhere. Thus, something essential to most organizations arrives through the supply chain.

Risk consciousness should be based on a short list of internal, organizational culture attributes:
1. Top management has to accept and believe in the need for risk management and has to provide all employees and stakeholders with the policy and objective of managing risk, not to mention the budget.

2. All stakeholders need to become involved directly in understanding risk management, not just by identifying specific risks but more specifically, by working with management to determine the steps needed to prevent losses resulting from a universe of risks, and creating a viable and workable disaster recovery plan -- based not just on specific risks but on the losses an organization incurs.

3. This awareness of risk has to be reflected in budgets and priorities within the organization. This applies at every step of the supply chain, remembering that as a chain, the entire process is only as strong as its weakest link.

Read this article on the website Click Here
Risks Managers: What should you report to the Board?

Posted by Steven Minsky on June 20, 2011

Boards are under pressure like never before to assure their organization has an effective risk management program. The SEC, through the Proxy Disclosure Enhancements amendment, is holding them personally responsible for risk management.

If your board hasn't already come knocking on your door for a briefing on the effectiveness of risk management, they will be soon. So the $64,000 question remains:

ERM Reporting: What should you present to the board?

The short answer is the larger picture of risk with a connection directly to the front-line. This is the crux of the problem. As you know, the board makes strategic decisions by viewing your organization from a 35,000-foot perspective. They aren't interested in a list of hundreds of risk indicators, or even the top 10 operational risks.

Your board needs to understand the sources of uncertainty that could impair continuing operations or reaching your organization's strategic goals. The risk is not the event of a lawsuit, but rather the uncertainty that employees are acting appropriately that the board needs to know about. It's not the event of supply chain disruption, but rather the uncertainty of preparedness for changes in weather patterns. The board needs to understand trends in uncertainty, that is the larger risk picture, on the commitments they have endorsed.

Sounds simple enough, so how do you assemble this information?

You need to take these big picture issues one by one, and connect them to the real activities that materially contribute to each issue.

How to connect operational risks to strategic goals:

1. Choose one of the board's strategic imperatives.
2. Identify the business processes that contribute to that goal.

3. Assess the root cause of risk for each corresponding process.

4. Connect the corresponding risk assessment templates to that strategic goal.

5. Repeat steps 1 through 4 for each of the board's strategic goals.

6. Report the impact of risk on each strategic goal to the board.

Any one of these steps can be a challenge for risk managers. Find out how ready you are to present to the board, evaluate your risk program with the RIMS Risk Maturity Model Assessment.

You can also learn more about what the board requires by watching this on-demand webinar What is Strategic ERM?

Read this article on the website [Click Here](#)
What is the risk awareness in your organization?

Posted by Michael C. Thomsett on June 17, 2011

A starting point for any risk management program should be awareness. No matter how evolved a program you have, and no matter how much effort has been invested in education, risk managers are continually up against resistance on many levels: executive, budgetary, priorities, and worst of all, lack of awareness.

Several attributes of a risk-specific program help overcome the lack of awareness. However, risk managers also need to accept the reality: Many people within the organization do not want to be aware of risk, because (a) it is "not their job" as the belief goes, (b) not all risks can be prevented or mitigated, and (c) it's not in the budget.

So as a starting point, here are four questions risk managers may ask in order to better understand how and where to start:

1. Is your organization's risk policy defined and does management agree on a policy of dealing with risks?

2. In the course of planning and budgeting, is the idea of risk introduced and discussed as part of that process?

3. Does management appreciate the different perspectives of suppliers, employees, vendors?

4. Has management set a theme of risk and integrated it into their programs (market expansion, budgeting, transparency, compliance)?

Chances are that your organization does not have a defined risk policy, or at least not a strong one. It is equally likely that your budgeting process, even if advanced and aimed at cost controls and improved profits, does not contain elements specific to risk management. Executives may not understand stakeholder risk priorities at all and may even never have been asked to think about this crucial issue. Finally, it is highly likely that the concept of risk integration has never been raised in any context.
In other words, even with advances in technology and globalization, organizations and leaders may continue to ignore or be unaware of the level of danger the organization faces - because ranges of risk are ignored or discounted.

Read this article on the website [Click Here](#)
Risk evaluation - getting around the budget issues

Posted by Michael C. Thomsett on October 28, 2011

The greatest problem for risk managers may be resistance from top management, based on their focus on budgetary issues rather than on risk exposure. Rather than asking "What are the risks?" so many instead ask "What does it cost?"

Let's face it, the finance departments influence decision-making, and for good reason. The balance between expenses and profits relies on making choices. Management looks for ways to cut expenses, and risk management seems an easy target. After all, that catastrophic event probably won't happen, right?

Risk managers know the frustration of battling this mentality. Three ways to make your point:

1. **Prioritize risks in terms of cost/consequence.** The "grid" of risk has four parts: high-risk and high-cost, high-risk and low-cost, low-risk and high-cost, and low-risk and low-cost. By categorizing risks in these four areas (high-high, high-low, low-high and low-low), you can more convincingly make your case for focusing on the high-risk and high-cost areas where the risk dollars spent provide the greatest protection. Realistically, the company may need to self-insure or transfer many of its risks.

2. **Create internal evaluation and educational teams.** You can educate management, not be demanding that they attend workshops you sponsor, but by creating small teams to evaluate risk and then report to you. The information you bring to the budget committee is much more convincing when its conclusions are developed by a team, and not just by you. Use the Six Sigma model to create analysis of the most serious risks, and ask the team to propose risk reduction methods, areas for transfer, and of course financial resources.

3. **Look for a balance between investment and mitigation.** It may be a risk manager's job to ask the company to devote budgetary resources to fight risk. But this is most effective
when combined with mitigation and preventive methods. This may include internal processes and controls; relatively easy steps to identify the supply chain's weak links (often found where goods and processes pass from one department or segment to another), and relatively small budgets for big risk reduction.

The risk universe is overwhelming if you try to read it all at once. But like a long book, if you take it one chapter at a time, and with these small ideas in mind, you may be able to make some headway through the budget committee.

Read this article on the website Click Here
Lack of knowledge means more uncertainty means greater risk. Assumed knowledge can be even more dangerous than lack of knowledge and risk workshops are a safe haven for assumptions because of time limitations and dominant personalities. Here are four sources of assumptions with some tips on how to handle them during a risk workshop:

1. Seniority - When you have senior people in the room, too many people assume they are right, or will give them the benefit of any doubt in their mind because of their seniority. If a senior person is making an emphatic point, pause the session immediately afterward and ask the room if they agree and survey the room for anyone looking like they are holding back and ask them specifically for their opinion - you will often be surprised with the result.

2. Research Vacuum - Too many people perceive research as too hard, too costly or both. Help the group to identify where there is most uncertainty in their risk assessment and ask them what it might be worth to be more certain about that risk. They then have a maximum budget for research that they can look into using. Sometimes a few "outside the box" suggestions are needed to get them thinking about how they might find some answers within the budget.

3. Historical Inertia - "This is just the way things have been and they have worked alright up until now". A classic comment which may be entirely valid (see next point), however, it must be challenged even if the environment is changing just a little bit. Start by asking what the results were of the latest "environment scan" for their business unit. This often shakes a few thoughts loose.

4. Change Agent - Quite the opposite of historical inertia; some people assume change is necessary because they perceive themselves as a "change agent". Sometimes "if it's not broken don't fix it" overrides the need to break historical inertia. At
worst suggest the need for a risk assessment of any major changes after the workshop. Where time permits, do a mini risk assessment of the suggested changes then and there.

Read this article on the website Click Here
5 Steps for Better Risk Assessments

Posted by Steven Minsky on October 21, 2011

Risk managers are charged with ensuring transparency, alignment, and forward looking views throughout the organization. The way this is achieved is through risk assessments.

Successful enterprise risk assessments can be a powerful tool for board and management level strategic decision making by connecting business activities to goals and identifying the risks that threaten to derail these strategic objectives. An unsuccessful risk assessment is little more than a form over substance activity that lacks context and actionable results.

So, how do you implement a successful enterprise risk assessment?

The key is being able to compare information across functions and levels while keeping one comprehensive risk picture.

1. **Standardize your Risk Assessments Templates** - Activities like vendor management, business continuity, compliance, IT, financial reporting, operations, internal audit, and others are all informal risk assessments. When these assessments are carried out on the same standards and assumptions, defined in a taxonomy, they can be compared and utilized cross-functionally.

2. **Common Root Cause Risk Identification Approach** - Risk managers should provide a common root cause risk library to process owners so that when multiple areas chose the same risk, systemic risks as well as upstream and downstream dependencies can easily be identified and mitigated. This method also identifies areas that would benefit from centralized controls so the extra work of maintaining separate activity level controls is eliminated.

3. **Performance Management: Alignment of Activities, Goals and Risks** - Risk managers need to tie root cause risks to strategic goals and trace these same risks through the process areas that they affect in order to determine which activities
will roll-up to impact organizational objectives. Once these connections are made clear, risk managers are able to prioritize the effectiveness of controls, so that resources and focus are allocated to the issues that will yield the greatest benefit to the organization.

4. ERM Reporting: **Group Information for Multiple Stakeholders** - Because assessments are conducted on the same standards and assumptions and risks are identified at a root cause level from a common library, process owners can do one risk assessment, and the information can be sliced, diced, and aggregated to serve multiple purposes. It will provide a functional insight for the process owner, tie into governance areas like vendor management, and serve a strategic purpose by rolling-up into board level objectives.

5. Risk Appetite: **Timing and Trends** - Risk assessments must be conducted on a regular basis and when approaching business changes, new initiatives, or high risk issues. Being able to view the trends over time gives the organization's static risk profile context and a reference point so that necessary actions can be taken when you start seeing small changes in your risk profile before things get out of tolerance.

To see these best practices in action to uncover changes in risk to prioritize controls, tests and business metrics, watch this 5 minute video.

Read this article on the website [Click Here](#)
Risk assessments are plagued by subjectivity which means they simply cannot be relied upon to meet their objective. Subjectivity prevents risk assessments from being used across business silos and makes verification by audit or compliance review impossible. Subjectivity can be overcome by using a risk assessment template framework with the following best practice attributes:

1. ** Adopt a uniform numerical scale** - Use a scale of 1 to 10, Scoring is based on a scale from 1 to 10, with 10 having the most unfavorable consequences to the organization, split into 5 buckets to provide a high and low of each bucket. (1-2, 3-4, 5-6, etc). Using a 10 scale makes the math easy and having only 5 buckets gives folks doing assessments flexibility to select the high or low of the 5 buckets.

2. **Define objective evaluation criteria** - Often, one person's 9 is another person's 7. You need to provide clear definition on what each of the 5 buckets are in unambiguous terms. You can chose multiple ways of expressing severity, both qualitative and quantitative, such as financial, legal, strategic, etc., yet only one of the criteria listed for a specific level has to be met in order to rate a factor at that level. Any set of standards can be compared, including laws, regulations and corporate policies and procedures, with current practices. Any qualitative criterion can be given a score to become quantitative and comparable across the enterprise.

3. **Calibrate risk assessment criteria** - Although a variety of assessment criteria is used, all these should be on a 1-10 scale and calibrated, meaning that the description of a 7, even if described differently in different risk assessment criteria has the same meaning of severity. This allows the aggregation of risk assessments to provide a holistic view of risk.

4. **Use universal business elements** - Break down risk assessments into basic elements like business processes and resources that are standardized across business silos, or
business units. Risk assessing vendor characteristics separately from the products and services they sell will produce risk assessments that make it easy to identify and maintain objectivity as changes occur like mergers and acquisitions or new product introductions, etc..

5. **Link risk assessment templates** - Link elements together, meaning connect vendors to the products and services they provide to the business processes that rely upon them. Link each financial element to the business processes that contribute to them. Link all of the internally developed applications and data repositories to the business processes that rely upon them to perform their responsibilities.

Linking these elements together enables risk assessment data to then be easily aggregated and reported using these linked relationships to provide a holistic picture of all your risk assessment template results. For example, a vendor can have multiple products and services of different quality and risk. Risk assessing the products and services individually and linking those risk assessments to the vendor profile provides a much clearer picture on the combination of products services and vendors used by a processes owner.

The result is a single overall summary score for each business process that combines the individual scores for each resources and financial item associated with that process and the process score itself. With this information, you can prioritize and focus your ERM efforts.

Click here to download a free risk assessment template you can use to organize your existing ERM Program information as the next step to centralizing all your ERM program data.

Read this article on the website [Click Here](#)
Paint Draw Pick... to Implement Enterprise Risk Management across your Organisation

Implement Enterprise Risk Management across your organisation no matter where you are on your Risk Management journey by taking these 7 steps:

**Paint a Picture:** Make sure you can show and explain what the end game looks like to top management and staff.

**Draw the Journey:** Let them know they are on a journey, describe it and tell them where they are right now.

**Pick the Low Hanging Fruit:** Don't try and win everyone over at once. Get going with those most likely to convert.

**Find your Risk Champions:** Develop a Risk Champions Committee - not THE Risk Committee, but a committee of managers who report on Risk to the top and who tailor your Risk Framework.

**Give on the Job Training:** Risk Management is best learned on the job. All training should be highly practical and as short as possible so you maximise attendance.

**KISS:** Keep it simple stupid. Although it is not simple, make it as uncomplicated as possible. Try to use business rather than risk terminology and modify existing processes and systems rather than create new ones.

Climb the Mountain: Generally the CEO/Board are not low hanging fruit. They may be strong leaders, but not Risk Leaders. Work up to them. Engage them early by using the steps above so that they buy in, then WIN THEM OVER so they are true Risk Leaders. It takes finesse.

Read this article on the website [Click Here](#)
Using Risk Assessment Templates to Prioritize Business Measures

Posted by Steven Minsky on December 7, 2011

The number of business measures within organizations is typically growing. Measures are often added on a reaction basis to loss events that have already occurred. Wouldn't it be valuable to be able to focus on forward looking measures? In most organizations, these preventative, proactive measures are indistinguishable when grouped with reactive measures, because the metrics do not formally tie back to any commitments or risks.

What if a risk or activity changes? Organizations have no way of knowing how and if these changes will affect their risk metrics. Risk Assessments and linking risks to activities allows organizations to start prioritizing what activities need to be monitored. Through regular quarterly, or even annual, risk assessments, organizations can detect increased threat levels and identify new emerging risks before they materialize and bring your business metrics out of tolerance.

Business measures are important because you cannot improve what you cannot measure, however this large number of unconnected goals is problematic because:

- **Measurement fatigue** - staff may simply ignore many measures because of a lack of time to assess them.

- **Measure obsolescence** - in a changing environment there is no effective way of knowing when measures no longer apply.

- **Lack of prioritization** - picking the measures to focus on is likely to be on an ad hoc basis and upon the whim of current staff.

- **Lack of continuity** - changes in the organization or the development of new lines of business may result in new measures while existing measures may be more effective.

- **Lack of coordination** - often measures apply to multiple risks or commitments across functional lines. The inability to formally tie
measures to risk or commitments does not promote inter-functional coordination resulting in business silos and duplication of effort.

- **Wasted resources** - The amount of resource available to accomplish business goals and to mitigate risk is finite. Staff will often continue to manage to obsolete or unimportant measures rather than aligning with current imperatives.

- **Resistance to change** - A difficulty to apply past experience to a changing business environment resulting in a tendency to "reinvent the wheel".

Much of the necessary information exists in organizations today; the missing piece is formalizing these critical connections. Enterprise Risk Management (ERM) software has functionality to identify risks and commitments; assess them based upon likelihood, impact and assurance; evaluate whether action is needed; devise mitigation or business building activities if needed, specify and record measurements to track effectiveness, and finally formalize the connection between all of these activities.

Connecting the measurements to the risk mitigation activities and business initiative data and then back to the underlying risk and commitments will provide the following benefits:

- **ERM Reports**: Explicit prioritization of measures based upon a risk/reward index and a dashboard presentation on the heat map dashboard in LogicManager.
Operational Risk Management: Real-time trending of measures on an ongoing basis with measure consolidation used to direct management attention to problem (out of tolerance) conditions.

- **Risk Assessment Templates**: Allow for rational elimination of measures that have low priority or non-existing connections to risks or business initiatives.

- **Performance Management**: Facilitate new business initiative business measurements prioritized upon risk or business commitments.

- **Resource Allocation**: More effective use of scarce resources. The key is working with the functional managers to make the connections. The immediate benefit will be to identify measures that are not connected to any risk or initiative and to determine if they should be eliminated. Then, once the connections are made, use the management tools in your Enterprise Risk Management software on an ongoing basis to improve utilization of business measures within your organization.

- Watch a complimentary 5 minute video to learn how to link risks to business measures.

Read this article on the website [Click Here](#)
How to measure your Enterprise Risk Management effectiveness

I am often asked for insight on business measures or KPIs for ERM programs to track overall progress and effectiveness.

The key question for risk managers is: how do I measure the value ERM is delivering to my organization?

The following are examples of measures that will quantify and measure the value your ERM program is providing:

Number of systemic risks identified

- Systemic risk identification will detect areas of upstream and downstream dependencies throughout your organization, such as when one area of the organization is unknowingly causing strain on other areas. Additionally, this method could also identify areas that would benefit from centralized controls so the extra work of maintaining separate activity level controls is eliminated, increasing organizational efficiency.

Percentage of process areas involved in risk assessments

- ERM is cross-functional in nature and cannot be done in silos. A business is the sum of its parts. The same is true of risk. A risk event in one functional area also affects other functional areas within the business. Process owners own the risk; risk managers own the completeness, timeliness, and accuracy of the risk information. The more process owners involved in risk assessments, the more accurate and forward-looking the information collected will be, both of which are hugely valuable to the organization.

Percentage of key risks mitigated

Having a sense of your overall risk coverage is important; however, it is not nearly as valuable as knowing the coverage of your organization’s key risks. Because all risk assessments should be conducted on standardized criteria, you can determine a uniform tolerance, or cut level, throughout the organization based on the resulting assessment indexes. This will help you to prioritize resources to the risks that need stronger coverage,
rather than wasting resources on risks that will have no major impact on your organization. This gap analysis with a tolerance level will also help you to identify emerging risks as they rise out of tolerance and it becomes clear that some mitigation activities in place are no longer sufficient.

**Percentage of key risks monitored**

Most organizations have no understanding of how the business measures that they rely on daily are tied to their risks. If a risk or activity changes, organizations have no way of knowing how, and if, these changes will affect their metrics. Through risk assessments and linking risks to activities, organizations can start prioritizing what activities need to be monitored. Regular risk assessments enable organizations to detect increased threat levels and identify new emerging risks before they materialize and bring business metrics out of tolerance.

Watch a 20 min On-Demand webinar “Streamlining Governance through ERM” to learn how to measure risk management effectiveness.

Read this article on the website [Click Here](#)
Risk taxonomy is the framework of naming, organization and managing the relationships to manage your risk information. Your ERM program and any Enterprise Risk Management (ERM) software you use depends upon it.

Most organizations have an organizational chart of how their people are connected. To be effective in risk management, organizations must also have an organizational chart of how their business processes are connected to create accountability and focus on business value.

The first step is to name, categorize and connect your business processes and sub-processes.

• **WHY: Establishing business process level accountability for risk:**
  The foundation for enterprise risk management is identifying an organization’s business processes and recognizing the owners as accountable for risk vulnerabilities, compliance and performance goals.

  Because all business activities are within business processes, all risks and mitigation activities also fall within processes. Therefore, defining processes is the first step in leveraging efficiencies and creating transparency for risk management, compliance and business performance improvement.

• **WHAT: Focusing on business value with Performance Management:** A business process is a set of coordinated tasks and activities that lead to accomplishing a specific organizational goal. Business processes include customer facing areas, those providing support functions as an internally shared service, or areas performed by an outsourced partner.

  End-to-end processes consist of multiple levels of sub-processes. The level of granularity, meaning the extent to which processes are broken down into smaller processes, evolves over-time. You may choose to get granular in areas of greater priority to the company and fill out the others over time.
WHERE: Consolidating existing risk assessment templates: Business Processes names, structure and their owners are typically already known within an organization and maintained by various functional areas such as finance, internal audit, HR, business continuity, process improvement, quality management, or other departments. There should be only one way to call and organize business processes enterprise wide, otherwise known as a taxonomy or naming convention. The ERM team has the responsibility to locate these lists and agree on a common single naming convention for the enterprise.

Definitions:

- **Business Process Owner:** the individual(s) responsible for process design and performance. The process owner is accountable for sustaining the gain and identifying risk and future improvement opportunities on the process.

- **Risk Owner:** the individual who is accountable for the validation, assessment and action plan to care for particular risks within the process.

The Process Owner is typically the risk owner. When is this not the case? When the business process is outsourced. Activities can easily be outsourced, but the ownership for the risks within such activities can never be outsourced and must remain managed within the organization.

The next step in building a risk taxonomy is managing resource allocation, the naming and categorizing of all the key people, systems, and vendor products and services used by these business processes.

Look out for my next blog on these topics! In the meantime, watch a complimentary 20 minute webinar: Streamlining Governance through ERM to learn more.

Read this article on the website [Click Here](#)
Organizations need to build a robust Enterprise Risk Management (ERM) framework or risk taxonomy, which provides a holistic view of all information and relationships across the organization. Taxonomy structures and preserves the integrity of information, so as changes occur in multiple parts of the organization, managers can compare risks on an 'apples to apples' basis and connect the dots between business areas. It is the critical foundation of your ERM program and any enterprise risk management (ERM) software automation initiative.

As I described in my last blog, the first step to building a risk taxonomy is identifying your organizations core business processes to create accountability and focus on business value.

The next step in building a risk taxonomy is to enable better resource allocation by the naming and categorizing of all the key people, systems, and vendor products and services used by these business processes.

Organize risk assessment templates by resources vs. by use or department

To make effective Enterprise Risk Management (ERM) simple and practical, you need to take complex material, break it down, and make it accessible for anyone in your organization. To do this, information should be organized by resource rather than by use or department, and organizations need to create a holistic profile for each critical resource in your enterprise.

By resources, we mean people and vendors and the physical assets, software applications, services and data repositories used in the organization. Everyone knows something about the relationships and data around these resources, but no one knows everything. The challenge is how to get everyone to contribute their "piece".

A risk taxonomy, provides a structure for information and ownership, by breaking down complex interconnected...
information into resources as basic building blocks. This enables everyone to understand and contribute their piece and take ownership for change management. These standardized building blocks become a library to be shared across all business areas and reduces unnecessary duplication and overlap.

2. Performance Management: Link resources to the Business Processes that use them

The relationships between the resources and the business processes that use them should be explicit as this determines business impact. The more clear the understanding of business impact, the more effective the governance activity will be. The connection to a business process provides a direct connection to the subject matter expert for the activity that uses the resource and knows the criticality of that resource to their activity.

The result is the identification of critical business processes based on a score that includes these key supply chain and infrastructure dependencies. Control and mitigation activities can then be organized within the business processes in which they operate and are connected to the resources they depend upon to complete this circle.

A common shared infrastructure, or risk taxonomy, is necessary to support risk management information across an entire enterprise. Through this approach, organizations will see the benefits of eliminating redundant work on assessments, controls and testing while reducing risk at the same time.

The next steps in building a risk taxonomy is standardizing risk assessment template criteria for these resources and processes, consolidating data collection, and understanding cross-silo dependencies.

Look out for our next blog on these topics!

Read this article on the website Click Here
Risk Taxonomy Step 3: Managing Cross-Silo Dependencies

Posted by Steven Minsky on March 21, 2012

A risk taxonomy, the brains of an enterprise risk management software platform, creates a common language to make working across operational silos possible. It also creates the basis for a risk management discipline, so rather than reacting to seemingly "one off situations" the entire organization can standardize and prioritize how assessment, mitigation and monitoring are applied in a common comparable way to build risk management competency across the enterprise.

See our other blogs Identify Core Business Processes and Link Resources to Business Processes that explain steps 1 and 2 of building your risk taxonomy.

**Standardize assessment criteria and weightings for Risk Assessment Templates**

Common standards and assumptions makes information collected across the organization objective, quantifiable and comparable, enabling better analysis, issue resolution and issue escalation when necessary.

**Rationalize and consolidate risk assessments and data fields**

Different areas across the organization are collecting the same information for resources, they just don't know it. For example, Accounts payable, contract management, vendor management, business continuity, and IT all collect overlapping information about your vendors. By understanding what information is being collected by these areas for each resource, you can easily rationalize and consolidate assessments and data fields. You can gather information across silos and identify areas where controls and tests can be consolidated.

**Make resource allocation available in a central place as a library**
Using information from one common place makes it possible to dramatically reduce rework, especially collecting and managing information, for both you and the process owners you work with.

**Formalize risk identification of resource dependencies to each other**

The library also helps you know who else is connected to the same information. The key is to figure out how all of these resources are related to each other and what combination of these resources are most important to critical areas of your business.

By connecting activities, or controls, to the vendors and other resources that activity relies upon at the business process level, the process owner and the activity owner can now be notified when resources change, both directly and indirectly, related to their areas of concern. This is a major contributor to business performance management and the value add of enterprise risk management.

Typically people in organizations only know one degree of separation in relationships. A risk taxonomy enables you to recognize all the relationships and notify appropriate related parties on changes, both direct and indirectly related to their area, so no one misses the "memo." Direct relationships are always known, it is the indirect relationships that are more problematic and hard to control.

Look at BP for example, the vendors were not in connection with each other or the processes owners involved. People were missing key pieces of the "memo" reporting that there were issues, so no one could put the puzzle together. In days were outsourcing of vendors and activities is becoming so extensive and complex, how do you maintain the connections between the risks encountered by your vendors and your business risk and control owners throughout the organization?

**Why did the CEO of BP get fired? Lack of establishing effective monitoring of risk!**
By building a risk taxonomy to define resources and their relationships, along with implementing common standards and assumptions across your organization, everything becomes comparable and objective -- everything is on the same scale. You can analyze, report, and make decisions taking into consideration every relationship related to the resource or process across the organization. This is how risk tolerance is aggregated and matched to the organization's risk appetite!

Watch our 5 minute video: Strategic ERM to learn how you can link your risks, processes, and resources in your risk taxonomy to your organization's strategic goals and key concerns to grow more strategic over time.

Read this article on the website Click Here
Top 5 Project Risk Management Practices

Project change management involves new IT systems, new products, and new markets, or reacting to a change in the business environment, such as regulatory or competitive actions. Project risk management is about identifying new risks or changes in the threat level of existing business processes. The challenge for project managers is how to get teams, functional areas, business processes, systems, and vendors aligned to new goals; moreover, how to get the needed transparency into the activities that have been agreed upon in project execution and how to prioritize the issues that surface every step of the way, until the project is completed. Project risk management is all about using project risk assessments as a method to gain a holistic view of risks across functions and silos. A project management office (PMO) needs this holistic view of risk to help serve their clients, which involves coordinating with multiple stakeholders and many moving parts.

The benefits of imbedding project risk management are specific and measurable. The PMO can reduce budget overruns and missed deadlines— their biggest concerns—if uncertain project events are dealt with in a proactive manner, directly translating to the organization’s bottom line. Helping the PMO to formalize their risk management practices dramatically reduces the team’s stress of “fighting fires” by repairing damage due to preventable risks before they manifest.

**Step 1: Formalize Project Risk Management:** Every project manager is already using risk management techniques in their job informally. Relay to project managers that not formalizing this existing work with methodology and software is as inefficient as doing project schedule in their head as they go along and not using a Gantt chart software package. Studies have shown that formalizing risk management reduces overall project management task work by 30-60%.
**Step 2: Project Risk Analysis:** Risk managers can help project managers very early on in their process. The first step in project risk management is to identify the risks that are present in projects. A root cause approach enables managers to understand the cause of risk and connect this to the effect of not managing this risk.

Failed projects show that project managers were frequently unaware of the root cause until it was too late. The frightening finding is that frequently someone in the project actually knew the root cause, but didn't have the structure to inform the project manager of the issue. Risk Managers can provide PMOs with this missing structure and methodology.

For example, a major concern for project managers is “Missed deadlines/project cost over-runs,” which is the outcome, or effect, of a particular risk. The key is to help them figure out what the cause of this outcome is, of which there can be many. Until the cause is identified, it will be hard to know what action needs to be taken. Not using root cause techniques will result in risks identified like, “Schedule rigidity,” which does not provide them the ability to determine where the source of the schedule issue lies - is it a people, process, system, or vendor issue? Each of these sources of risk can cause schedule rigidity, and until they know which of these categories is causing the issue, action is still unclear. Risk Management software can provide project managers a library of root cause choices such as, “Stakeholders unwilling to act or move,” which let’s them know it’s a people problem verses “Inefficient, non-value added workflow,” which let’s them know it is a process issue at hand to prompt project managers to think about the type of risk which greatly simplifies the important step of acting on the risk.

**Step 3: Prioritize with project risk assessments:** As risk managers know, treating all risks equally wastes a lot of time and effort. Some risks have a higher impact and greater likelihood of occurring than others. Through formal risk assessments, risk managers can help project management offices prioritize where time and resources are better spent based on the risks that can cause the biggest losses and gains. By giving them standardized
enterprise-wide evaluation criteria that applies to all risks and all projects, they will not only be able to prioritize risks within each of their projects and be able to prioritize time to the tasks associated with the largest risks across all of their projects; but their assessments seamlessly integrated into your ERM efforts. You can find risk assessment template guidance here that explains how to standardize your assessment criteria to prioritize risk.

**Step 4: Business process improvement:** The structure that risk management offers provides the ability for project managers to make clear who is responsible for what risk. The solution is simple: based on the priority score of Step 3, they can assign a risk owner for each high risks and goals that have been assessed. The risk owner is the person on the team who has the responsibility to plan activities. Ownership also exists on another level; if a project threat occurs, someone has to be held responsible. This sounds logical, but it is an issue that has to be addressed before a risk occurs, especially if different business units, departments and suppliers are involved in the project. An important side effect of clarifying the ownership of risk effects, is that line managers start to pay attention to a project. The ownership issue is equally important with project opportunities.

**Step 5: Project Risk Management Software:** Some project managers think they are done once they have created a list with risks and mitigation activities. The real value risk management provides is achieved by using those risks to get transparency into the true progress of a project, which is challenging. For example, 50% expenditure of budget or time does not necessarily translate into 50% achievement of goals. Progress means mitigation of the risks, achievement of the goals, and compliance with regulatory or internal standards.

Unfortunately, lots of project teams struggle to cross the finish line, being overloaded with tasks that need to be done quickly. Helping them to connecting activities to the risk assessment of Rule 3, means that each of these tasks will get a “priority score” that helps project managers to understand what is most
important for follow-up to mitigate risks and achieve goals. Managing risks helps to focus on the current situation of risks and goals. Has the relative importance of risks or goals changed? Project risk management software answers this question and helps project managers pay attention to what matters most for their project to deliver business value.

The 5 risk rules above give you demonstrate how enterprise risk management techniques and software provide a structure for business process improvement throughout the organization to gain efficiency and quality improvements.

Watch this 5 minute video on streamlining and improving governance activities, like project management, through ERM. Risk management is all about getting clarity on where your organization currently stands and measure the effects of efforts to continuously implement improvements to make it even better.

Read this article on the website Click Here
The first shoe to drop was government regulations holding the Board of Directors personally responsible for the effectiveness of enterprise risk management programs at their organizations. Boards are given a choice between proving their risk management programs are effective or disclosing their ineffectiveness in risk management to the public. If they do neither, it is considered fraud, as not knowing about a risk is no longer a defense.

What does enterprise risk management effectiveness mean? Not being involved in the day-to-day running of the company where most operational risks actually occur means Boards of Directors must, through their risk oversight role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are effective at identifying all risks and demonstrating assurance over the most material ones.

Risk is viewed at its highest level by the board. Some people make the mistake of inferring that this risk information should then also be collected at only this high level, but this is ineffective because of the gap between senior management and the front line activity level where risks first arise. The key to determining the effectiveness of a risk management program is the ability to collect risk information from the business process-level and
aggregate this information, while preserving the effects of related upstream and downstream dependencies.

Since the liability for error is so high, Internal Audit has now been tasked to do the fact-checking on the risk management information being presented to the board to ensure its integrity at the front line business process level. The Institute of Internal Auditors (IIA) announced this week it has revised its International Professional Practices Framework (IPPF), effective Jan. 1, 2013. These mandated changes require auditors to validate the most timely and most significant risks, especially those that impact the achieving of the organization's strategic objectives.

The role of the enterprise risk manager has now finally become clear to close the gap between strategic level risk and all the operational risks at the activity level at the front line of organizations. The risk manager is responsible for setting the standards, practices and procedures for effective risk management and embedding them in all existing business processes. The risk manager is now accountable risk metrics. This requires putting a mechanism in place to collect this risk information at level where most operational risks materialize and aggregate this risk information to a level the Board cares about, while preserving the links to the front line and the resources involved and then tie together the risks in related business processes--all at the activity level so an audit trail is clear for internal audit to follow.

Organizations have realized that their board level attestations on the effectiveness of risk identification and assessment can no longer just be a facilitated interview at the senior management level; instead, there needs to be a rigorous process at the activity level through the lens of what is material, not just in isolation of a single business silo, but overall as all the pieces come together at the top. The goal is to identify and objectively assess operational risks and ensure risk mitigation is in place at the activity level independently and then collectively. This integrity of this risk information needs to be preserved when aggregating and summarizing by the strategic goals of the organization.
A ERM Software or GRC Software with a risk based approach is the only way this process will work effectively and the RIMS Risk Maturity Model spells out each of the 25 requirements that must be met to put a risk taxonomy in place for an effective and efficient enterprise risk management program that meets the rigor of compliance and now internal auditors review.

Read this article on the website Click Here
I have had some very interesting conversations lately with Boards, Senior Managers and Risk Managers about risk appetite. Here are some insights:

Describing what we mean by risk appetite: Risk appetite is risk speak, however, it can be easily explained. With private sector firms I tend to describe using dollars as the example - "How much capital are you are willing to risk to try and make your forecast profit?" For not-for-profits I tend to bring it back to values - "What are you willing to do to achieve your mission? What would you not do?" And for the public sector I tend to use their number one objective in their corporate plan - "What are you willing to do to achieve your number one objective? Would a few minor adverse audit findings be OK? Would you be prepared to weather the storm if the media ran with a story about your methods?"

Why risk appetite is important in risk management: I find putting risk appetite in context with how it is used when assessing risk is quite important. I use the example of crossing the road. The objective is the same, however, there is always a reason (running late for a meeting, running late for a hot date, to save your 4 year-old child from being abducted by a stranger). Your willingness to get to the other side based on your assessment of difficulty level to cross the road is an expression of your risk appetite.

Risk Appetite Statements: While risk criteria in the form of likelihood and consequence tables and a risk matrix are valuable expressions of risk appetite, staff who were not involved in the discussions that formulated them are not aware of all of the thinking behind them. Providing additional commentary on each category of risk and on the core corporate objectives will communicate a much clearer message to staff as to what constitutes acceptable behaviour.
Can a computer virus make you ill?

How can we plan for a risk that is not even known? The answer, of course, is that we cannot. Planning by nature has to be aimed at managing losses resulting from unknown and unthinkable disasters.

For example, an organization needing to protect its proprietary assets may be wise to diversify its storage and even access to counter potential losses from cyber attack, industrial espionage or internal sabotage.

What happens when the entire system is down for an extended period of time? In the early days of computerization, companies used to employ a back-up consisting of old-style hand entry and storage of data. I can even recall working for a company in which my manager gave me a massive monthly print-out from the “computer department” and had me check the math. The trust level in those days was low, and managers did not understand what computerization was all about. Today back-up has to be more comprehensive and sophisticated, but we still need it.

Are we better off today? Maybe not. Everyone knows how online and IT stuff works, but from the perspective of risk management we are more vulnerable now, not less. We are so dependent on automation for so much, that a system-wide failure makes us helpless and robs us of even the most basic information.

I have focused in past blogs on the potential threat of pandemic as both a health and supply chain issue. But perhaps the next pandemic threat will come from an online infection and not from an actual viral or bacterial attack. A few years ago, I saw a letter written to a local newspaper from someone who had heard about a computer virus. The writer asked, “Can this make me and my family sick?”
Can a computer virus make you ill?

It might sound funny, but as it turns out, it could be the most important question risk managers can ask, especially when it comes to protecting IT assets.

Read this article on the website Click Here
Striking the balance in data governance

Posted by Norbert Boon on September 13, 2010

Despite recent news reports that the Basel III liquidity requirements are to be pared back, financial institutions are still facing vast regulatory challenges. They already have to hold more capital and liquidity, as well as report on this daily. Going forward, institutions will also have to demonstrate the processes and controls used to put together reliable information. Never before have risk and data management been so interwoven.

The real challenges facing institutions looking to showcase their transparency to regulators are the problems that result from siloed business units and manual processes. These can result in institutions not being able to determine a good instrument price from a bad one, or even tell who issued the instrument in the first place. If they can’t do that then they certainly can’t demonstrate independent pricing. Furthermore, data management often falls under the responsibility of IT. However, all too often the IT department doesn’t have the specific front and middle office insight needed to ensure that data is managed according to business requirements.

Let’s not forget what’s at stake if data governance fails – sure, the fines can be large, but it’s the increased capital margins entailed in not being able to demonstrate compliance that really hurt. Also, throwing money at the issue and massively boosting compliance costs is not necessarily an option at a time when budgets are so severely limited.

So what’s the solution? Institutions need to take a business process-led approach to data governance, based on the principles of independence and transparency. Incorporating business rules into data management is a must. These rules or service level agreements will be specific to the bank – such as guaranteed delivery times of prices from specific countries. Right now, most banks haven’t yet joined this up to the data management process, which is what makes it so difficult to determine what went wrong or gain an early warning of potential issues. As a result, what
Striking the balance in data governance

could have been addressed as a small discrepancy often snowballs into a big problem.

Equally important is being able to draw up a full audit trail of the data. This should not only show exactly where the data has come from, but must also provide real-time information about all data events, such as errors, new product take-ons and model updates. Continuous monitoring for data governance of the whole, and preferably centralised, process is also paramount. In taking this measure, banks will achieve better compliance and drive down operational risk by giving business users unparalleled transparency.

These best practices – particularly if conducted across price, reference, counterparty and corporate actions data – are key to mastering the compliance and competitive balancing act. If institutions act now and get this right, they will not only comply with these increasingly stringent regulations, but also reduce their risk and capital overhead.

Read this article on the website Click Here
Identity and Access Management (IAM) – Thoughts

It’s high time for big enterprises to realize the importance of identity and access management (I&AM) technology as an integral part of their security footprint. Even though I&AM is in the limelight for quite long time, still I believe it’s a relative new term that means different things to different people.

What is Identity and Access Management (I&AM)?

As Wikipedia says, “Identity management or ID management is a broad administrative area that deals with identifying individuals in a system (such as a country, a network or an organization) and controlling the access to the resources in that system (services, applications and data) by placing restrictions on the established identities”. In simple words the ultimate aim of I&AM solution should be in providing “right people with the right access at the right time”. I&AM is a combination of processes, policies and technology (products) to manage access to enterprise resources.

In a nutshell, an I&AM solution should be able to provide some or all of the benefits listed below.

- SSO for user and application.
- Aggregate Identity from multiple applications/systems.
- Role & Rule based Access management for all types of users (internal users, external users, partners, vendors, contractors etc).
- Complete auditing and accounting capabilities.

Key Business Drivers

- Regulatory compliance with respect to accountability
- Increased user experience
- Management Control
Identity and Access Management (IAM)

- Operational efficiency

The biggest challenge most Chief Security Officer’s face these days are managing access to systems, devices, data and applications scattered across internal and external systems. Moreover, they must provide this access for a growing number of identities; (internal users, external users, partners, vendors, contractors etc) without compromising confidentiality, integrity and availability of data.

Challenges

- Like SIEM deployments, you need to configure connectors to everything when setting up password management
- I&AM system does not remain static over time
- Single Sign-On Capabilities
- Federated identity management (SSO between companies)
- Identity Aggregation issues from legacy applications

Trends

- The trend of integrating IAM and DLP. This was demonstrated by CA, Inc., at the 2009 RSA Conference in Dave Hansen’s keynote.
- Bring Identity Management into SOA (service-oriented architecture)

Vendors

- Oracle
- CA
- IBM
- Novell
- Courion
- Sun Microsystems
- Microsoft
- SAP
- Hitachi ID Systems
Cloud Computing – Chief Security Officers (CSO) Concerns

If you do a Google search on ‘Cloud Computing Security’ you will get about 13,600,000 results and that’s too much of information for anyone to start. So let’s try to summarize the information keeping in mind of CSO’s concerns on cloud computing.

What is Cloud Computing?

In simple words, ‘Cloud Computing’ is a collection of Internet or private-network based services, providing users and devices with scalable & economical (pay-as-you-go) information technology capabilities. The services offered by the cloud can be email hosting, email security, software development platforms, CRM, virtualized servers and storage, etc.

Even though there are multiple deployment models for cloud computing, the most common and popular are private and public clouds. The best example for private cloud is Defense Information Systems Agency (DISA) cloud and for public cloud is Google Apps and Amazon Elastic Compute Cloud (Amazon EC2). Major cloud computing categories can include software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS).

Cloud computing is poised for significant growth over the next few years. Gartner, for example, projected in March 2009 that sales of cloud computing services would almost triple over five years, from $56 billion in revenues in 2009 to $150 billion in revenues in 2013.

So what are the major security concerns?

• User Privileges

When your data is in cloud, it will be possible for cloud administrators to have privileged access to your data and sometimes these users will have malicious intention which will result in data loss or data leakage. As enterprises don’t
have complete control of the data processed outside of the enterprise, ensure that enough information is collected of people who administer the systems and data in cloud. Ask, whether the vendors have Individual Screening Policy and Confidentiality agreements with potential employees.

- **Incident Handling**

  As clouds follow multi-tenant model with services scattered in the cloud incident handling can be difficult. Make sure that you are aware of how the cloud provider handling logs and how much they can support in case if incidents.

- **Logical data separation**

  While in cloud, all data separation is logical and this will bring risks associated with sharing data storage. Check that whether proper encryption and access controls are implemented for your critical data.

- **Application related risks**

  When applications are shared there can be security issues due to Insecure Interfaces and APIs. As the application moves from internal to external model the risk will increase as application exposure is high. Ensure that SaaS applications are used as stand-alone services, with no integration with other applications or other PaaS or IaaS services. Be aware of SaaS API’s using REST (REpresentational State Transfer) model, as REST doesn’t have any predefined security methods.

- **Network related risks**

  When your application moves from internal to external, the network exposure and dependency on network increases. The best examples can be man-in-the-middle attack or DDoS attack targeted against your internet gateway or your cloud provider’s gateway which will result in service outage.

- **Disaster Recovery**

  Make sure you are aware of disaster recovery options provided by your cloud provider.
• Legal

Whether it’s for regulatory compliance or any other legal requirement, customers are fully responsible for the confidentiality, integrity and availability of their own data. So make sure that you know how the cloud provider is handling your data.

Conclusion.

Because of all the above security concerns, can we say that it’s not good to go for cloud computing? The answer is no and the best approach will be to start with moving less critical services to the cloud as well as make sure that you are fully aware of what the cloud service provider is providing. Further do proper due diligence and ask for specific certifications like SAS70 Type II or ISO 27001 achieved by the provider. Even though SAS70 certification does not guarantee everything is fine with the provider, it can be a starting point.

Read this article on the website Click Here
Introduction

Let’s start with what’s Web 2.0 before getting in to the risks.

The term Web 2.0 is commonly associated with web applications that facilitate interactive information sharing, interoperability, user-centered design and collaboration on the World Wide Web.

For some of you still not clear of what’s Web 2.0 let me put it down in a different way. Web 2.0 is Facebook or MySpace or Linkedin or Twitter or the blogs or the Wikis or any web site which allows the visitor to interact by posting updates, comments or uploading pictures or videos.

The biggest challenge of the Web 2.0 world is that security must focus on protecting open systems rather than shutting everyone out. The social networking tools built on web and web 2.0 are incredibly powerful and useful: in some cases it can make employees more productive and speed up decision-making and in some cases they can allow companies to gain a competitive advantage over their rivals, and they can significantly reduce the cost of doing business.

Some Stats

According to a study by global communications firm Burson-Marsteller, more than three-quarters of the Fortune Global 100 companies are using at least one of the most popular social media platforms (Twitter, Facebook, YouTube, and corporate blogs) to actively engage with stakeholders. Sixty-five percent of the largest 100 international companies have active accounts on Twitter, 54 percent have a Facebook fan page, 50 percent have a YouTube channel, and one-third have corporate blogs.

The Nielsen Wire reports that the world now spends over 100 billion minutes or 22 percent of all time online on social networks and blog sites.
So what’s the risk?

The trusted nature of Facebook, MySpace and other social networks allow hackers to launch exploits and spread Web-based malware. Research says that, high number of users click on any link send by their friends in Facebook or MySpace or Linkedin due to the façade of trust these sites have. They won’t exhibit same amount of caution on social networks as they would when communicating in person.

**Phishing Scams**

I hope most of you are aware of the phishing scams common in email networks and it reached a stage where these techniques are extended to social networks. In email networks users are typically lured to a fake financial institution web site controlled by cybercriminals and once the data is entered into the fake site, it is stolen and used in identity theft crimes.

The open and trusted nature of social networks is making it easier to have same kind of scams and as per security company Kaspersky there were several phishing scams targeting Facebook or MySpace where a user received an email (from a trusted friend) with a link to a groundbreaking news event or an exciting photograph or video. A user clicking on that link is taken to a bogus site that imitates the login page of Facebook or MySpace. The end result is another stolen credential.

**Web-based Malware, exploits and other attacks**

As email is getting more and more secured by having multiple levels of malware protection and spam filtering, majority of malware is today distributed through websites. The methods could be asking the user to visit a website to get some freebies or to view some amazing video by downloading some plug-in and their by infecting the system. In some cases the malwares will be exploiting the known or zero day vulnerabilities identified in the operating system or other software’s (Flash, Adobe, Java etc) users use.
The malwares entering the system this way will have the capability to steal sensitive information from a computer or make the system part of a botnet network.

**Data Breaches and Data Leak**

Inadvertent data breaches can occur when users use Web 2.0 tools. This could be the case where a user accidentally entering some sensitive information on the web that can harm the reputation of his or her employer or inform the world of some confidential activity.

It’s possible to leak Sensitive or confidential information through social network or through social network based instant messaging

**Short Links**

Due to the extensive use of status update sites, blogging sites and microblogging sites like Twitter, use of URL/Link shortening is very popular and this creates a security risk where end user has no way of knowing what is on the other end of the shortened link without clicking on it. This gives cybercriminals the potential to send legitimate sounding links that actually lead to malicious sites.

**What’s the solution?**

**Risk Management**

The first step in risk management is to understand the type of risks organizations facing from the variety of Web, Web 2.0 and social networking threats and the nature of these threats. This can vary from organization to organization and user group to user group. Use publically available sources to provide this education, including vendors of Web security gateways, industry analysts, consultants, speakers at trade shows, Webinars etc. The key for any Security Manager is to educate himself or herself about the nature of the threats, how they could specifically impact their organization, and the remedies that are available to prevent and/or remediate them.
The next step is to carry out a detailed audit of the organization’s Web and endpoint security controls. The goal is to identify the holes in the security systems and to see what protection method is implemented. The result of this audit should be a vulnerability assessment that clearly defines where the system/user/network is protected and where it is vulnerable to attack and the criticality of the risk.

**Policies**

Depends on your organizations requirements, make sure you have clearly defined policies on what’s allowed and what’s not allowed. Based on the policies, educate employees on safety and security, and provide a framework for managing violations.

**Policies need to cover:**

Details of monitoring and blocking in place, content users are allowed to share and services part of social networking allowed.

**User Awareness**

Educate users about the risks of Web 2.0 and make sure they are aware of all the risks associated. Tell them in the world of Web 2.0 or Social Networking ‘Don’t trust anything’, ‘Challenge everything’ and finally ‘Have your own privacy’. Further make sure users are aware of the existing policies and enforcement process.

**Good Endpoint Protection solution**

Invest in a good endpoint protection solution. The days of having Antivirus and Antispyware protection based on signature analysis only is gone. Other than the Antivirus and Antispyware protection you need to have an endpoint protection solution which has more features like application & device control, HIDS/HIPS, firewall etc and malware detection capabilities based on signature, heuristics or behavior based.

**Secured Web Gateway**

For web traffic you need to employ malware, content and URL filtering technologies. Organizations need to ensure that all web
traffic coming and going is passed through a Secured Web Gateway solution and typically, these security solutions are capable of efficiently thwarting the majority of malware and malicious content that propagates through web 2.0 technologies. Additionally, Data Loss Prevention is an effective tool for monitoring any outbound communications, especially social networking. Using data loss prevention solutions that prevent sensitive data traveling outside the corporate network can be extremely valuable in keeping corporate data from leaking out to a social network either accidentally or intentionally.

Read this article on the website Click Here
Importance of Patch Management in effective IT Risk Management

Posted by Biji Scaria on February 20, 2011

Introduction

The classic text book definition of risk is, “the probability of a threat agent exploiting vulnerability and the resulting business impact”. Vulnerability can be from applications, software’s, firewalls, people, process, location etc and what we’re trying to see here is the vulnerability from software’s or applications and importance of patch management which in turn will result in effective risk management.

Effective Patch Management = Effective Software Vulnerability Management = Effective Risk Management

Background Information

National Vulnerability Database (NVD), reports 4,639 vulnerabilities (CVE) in the year 2010 and as per Secunia for the period 2007 to 2009 vulnerabilities in a typical end-user PC almost doubled from about 220 to 420. Secunia says “A typical end-user PC with 50 programs installed had 3.5 times more vulnerabilities in the 24 3rd party programs installed than in the 26 Microsoft programs installed. It is expected that this ratio will increase to 4.4 in 2010”. Over the years the vulnerabilities reported in 3rd party (non-Microsoft) programs are increasing with an alarming rate. Today patch management is critical not only for big enterprises, even a company with couple of servers has to spend some time in identifying and patching.

The high influence of vulnerabilities has resulted in systems constantly being threatened by new attacks and the level of damage caused by these attacks can be quite severe. Some of the worms and cyber attacks utilized the existing vulnerabilities are Operation Aurora, Stuxnet, Downadup/Conficker, Code Red, BugBear, Nimda, Blaster, and MyDoom. The interesting fact was, each one of them attacked a known vulnerability for which a patch or other mitigation steps had already been released.

Patch and Vulnerability Management Process
As with any risk management process, there should be a systematic approach for patch and vulnerability management. This systematic approach should make sure all systems, software’s and applications are audited frequently to identify the vulnerabilities existing. The patch management life cycle should be continuous and a typical life cycle can be Auditing, Identifying Vulnerabilities, acquiring patch, testing and deploying.

Many organizations, especially those with extensive Microsoft platform deployments have developed elaborate processes for Patch Management to the Production environment. But the key for successful patch management these days are patching non Microsoft applications as well as patching test environments. How many organizations are spending time and resources on patching non Microsoft applications?

**Solution**

For effective patch management you have to use multiple solutions and depend on the budgets available and size of the organization you can go for Group Policy, WSUS, MBSA, Microsoft SMS, Secunia CSI (Corporate Software Inspector), GFI LANguard, Altris, IBM Tivoli etc

**Conclusion**

In IT Security, we talk a lot about having good firewalls, IDS, IPS, Antivirus and other security measures and most of the time we miss importance of effective patching process. Further majority of user’s and businesses alike still perceive Microsoft products to be the primary attack vector, largely ignoring third party programs and operating system. It goes without saying “Patching vulnerabilities provides better protection than thousands of signatures as it eliminates the root cause”.

Read this article on the website [Click Here](#)
As the use of cloud computing becomes more available and more exciting, great emphasis is place on data efficiency but the security risks often are overlooked or even not known.

Most risk managers are completely aware of the security risk. Some data are quite sensitive including customer information, marketing plans, proprietary research and product development, and trade secrets, to name only a few.

However, is awareness of this risk enough? Many hidden risks may pose a more severe threat. For example, your organization might undertake an extensive audit to ensure that its potential cloud provider enforces strict security protocols equal to those of its own internal IT environment. However, does that ensure that your data are protected at the same level?

Not necessarily. As the growth of cloud computing expands, many smaller providers are going to want to join in, and some will not have the same applications or storage capacity as their larger rivals. As a result, a new type of secondary provider is going to emerge, the cloud subcontractor. This organization will provide services to the primary cloud provider. However, the great risk is that this subcontractor may not apply the same security as the primary; and the primary may not disclose its use of a secondary provider to customers.

Another hidden risk is found in the compliance area. Some organizations (such as defense contractors) are forbidden by law to move classified information outside of the host company. As a result, they may contract with a cloud provider located in the same country. However, the use of a subcontractor is invisible and may not even by known to the customer. At the same time, though, the customer is responsible - and liable -- for data security.

The new universe of cloud computing is a wonderfully exciting one, offering great advances in technology at least as promising
as the Internet was when it was first introduced. But like the Internet, there is no assurance that security will be better in the future. Based on history, it is more likely that with advanced technology comes higher, not lower threats.

**Editorial additions: The relevant best practices, white papers and case studies:**

**The Top Ten Considerations for Cloud Computing**

Business and IT decision makers are increasingly confused by the rising number and type of cloud computing solutions. Everyone it would seem is now promising to save you time and money with this or that kind of web-based service for everything from email and enterprise applications to storage and data management. Regardless of the information overload, however, organizations of all types and sizes must embrace the age of computing without borders to increase competitive advantage and grow their business.

Sounds great, but it isn't easy. This on-demand Webcast, featuring the editors of TechRepublic and ZDNet.com, provides The Top 10 Considerations for Cloud Computing that will not only satisfy your need-to-know but will also help you make a more informed decision about the future of your business.


**Evaluating and Contracting for Cloud Financials: Best Practice Considerations**

In the white paper "Evaluating and Contracting for Cloud Financials", you'll find practical advice and tips to ensure the choice you make is right for your organization. You'll learn:

Why the Web has shifted the power to the buyer and, most importantly, how you can leverage that power during vendor selection and contract negotiation.

Why Service Level Agreements are key to a successful vendor relationship and what you need to understand to set expectations, guarantee performance and reduce risk.
A hidden risk to cloud computing

How to think about the ROI of cloud computing versus on-premises solutions. When done accurately, the numbers speak for themselves.


Moving your business to the cloud.


Read this article on the website Click Here
We may all expect that security is going to be as important in the near future as data efficiency. The exciting developments in cloud computing make this two-part challenge glaringly important. Of course everyone wants data efficiency and unlimited, easily accessible storage. However, the future success stories of cloud computing may be those providers able to offer these benefits along with exceptionally high levels of security.

Four areas are likely to dominate the discussion of security in cloud computing:

1. **Cross-reliance trends.** One likely outcome to cloud computing will be the increased reliance among private sector companies and public agencies on the cloud, but even more important upon one another as well. As the IT environment expands rapidly, it will cause increased shared interests in the two big sectors, in terms of all aspects to the cloud: data management, processes, storage, retrieval, security, and communications.

2. **New host architecture models.** The cloud, like its grandfather the Internet, will clearly be a dynamic set of technological capabilities. The need for improved and higher-level security by itself will cause changes in cloud architecture. However, marketing priorities will also come into play in the ever-evolving nature of the cloud. The new methods are likely to include wireless data transfer, a growing role for social media, and of course the rapid expansion and reliance on hand-held devices as part of the cloud.

3. **Accelerated threats and sophistication of threat advancement.** Just as technology advances in a positive manner, so will the threat universe. A black market is already evolving for intellectual property theft and misuse, and in the cloud this is sure to continue. The IT challenge of the future will be to remain steps ahead of threats as the cloud evolves and expands. Man-in-the-middle attacks and domain squatting are
likely to be serious issues, but they might also be the tip of the iceberg.

4. **Difficulties for law enforcement in keeping up with evolving threat levels.** By definition law enforcement is most often responsive. Given the rapid growth of cloud technology and its global attributes, this problem is going to become more severe in the future. Unfortunately, cyber crime is becoming very profitable, and law enforcement will need to step up its cooperative efforts with industry and government to figure out how to curtail these activities.

Read this article on the website [Click Here](#)
The cloud is worth the risk if the annual benefit minus the expected cost of risk is greater than the cost to run in-house. A simple statement, however, on closer inspection the complexity of the decision becomes apparent and the engineer in me rises to the surface. Below is the cloud outsourcing decision expressed in mathematical terms. If you follow it through your cloud outsourcing decision should become clearer, even if it is difficult to assign numbers to give you an accurate answer.

In mathematical terms:

If \( B - E(R) > H \) then the cloud is where you should be, where:

- \( B \) = The Benefit that would accrue each year
- \( E(R) \) = the annual expected cost of Risk
- \( H \) = Annual cost to run in-House

So the answer comes from breaking down \( B \), \( E(R) \) and \( H \) so you can assess their expected results and run the above equation. Taking each one in turn:

**Benefit**

\( B \) can be expressed as:

\[ B = C + O \]

- \( C \) = Cost savings
- \( O \) = Opportunity derived

Cost savings should be relatively straightforward to calculate, however, don’t forget to include more difficult items such as efficiency savings if the system you are moving to will save your people time and effort.

The more challenging task will be determining the extent of the opportunity from utilising the cloud. For many companies this will be much more important than the cost savings with
opportunities such as speed to market with a new product, solving a customer service problem in double quick time or freeing up key internal resources for another IT project dominating the equation.

**Risk**

\[ E(R) = (L \times Pr1) + (Re \times Pr2) \] where:

\( L \) = liabilities (such as from a breach of privacy)

\( Pr1 \) = annual probability of incurring the liabilities

\( Re \) = reinstatement costs (the additional costs/losses from running your operation and the costs to move to another provider or to reinstate the service in-house and the cost to reinstate your reputation that will surely be damaged in such an event)

\( Pr2 \) = annual probability of incurring the reinstatement costs.

Here is where things get even more difficult. Depending on the contract you have with the cloud provider, their ability to meet any claim you may have against them and any cover you may have from your own insurance, these liabilities could be relatively small or very large. The reinstatement costs are also very challenging as you need to consider the effectiveness of any Business Continuity Plan you have in place, the higher costs of replacing the system as quickly as possible and of course that king of intangibles, your reputation.

**In-House Cost**

\[ H = D + ID \] where:

\( D \) = Direct costs such as hardware, software and support staff

\( ID \) = Indirect costs such as a portion of IT management and corporate overheads
These costs are generally the easiest to estimate as you have real data and can make educated guesses about apportionment of costs as these are much more visible to you.

Now before you run off and start getting the data and the team around to help you with your estimations, there is one more thing you should consider. Are you going to assume the answer for this current year is going to be the same each and every year or will any of these variables change substantially? If the answer is the latter, then you need to forecast how each value will vary over time and then discount them back to today’s dollars and then run the equation.

www.rmpartners.com.au

Read this article on the website Click Here
A couple of weeks back I was approached by a HFT magazine editor and he asked me whether I would be interested to write down some of my experiences in HFT. As I am not directly participating in the midst of HFT at this point, I had to give it quite some consideration. Why would I do this? Placing myself in a vulnerable and visible position is not my first nature. Still I strongly believe in taking away the mystique or even – allow me – hysteria regarding this type of Capital Markets business. In my opinion the world of low-latency/hi-freq trading has to try and get rid of the negative image. It deserves some consideration to explain in a bit more detail what HFT is all about. What techniques are being used and – more generally – what the business reasoning behind HFT is.

So why does HFT need more transparency? Very simple. EU lawmakers in Brussels and national regulators have very little knowledge regarding the business and technological concepts driving HFT. This can automatically lead to potential actions that can harm the trading firms directly.

Secondary effects can be envisaged impacting liquidity and widening spreads on multiple platforms. I will get back to you regarding the implications of losing liquidity and widening spreads some other time.

First the negative effects of lawmakers and regulators not having any clue what HFT is all about.

About a year ago I was invited to be part of a speakers panel at one of the first professional Hi-Freq conferences in London. At the time I was MD at an Algo/HFT market making firm primarily participating in quantified dispersion of volatility and
equity arbitrage across multiple venues. We spoke about market access, risk and regulatory influences. I became very enthusiastic recognising attendees from the FSA and the Dutch and French regulators at this conference. On the podium I invited the Hi-Freq world to open up towards each other and break down the barriers. At the same time I invited regulators to step into my office and literally have a look at what we exactly did. It took another couple of phone calls and emails on my initiative before representatives from the Dutch and UK regulator actually did visit the office. I’ll point out two very important remarks they made that will paint us a picture still waking me up in the middle of the night...

Looking at the order books and depth of Nokia quoted on OMX Helsinki and Nokia quoted on Chi-X one of them asked the following: “The order book on OMX we believe, but we are under the impression the order book on Chi-X is not real...”. The other remark was one regarding liquidity providing on multiple platforms: “We consider demanding liquidity providers and arbitrage traders to keep their quotes in the market for a minimum time, for example one second”.

I won’t disclose which regulator came up with what question and to be honest, I am happy with the fact they put their questions forward. At the same time it clearly tells us where they are in understanding the business they have to regulate.

Obviously I spend a bit of time explaining how a multilateral trading platform like Chi-X works and what would happen if arbitrage traders have to keep their quotes in the order book for a minimum time frame. It just goes to show that although MTF’s came to live due to the implementation of MiFID in 2007, the lawmakers and regulators still had to do their homework. On the other hand this is fact of live the Capital Markets business and more specifically the HFT world needs to take into account.

I can already hear you think: “Do we have to educate those regulating us?” And the answer is ‘Yes’, I am afraid. If we would like to continue trading with algorithms on a low-latency
Transparency for High Frequency Trading
Regulators, an Introduction. Contributed by Walter Hendriks

infrastructure connecting multiple exchanges to trade extremely tight spreads, we have no choice.

Nobody needs new EU regulations based on a lack of understanding what this business is all about. Fortunately some of the top tier market making firms in Europe and the US understand this difficult situation. They have started to write down specifics regarding the trading techniques used and the ball is definitely moving towards the corner of the regulator. Now it’s up to the national regulators and the European Securities and Markets Authority (ESMA) to pick up from here and start communicating with the HFT world to get a better understanding.

As promised next time I’ll discuss a bit what liquidity means to the financial markets. Don’t hesitate to let me know what you think!

Best regards,

Walter Hendriks
Principal Advisor

Financial Markets Advisory - fm-advisory.com

wh@fm-advisory.com

17th of January 2011

Read this article on the website Click Here
The amazing power of candlesticks - reduce the timing risk of trading

The chronic problem every trader faces is one of timing. It is relatively easy to identify high-quality companies whose stock you want to trade. But getting on and out at the best possible time is a real challenge - unless you have the tools to pin down the most likely timing of trend reversals.

Fundamental investors tend to look down at technical signals, claiming that short-term price movement is chaotic and unreliable in comparison to primary trends and, of course, fundamental strength or weakness. Yes, short-term trends are very chaotic and that's just the point. Because price movement is illogical and often an expression of over-reaction to current news, signals of reversal are reliable, accurate and can help you get a jump on most other traders.

Candlestick charting is one answer. Candlesticks are formations of one, two or three consecutive sessions that, by their patterns, signal that reversal in the trend is about to occur. This is not technical voodoo. Some reversal patterns are correct up to 80% or 85% of the time. So if you traded on such reversals just by themselves, you would be right in your timing in a majority of cases.

But that's just the beginning. Every indicator, including candlesticks, is made much stronger when confirmed with a different and independent signal. It may consist of another candlestick formation, volume spikes, well-known technical signals (like head and shoulders or double tops or bottoms), repetitive gapping action, or momentum oscillators.

So using candlesticks as the first step and then seeking confirmation as a second step are going to vastly improve timing of entry and exit. One final point worth remembering: reversal is most likely to occur as the price trend moves close to support at the bottom, or to resistance at the top. The trading range borders are the "lines is the sand" of a trading trend, and when you see
reversal signals close to these price lines, pay attention. By the same argument, when you find and then confirm continuation patterns at or near support or resistance, it could be a sign that a breakout is about to occur, meaning setting up a new trading range.

Candlestick patterns are so important to traders that I have published a book on the topic. Published by Wiley, it can be pre-ordered and will be on the market the first week of February. If anyone has questions about candlesticks and how to use them, please drop me a note. I promise to answer all messages personally and promptly. To order the book, go directly to the publisher's website at John Wiley & Sons or to Amazon.com. You can also learn quickly and easily how to master the powerful world of charting at this link: candlesticks

Read this article on the website Click Here
A quick and easy way to master the world of candlestick charting

To all of my friends: If you find trading and investing to be mysterious, you might be very interested in unraveling the candlestick to vastly improve your entry and exit timing.

In a nutshell, candlesticks are visual representations of a session's trading activity: opening and closing prices, trading range and direction of movement. This lets you understand right away how each session's price action moved, but equally important, you can get a sense of an entire chart's history based on candlesticks.

This topic has interested me for a long time and I have written two books on the topic. However, if you are interested in a quick and easy method for mastering candlesticks, check out the complimentary information to reduce your trading risks through improved timing, at this link: candlesticks -- I hope you will let me know your impressions, and that this information helps you to develop a new, improved trading system.

Read this article on the website Click Here
The problem most traders face is one of timing. You find reversal signals and know there's a likely change in price direction; but exactly when do you pull the trigger? You may enter new positions or exit existing ones, but the timing has to be reliable to make your trading agenda effective.

The risk here is one of timing as well. If you act too quickly, you might lose potential movement in your favor, and if you wait too long, you could lose many points of profit as well. You rely on

5. **Confirmation.** Traders follow a two-step procedure. First, you find a reversal signal, and second, you confirm it with an independent, separate indicator telling you the same thing. This may be another candlestick, a traditional technical change, or a momentum oscillator, for example. Confirmation is a requirement, no matter how strongly reversal is indicated.

6. **Trend awareness.** You have to have a trend in effect in order to reduce it. So if you find a bullish reversal, it is applicable only if a bearish trend has been underway. A bullish signal in the middle of a bullish trend is a continuation pattern. You need a trend to reverse, so you cannot be myopic in how you view trends and reversal signals.

7. **Reliability of signals.** Finally, you need strong and reliable signals. Some candlestick formations are reversals only 50% of the time. That's not of any value at all. You need an advantage, so seek formations with very high levels of reliability.
One of the best of these is called the "white soldiers" (or, "three white soldiers"). Each session opens within the trading range of the previous session and then closes higher. This is show below.

This appears at the bottom of a downtrend and signals bullish reversal. It is reliable 82% of the time. That is incredible and when confirmed with a second indicator, you can proceed with confidence.

The opposite of the white soldiers is the "black crows" (or, "three black crows"). This is a bearish reversal signal when found at the top of an existing uptrend. Each session opens within the trading range of the previous session and then closes lower. This is shown below.

The black crows is reliable 78% of the time. So these two indicators -- white soldiers and black crows -- are among the best reversal signals. They also appear often in charts, so they can be used with confidence, especially when they are in the right place (white soldiers at the bottom of a downtrend, and black crows at the top of an uptrend), and when they are confirmed with other signals.

Many candlesticks are reliable, but these two are among the best. Reliability around the 80% level is something you cannot ignore. I have written a comprehensive reference on the topic, The Bloomberg Visual Guide to Candlestick Charting (John Wiley & Sons) that explains the uses of dozens of candlesticks as well as confirmation signals. As the name implies, this is a highly visual book published in full color and with dozens of illustrations.

It can be ordered directly from the publisher, John Wiley & Sons or on amazon.com at Amazon.com

Learn much more quickly and easily with complimentary guidance tools at candlesticks
Just three years ago the G20 leaders agreed upon a common course to regulate the financial markets, with focus on standardising OTC derivatives. In that time regulators have created the largest reform packages since the dawn of modern financial history including Dodd-Frank and the European Market Infrastructure Regulation (EMIR).

But are market participants prepared to cope with the consequences of these regulatory behemoths? With regards to OTC derivatives, under the new rules, these are supposed to be traded electronically and cleared centrally – provided they are ‘standardised’. Let’s look at two corresponding aspects of the G20 clearing mandate: the term ‘standardised’ and the instruments that are deemed to be clearable.

**Standardisation**

The G20 mandate speaks of ‘standardised OTC derivatives’ that should be centrally cleared. But what and who defines ‘standardisation’? There is now an understanding that this will be decided by the relevant regulatory body – but in close coordination with the clearing house(s). This results in two approaches. The bottom-up approach is where a clearing house approaches a regulator with a product which is then mandated for central clearing. A top-down approach sees the regulator with the power to identify OTC derivative contracts for clearing irrespective of whether a clearing house can actually clear them. The top-down approach makes some market participants squirm as many questions are unanswered, raising the level of insecurity.

**Instruments**

Instrument-wise there is also uncertainty around what is going to be clearable from the start and even more importantly, what will be clearable in the mid- to long-term future. For now, there is a common understanding in the derivatives market that single
name and index credit default swaps (CDS) as well as single-currency interest rate swaps (IRS), will be immediately clearable, as clearing houses offer this service already today. Currently not eligible for clearing for example are IRS that are denominated in less common currencies, have two currencies (e.g. cross-currency swaps) or possess an optionality in the contract (e.g. a break clause).

Clearing regulation is fraught with complexity but market participants now have certain guidelines on which to base their clearing strategy. However, there is a strong case for each financial institution (FI) to establish a standing clearing working group (involving ALL affected business units front-to-finance) that is up to speed with the latest developments on regulation, clearing houses and market initiatives. FIs should also ensure that they are engaged with their respective representative industry bodies in order to prepare adequately for the future.

Stay tuned for the next part of this OTC clearing blog series which will look at regulatory complexity and the alignment of exemptions.

Read this article on the website Click Here
“ [...] The financial crisis that began in 2007 had its origins precisely in overcomplex regulation.”

These are the wise words of Niall Ferguson, Professor of History at Harvard, speaking at this year’s BBC Reith Lectures. He goes on to cite Dodd-Frank as a near-perfect example of excessive complexity in legislation.

Those of you who had the pleasure of sifting through the proposed rules, discussion papers, and guidance will agree that the inherent complexity is immense. The recent Dodd-Frank progress report by law firm Davis Polk cites that the two years since Dodd-Frank’s passage have seen 848 pages of statutory text expand to 8,843 pages of regulations.

For OTC players, trying to align current timelines in the regulatory onslaught is tricky, and continuous, given:

- Dodd-Frank: Q4 2012
- EMIR: Early 2013 (although this may be moved out by 6 months)
- Basel III: Early 2013

The counterparty-driven credit value adjustment (CVA) charge for bilateral OTC derivatives which Basel III introduces can easily triple the core capital needs of today. There is currently no CVA charge for cleared OTC derivatives, but if EMIR comes into force six months after Basel III what will financial institutions do in the meantime? From where will the necessary additional core capital be raised?

In the US, the SEC and CFTC have come up with exemptions for clearing obligations. Financial institutions with less than a $10bn balance sheet do not need to clear OTC derivatives. Some co-ops are exempt as are corporates which use derivatives to hedge commercial risk. Some of these exemptions find their correspondence in EMIR but others don’t.
As a consequence of this complexity, market participants are unsure with whom they will be able to clear OTC trades. This will also have a material impact on the pricing of products. In addition to these looming deadlines there is the overhaul of MiFID (the ‘Markets in Financial Instruments Directive’) which is also in the pipeline. Once Dodd-Frank and EMIR are actually ‘up and running’, it is likely that Dodd-Frank II and EMIR II won’t be far around the corner, not to mention Basel IV.

Look out for part 3 of this OTC clearing blog series which will cover extraterritoriality.

Read this article on the website Click Here
After almost two years since the Dodd-Frank Act (DFA) was put on the statute books, the first swap-related articles finally take effect on 12th October this year. Now everyone can be assured they are trading, clearing and reporting under a common set of rules, right?

Not so. While DFA requires market participants to report OTC trades to Swap Data Repositories (SDR) and introduces conduct business rules, other jurisdictions have not yet finalised their respective regulations. A regulatory conundrum arises: how will rules drawn up in one jurisdiction apply in others (also known as extraterritoriality)?

There are many unanswered questions around extraterritoriality and this is one of the reasons trade bodies like The International Swaps and Derivatives Association (ISDA) are crying out for clarification:

- Will regulators recognise one another’s regimes to ensure continuous trade relationships around the globe?
- Will firms clearing via clearing houses outside their jurisdictions be able to continue to do so?
- When trading across jurisdictions, which of the counterparties is required to do reporting, or is it both? To which SDR will they report?
- If DFA comes into force earlier than other jurisdictions, does a trade need to be cleared at all? Will end-user exemptions come into play or not?

As Larry Thompson, general counsel at The Depository Trust and Clearing Corporation (DTCC), recently pointed out: “Harmonisation of regulations is paramount because, unlike the securities markets, derivatives have no set domicile – these markets and their participants are global and diverse.”
The new regulatory landscape will keep financial institutions under the scrutiny of their domestic regulator, and potentially also under foreign regulators due to extraterritorial reach. The lack of harmonisation across jurisdictions represents a challenge for firms, as does the fact that industry practices are still evolving as regulatory requirements across the globe unfold. Flexibility and adaptability are key but sadly this has always challenged financial institutions.

The pace of these changes makes it difficult to adequately adapt to regulations and, in some cases, is creating rework of analysis already conducted due to changed or additional regulatory requirements. Global regulatory alignment in this matter, therefore, is an absolute necessity to calm fears and reduce uncertainty of market participants.

*In the next part of this OTC clearing blog series we will look at implications on collateral management.*
OTC Clearing: part 4 - OTC clearing and its impact on collateral management

Collateral: banks, broker-dealers, funds and clearinghouses all need it more than ever. Collateralisation of bilateral as well as cleared OTC trades is essential to ensure a functioning and stable financial market that is able to absorb potential shocks of Lehman-esque dimensions. Upcoming regulations like Basel III, Dodd-Frank and EMIR and margin requirements for non-centrally-cleared derivatives will enlarge the required collateral pool considerably.

Isn’t there plenty of collateral available already? Not exactly! Estimates from various sources suggest that the additional collateral necessary to cover the rising demand is between $2 trillion and $4 trillion. With cash collateral being the most expensive but also most successful option (i.e. being fungible, reusable and easy to manage operationally) the expansion of collateral types under consideration as part of the Basel Capital Adequacy Consultative document will see an increased use of diverse collateral (eligible instruments like government bonds). This change will lead to new requirements like complex collateral valuation tools.

But there is currently a squeeze on what is acceptable collateral in today's volatile trading environment. This could make maintaining collateral an expensive proposition. Long gone are the days where there was plentiful high-grade sovereign debt available. The International Monetary Fund predicts that sovereign downgrades will reduce the supply of general collateral b... 

Clearing houses, looking for alternatives, are starting to also accept gold bullion and high-grade corporate bonds but this is only the tip of the iceberg. Clearing brokers are offering their clients collateral transformation services to swap non-eligible assets into cash, albeit at a cost.
As a consequence financial market participants need to re-evaluate the way they are performing collateral management today. A siloed approach to collateralisation looking at collateral for repo, listed products and OTC products separately for example, won't work in the future. It is essential to use available collateral to your best advantage but this is only possible if there is a holistic company-wide view on collateral management, as close to real-time as possible.

Collateral management needs to be viewed not as a cost centre but rather as a provider of an invaluable service to the trading function and to clients alike. Moving along the maturity model stages collateral management might even become a profit centre by utilising re-hypothecation, optimised collateral/netting as well as collateral ‘upgrade’ trades. Visit our paper with more details on this topic here.

Next week our OTC clearing blog series will look at reporting requirements to trade repositories and the unintended consequences in this area.

Read this article on the website Click Here
In order to monitor systemic risks as near to real-time as possible regulators have introduced the requirement for market participants to report all OTC derivatives trading activity to swap data repositories (SDR). The aim is to boost transparency and surveillance capability. The idea is strikingly elegant, yet fraught with complexity when it comes to application by market participants.

The reporting is mandated through Dodd-Frank and EMIR. SDRs need to be registered with the respective authorities in the various regulatory regimes. For example, a few days ago the Commodity Futures Trading Commission (CFTC) provisionally authorised The Depository Trust & Clearing Corporation (DTCC) to create and operate a multi-asset class SDR in the U.S.

The DTCC is just one of a multitude of local and global trade repositories that will receive registered status. This creates a number of challenges for all market participants. Financial institutions need to decide which data to report to which repository. Sounds easy but:

- Which trades do you report to which repository?
- Do you need to report to more than one SDR?
- Where are you counterparties reporting to?

Some reporting requirements are not even finalised yet and with others it seems doubtful if they can sensibly be implemented. For example, ESMA asks in its current proposal that collateral which is held/posted against each individual trade is reported. This is tricky if you have netting agreements in place where there is an exchange of collateral based on the overall portfolio with a counterparty.

Most institutions do not currently have infrastructure designed to accommodate large real-time reporting requirements.
Information is typically stored across various systems and siloed by product or business line.

Regulators will face the daunting task of bringing together a vast amount of data from the various sources globally, their goal being to enhance transparency, reduce systemic risk and find patterns that allow early intervention. Suddenly, ‘Big Data’ comes to mind and the task is not made easier when diverse reporting standards with differing data formats exist.

Another challenge is the recently fledgling global consensus on unique industry-standard identifiers that will be essential to the effectiveness of new reporting processes. In a CPSS-IOSCO consultation report on OTC derivatives data reporting an..., Unique Transaction Identifiers or Unique Swap Identifiers (UTI or USI), Legal Entity Identifiers (LEI) and a product classification system, known as Unique Product Identifiers (UPI), have been recognised as the prerequisite to effective data reporting and aggregation, with LEI und USI already in the definition/implementation phase.

There is a clear need for interoperability across SDRs and between regulators to overcome the challenges and make it easier for financial institutions to report the necessary data.

Coming up next week in our OTC clearing blog series is a deeper look into what LEIs can do for you.

Read this article on the website Click Here
Just one year ago you were probably aware of ISINs, BICs and/or SWIFT codes. But LEI, USI or UPI would probably have elicited a mere shrug. In the regulated world of OTC derivatives, these acronyms are the foundation for stringent and consistent regulatory oversight.

The Dodd-Frank Act mandated the creation of the Office of Financial Research (OFR) with the task to collect data from financial market participants to allow for enhanced visibility and transparency of a highly interconnected global market. The concept of a legal entity identifier (LEI) was adopted to facilitate this task by consistently identifying parties to financial transactions.

Some parties may be frustrated with another identifier having to go into the system, but let’s take a look at the design and proposed governance to better understand the benefits. Based on the ISO standard 17442, the LEI is a ‘non-speaking’ 20-digit alphanumeric identifier governed by a three-tiered structure of Regulatory Oversight Committee, Global Operating Unit and Local Operating Unit. It is a commonly accepted standard for the unique identification of financial counterparties. Tim Lind, head of legal entity and corporate actions at Thomson Reuters said that he’s “never had a conversation with customers – with anyone in the market....

There have been past initiatives which tried to achieve this, like the IBEI. But never before was such an identifier backed by regulatory demand, which will propel the LEI to the forefront of counterparty management in financial institutions. Although for now regulators only demand the LEI for reporting purposes the number of usage possibilities are varied.

First, the LEI will provide complete and consolidated information about the entire firm’s positions, rather than the narrowly focused...
TRADING AND DERIVATIVES

silos of mismatched data. A seamless integration between trading, risk, settlement and accounting systems will become reality.

Secondly, having a firm-wide view on what business is being done with an institution will help in understanding that counterparty’s risk profile and will also be the base for cross-selling activities that will ultimately enhance the revenue and profit generated with a customer.

Lastly, together with the implementation of other regulatory-backed identifiers, like the unique swap ID (USI) or the unique product ID (UPI), internal and external reporting will become streamlined, timely, more accurate and cost-efficient.

Financial institutions must grab this opportunity to upgrade data management infrastructures to not only incorporate LEI, USI, UPI and others into the existing framework but rather use them to lay the foundation for the future data landscape of the organisation. Although there is a cost involved in upgrading data management infrastructure, the price of not doing so – and the associated risks – is overwhelming.

Next week’s post in the OTC clearing blog series looks at new emerging trading venues.

Read this article on the website Click Here
In the ‘new normal’ of highly regulated financial markets, corporate treasurers are feeling the reverberations in their daily activities. Corporates are using swaps to hedge their commercial risks, stemming from currency, interest and commodity price exposure. To mitigate such risks treasurers have a whole arsenal of instruments ready to deploy such as swaps, forwards and options as well as individually structured products.

Under current bilateral trading agreements, corporates typically do not put up any collateral with mostly one-way netting agreements in place and sometimes no netting agreements at all. Swap activities and the resulting mark-to-market valuations are covered by extended credit lines of their financial counterparties.

Pending regulations for the financial sector (especially Dodd-Frank Act (DFA), EMIR and Basel III) will have a direct impact on corporates who are classified within these frameworks as non-financial end-users. Whereas Dodd-Frank and EMIR require standardised swaps to be centrally cleared, Basel III introduces the CVA (credit value adjustment) charge which makes bilateral swaps vastly more expensive as the amount of core capital required is three times higher than before.

But corporates are granted exemptions under DFA and EMIR:

- **End-user exemption under DFA**
  - Exemption from mandatory clearing and trading if swaps are used “to hedge or mitigate commercial risk”
  - Notification to the Commodity Futures Trading Commission required
  - Board approval to opt out of the central clearing requirement

- **End-user exemption under EMIR**
- No clearing obligation as long as certain thresholds are not breached

- Thresholds apply to all trades not “objectively measurable as reducing risks”, which means not used to hedge commercial risks

- Current thresholds for credit and equity derivatives are €1bn and for interest rate, FX, commodity and other derivatives, €3bn

Here’s the catch – no such exemption has been granted under Basel III until now. The result is the application of a CVA charge by financials when calculating the core capital consumption needed for deals with corporates although such trades would not be required to be cleared. The respective cost of trading is likely to be transferred to corporates making their hedging activities more expensive. One estimate by a group of 17 large German corporates puts this at... and consequently there is still industry confusion about which exemptions will be granted.

The European Association of Corporate Treasurers (EACT) is at the forefront of lobbying efforts to bring in line the CVA charge application with EMIR exemptions. But currently, corporate treasurers’ use of swaps could move in different directions if an exemption under Basel III is not achieved. Firms may:

- Keep going as before and bear the additional cost of trading

- Adjust current processes to enable central clearing of swaps, which would alleviate the cost stemming from the CVA charge but would require corporates to put up collateral that they typically do not have

- Reduce or effectively stop the hedging of their commercial risks to take on the risk rather than the cost.

As David Lawton, Director of Markets at the FSA put it in a recent... “These are not challenges that will go away overnight [...] I would encourage you to engage as much as possible. Consider whether you need to amend existing or enter into new bilateral credit support documentation to meet new margin requirements. Review existing operational processes to ensure
they conform with the new technical standards. Provide notifications in good time to regulators if intending to rely on exemption.”

Read this article on the website Click Here
Operational Risk

Getting your data ship-shape to weather the buy-side perfect storm

Posted by Dick Severs on January 20, 2011

“You could be a meteorologist all your life and never see something like this. It would be... the perfect storm.” So goes a classic line in one of the few great Hollywood fishing epics. The Perfect Storm finds fisherman George Clooney and his shipmates venturing out into dangerous waters and being trapped between two momentous and powerful storm fronts. Asset managers may well empathise.

On one front, ever more powerful regulation is blowing in, growing as it does. This regulation comes with ever-increasing demands for transparency around liquidity and capital requirements. Frameworks such as UCITS III also require liquidity reporting to be done on a more frequent basis. Not just that, but institutions will now have to demonstrate data quality and the provenance of data used to derive calculations – with regulations such as Solvency II coming into force in late 2012. Finally, you have central banking authorities within each country defining specific domestic reporting requirements.

Meanwhile, sweeping in on the other front comes ever increasing volumes of OTC derivatives trades – with many segments of the market continuing to expand despite stricter regulation. This is great news for those fishing for a big profit, with these complex and specific instruments potentially very lucrative. But OTC trades are generally more data intensive than other, more standardised trades – and also require greater risk management.

So how should asset managers contend with the data waves caused by these two storm fronts crashing together? The answer is that they need to streamline their boat – no mean task.

Currently many buy-side institutions manage their processes with fragmented systems, disparate spreadsheets, complex customised downstream and manual processes – all of which
create a web of silos. This can result in real headaches. One asset manager I was speaking to recently could only process three of a certain complex OTC derivative a day, as his systems just could not cope with any more and back office workarounds had to be installed. If asset managers want to overcome these issues, they need to update their wider infrastructure and ensure that they have the data governance processes in place, front to back, to effectively manage not just their trading, but also administration and execution.

One issue when implementing this, though, is that all too often the businesses users captaining the boat don’t take enough of a lead role. Those in the back office have a great understanding of technology, but it’s only when a holistic view is developed, taking into account business needs and technological opportunities, that a strong solution can be found.

What’s really needed is for buy-side institutions to adopt a process-driven approach, whereby infrastructure and data management solutions are specifically wrapped around business requirements. The ultimate goal is to develop a framework that enables business users to monitor risk and compliance in real-time. Get this right and not only do you meet regulations – you also reduce your operational risk, improve your data governance and are more free to focus on generating alpha for clients. Then it’s plain sailing and blue skies ahead.
Deception—Proof Fraud

Posted by Dimitar Zayakov on March 31, 2011

Usually deception and fraud are assumed to be, if not synonymous, at least in a relationship of implying each other. This is a well justified view since deception is misrepresentation, distortion of truth, and hiding the truth while fraud is gaining something one is not entitled of or preventing illegally and/or immorally other persons to make a gain and causing them suffer a loss as a consequence of deception. To put it in brief, deception is the first step (a preparatory stage) and fraud is the second one—the fulfillment (No doubt, temporally both steps could coincide, but logically they are distinguishable).

There is, however, a vast area of emerging fraud aerobatics where deception cannot be identified but fraud, nevertheless, is present. This possibility is due to the connection between deception and truth and, on the other hand, between fraud and unauthorized gain/loss. It is perfectly possible that truth is not to be distorted (no evidence for deception) but fraud is still committed. In most cases, a statement is perceived to be false when it does not correspond to the matter of fact. This allows envisaging a situation where reality is defined and constructed way of statements expressing vested interests to correspond to it. The goal of such correspondence would be to ensure an unauthorized gain or cause an unjustified loss to another party, that is, fraud. This could be exemplified by mass privatization in a volatile situation. In such a case, there is no guarantee that the privatization companies, which have collected the privatization stocks, will be in a position of paying any dividends and even of existing on the market in foreseeable future. Therefore, no deception can be claimed where they stop (or even do not start) paying dividends or disappear from the stock markets. Which means that the losses of hundreds of thousand or even millions participants in a mass privatization are fraud free. The same holds true about situations of hyper inflation.
Another way to view truth would be to compare a statement to a set of initial principles. If the given statement corresponds to that principle set, it is true and if not, it is false. In this case too, the principles could be manipulated in such a manner as to secure the correspondence of the needed statements and to avoid any hint of deception. For instance, an industry can be suggested being in bridge of the principles of doing a sustainable business. No surprise, this industry will be under the constant threat of eminent bankruptcy and no deception could be argued of when the bankruptcy really happens. Neither the losses of industry’s shareholders nor the gain of those who profited from the bankruptcy could be considered as fraudulent.

Finally, truth could be described as what is beneficial for a community or for the society as a whole. Any assertion and action which does not contradict this definition would be true. The money acquired from some activities could be spent highly beneficially on a certain community (but be disastrous for the rest of society) and in this sense not constituting deception; for this reason the above money producing activities will not be classified as a fraud neither the subsequent fund investment as a money laundering.

In all above cases, there is no deception. Nevertheless, fraud is present. What is the criterion for a fraudulent activity? Being illegal? But any statement and following action that is deception-free and does not rely on violence will comply with the letter of the law. To extend the scope of the law a judiciary is needed ready to identify something as a fraud on the ground of acquiring unjust gain and/or causing unjust harm no matter whether any deception is detected or not.

By Assoc. Prof. Alexander Gungov, Ph.D., Senior Consultant

To get the full analysis, please contact office@risksolution.org

Read this article on the website Click Here
Russian Amateur 'Web Detective' Interviewed on Successes in Finding Criminals

In the United States everybody knows about people once they have broken the law. If a gently smiling neighbor has served a sentence for rape, people are immediately warned: Bear this in mind, be careful. In Russia there might be drug dealers living in the next-door apartment -- the entire apartment block will know about it, but the neighborhood policeman will not have a clue. Our agencies are not coping with hunting down criminals, and so officials from the central Interpol bureau requested assistance from World Wide Web users because "in our time it is possibly much simpler in some cases to find a criminal on the Internet than in real life."

The success of Roman Romachev, who found eight individuals in four hours, exceeded all expectations. The Web detective talked to Moskovskiy Komsomolets reporters about his know-how.

[ Goncharova ] Roman, why did you respond to the appeal from the international police force? [ Romachev ] I decided that it was interesting and that I could be useful because I have been professionally involved in business intelligence on the Net for seven years now. In four hours on a popular social network I found eight individuals on the international wanted list being hunted not only by Interpol but also by the Republic of Kazakhstan Financial Police and the Republic of Belarus State Control Committee.

[ Goncharova ] But it is possible to "encrypt" yourself, to post a fake photo... [ Romachev ] I found not fakes -- that is, people who
register under assumed names -- but real people on the wanted list.

There were very good-quality photographs of them on the social networking site -- unlike the ones posted on the Interpol website and other law-enforcement agencies' sites. They openly identify their friends and constantly visit the site without fear of the law-enforcement agencies. I made screenshots from which it was clear that, for example, they were either "visiting" the social networking site at that moment or had been there the previous day. That means, it is not difficult to find these people.

[Goncharova] What did you do with this dossier? [Romachev] I decided to send it on to the proper destination -- to the Russian National Central Interpol Bureau.

Thanks to my long-standing FSB [Federal Security Service] connections and personal acquaintanceship with some high-ranking Interpol officers I made direct contact with the leader of the department that handles people on the international wanted list and talked about the situation. Particularly about the people that I had found. To begin with his response shocked me: He said that they had no such criminals on their database. We agreed to meet, and the following day I went to the National Central Interpol Bureau. I telephoned downstairs. He confirmed that, yes, such people were on the database.

[Goncharova] What kind of people are we talking about? [Romachev] There are two criminals who are being hunted by Costa Rica for committing a murder.

There is Mariya Kortina, who is being pursued by Interpol for the illegal acquisition, storage, and manufacture of narcotic substances and at the same time is relaxing on a beach in Spain with her family. And Konstantin Perepyatenko, who is being sought by Interpol on suspicion of crimes against the person's life and health, is currently living in Germany.

[Goncharova] Have they been arrested? [Romachev] No. The site indicates that Mariya is living in Spain; as she has Russian citizenship, the criminal should be extradited to our country. But
this is not happening for some totally unconvincing reason. Perepyatenko, however, has dual citizenship, and in accordance with the law Germany is not obliged to extradite him; plus he has now been sentenced to one year there for causing grievous bodily harm.

There is a complex system of interactions between countries. In Russia the question of extraditing individuals who have committed a crime is generally under the jurisdiction of the General Prosecutor's Office. All of this is clear and obvious, but I was struck by something else. That Interpol had absolutely no interest in the information that I had collected. They were not interested in the high-quality photographs. And the officials' tone was condescending: Leave us in peace, they said, this is of no interest to us.

[Goncharova] But are you not afraid? These are serious people, the international police are not pursuing them just for the fun of it. [Romachev] There are definite fears. So I am not identifying the pages of the two citizens who are being pursued for murder.

[Goncharova] If you found eight individuals in only four hours, so why can police officers not cope with this task? [Romachev] Our agencies are still very badly equipped. Many people simply do not know how to utilize modern technologies. I fussed like an old hen over the dossiers that I had collected.

In this connection all civil initiatives in Russia encounter bureaucratic obstacles and passivity on the part of representatives of the law-enforcement agencies.

[Goncharova] Did you look only on one social networking site? [Romachev] Yes. On it the owners of pages indicate their age -- this is convenient: Birth dates are indicated in police files. Although I do not rule out the possibility that quite a few other people are to be found on other social networks that are more popular, incidentally.

[Goncharova] You said that, in addition to the criminals that you found for Interpol, there were also criminals from Kazakhstan and Belarus. Are these states' law-enforcement agencies
interested in their whereabouts? [Romachev] In Belarus futile attempts were made to get through on the phone and convey the information. I asked a journalist acquaintance to obtain an official comment -- she was directed to the press service, where the telephones remained silent.

But in terms of Kazakhstan things worked out very productively, you might say. The people there were very interested in my information. They started to telephone regularly and consult about how to put together a request to the social networking site and how to track down lawbreakers through their IP address. The representative of the Republic of Kazakhstan Financial Police begged me not to name the criminals because detective measures are currently in place, and he also promised that in the future he will approach me for assistance in tracking down other violators.

[Goncharova] Are volunteer assistants' efforts rewarded in some way? [Romachev] Not in Russia. But in the United States the FBI pays a bounty for hunting down a criminal. If you remember the old westerns in which a substantial sum is offered for a criminal's head and a posse hunts him down, the situation nowadays has virtually not changed -- it is a lucrative business. There is a list on the FBI website of who is on the wanted list and how much will be paid for finding him. The FSB announced a reward for information about the suicide terrorists who blew up the Moscow metro, but this was a one-off action and, to the best my knowledge, this money has not been paid to anybody.

[Goncharova] Roman, do you intend to continue your "headhunting" in the future? [Romachev] Yes, this process has engrossed me very strongly. As the saying goes, "there is no such thing as a former [silovik]," and so, even on ceasing to serve in FSB agencies, I am continuing to stand guard over the economic security of the state, trying to protect entrepreneurs from relationships with fraudsters. In the West this business is very profitable because it is actively supported by the state. Some 70% of intelligence bureaus work for the state on an outsourcing basis.

Regulation E: Using It To Our Best Advantage To Reduce
Regulation E: Using It To Our Best Advantage To Reduce Our Client Based ATM Fraud Risk Without Affecting The Legitimate Client

Posted by Harry J Houck Jr. on October 7, 2011

Reg. E (specifically 205.11 Procedures for resolving errors) as those in the business who know like to call it is, in short, the law gives consumers protection and certain rights regarding claims of fraud and/or errors on their bank accounts.

When this provision was first established, it was a victory for the honest consumer because some banking institutions may have made it incumbent upon the consumer to prove they did not commit the fraud reported in their accounts resulting in denial of their claims. It is now incumbent upon the financial institutions to prove a consumer’s liability.

This regulation put the banks on notice that if they did not follow the regulation, they would be subject to unwanted scrutiny, heavy penalties and civil liability from banking regulators. These liabilities and penalties instilled fear in financial institutions, which resulted in a pay the claim attitude (then deny it, and take the loss.) This contributed to an existing atmosphere conducive to fraudulent behavior in this country or what I like to call “a fraudsters Disneyland.”

Naturally, what occurred is that some institutions became more vulnerable than others because their flawed investigative policy resulted in a reluctance to deny claims. Fraudsters and possibly terrorists too, target specific institutions because of their policies.

Some financial institutions are now advertising that they will reimburse fraud claims within 24 hours. This customer service issue will surely put a smile on the fraudsters face. It will make it easier to commit fraud and have the money credited to them even faster.

For those consumers that are true victims, I say that’s great and it should be done. However, between 15%-40% of ATM, Point of
Regulation E: Using It To Our Best Advantage
To Reduce Our Client Based ATM Fraud Risk
Without Affecting The Legitimate Client

Sale and Debit Card claims are from clients that require scrutiny. (Such claims are fraud reported within 90 days of the account opening, the 2nd or 3rd claim within a year and/or the claim of a client losing his card with the pin written down on the back of the card.)

It’s too easy to claim fraud in these situations, and once a provisional credit is issued the money is taken out of the account and the client disappears.

Could it be that financial institution’s loss prevention units aren’t very good at investigating fraud? Do they have the investigative acumen required?

There are so many claims, they cannot properly investigate every one; not to mention, the fear of denying a claim and the penalties of this regulation, which I believe after customer service is one of the reasons so many fraudulent claims are honored. This Regulation, although unintentionally, has created a sense of paranoia among financial institutions. Even in cases where claims such as these are denied, if the fraudster is smart enough and makes a complaint, some banks will usually pay these claims to avoid the cost or hassle of litigation. The Regulation does state that FI’s may not be held liable if they show good faith in their investigations. How many investigators are aware of this and are willing to take the steps to conduct this good faith investigation and deny the claim? How many investigators know what this means? It’s probably safe to say that most of the investigators on the loss prevention side of FIs aren't former law enforcement investigators nor do they know the Regulation.

Investigations are usually based on a checklist of questions that are inadequate. They rely on the Compliance and Legal Departments to make sure the Regulation is being followed. However, all too often it’s compliance that sets the pace looking at customer service as the broader perspective.

Case in point: A client made a claim with a bank stating that he left all his bank cards in his car when he was moving, and his car was broken into and all the cards were taken when he was on vacation in Florida. He stated that he had the pin numbers
written down on an index card with all his cards in the car. All were in the same box that was stolen and monies were taken from all the cards via ATM machine withdrawals over a 10-day period. Total claims made on all seven institutions involved over $80,000. After my initial interview, I contacted the six other institutions involved, which also included a major brokerage company. All the institutions you would know by name. All six told me that they were paying this claim because they didn’t want to violate the Reg. I asked all the institutions to hold off on paying the claim and within days I could deny his claim. It turned out this client was never on vacation in Florida at the time of the fraud; he was at work. I found several inconsistencies in his statements to me. A further interview revealed that he lied about the claim, and that he was the one who made the fraudulent transactions. As a result, all the institutions involved denied his claim, and a FBI investigation was later conducted. How much work did this take: maybe 10 calls and 3 - 4 man-hours over a 3-day period? The cost of denying this $80,000 claim was about $300.00; not bad, right. I have no problem investing $300 dollars to save $80,000. Do you? During my investigation, I never violated the Reg. Why? I conducted a good faith investigation. This denial could and would stand up to any scrutiny by regulators. I proved that the client was the “bad guy.”

A common argument made by bankers is: “We made $150,000,000 last year and $2,000,000 of those were losses due to fraud. No big deal. It’s the cost of doing business.” This way of thinking is way outdated and requires a major paradigm shift. For example, $2,000,000 in losses this year makes the fraudsters want to double it next year because we made it much easier for them this year and it will be even easier the next. Especially vulnerable are small banks that cannot absorb such losses. They pour more resources into the investigative side, or they make the wrong decisions and deny a legitimate claim by a client leaving them wide open for the sting of the regulators for violation of the Reg.

With fraud on the rise year after year, it’s going to eventually get to unacceptable levels. It appears that the more technologically
advanced we get in the industry the more vulnerable we become. Investigating the non-client fraudster is hard enough and with the resources available to the Criminal Justice system we cannot seem to ever get a lid on that problem and probably never will. Law Enforcement is inundated with fraud cases that are at uncontrollable levels. We cannot depend on the statistics we read about regarding ID Theft because most fraud is not reported to the police. Customers who become victims usually just call the bank, and their claim is paid. They see no reason to go to the police; they see it as the bank’s problem. It seems to me that we can put a lid on client-based fraud, and it is easily investigated. We do have the ability to control it if we want, in a cost-effective manner.

We also, to a certain extent, need to make consumers responsible for some of their actions. It’s my opinion that if someone writes their PIN number on the back of a bank card, they are indeed compromising that information and should be liable for any loss incurred as a result of that card’s loss. Now, I know fraud investigators agree with me here.

However, Regulation E does not. This is a common sense issue. I mean really, let’s wake-up! A police report of the fraud should be required.

We can’t be willfully blind to the fact that financial fraud is not affecting us. If we wait to properly address the situation, it may be too late. When I was a detective with the NYPD investigating ID theft in three years I saw the complaints more than triple and, of course, these are just the persons who make a report; most don’t.

When I was a VP at Citibank, I developed and instituted a new Regulation E investigation unit called the Major Incident Unit. In short, this innovative investigative process that I developed significantly reduced Citibank’s client based fraud exposure. Let’s put it this way, if you’re a client at Citibank looking to make a false claim, it’s over for you. The unit was so successful they tripled the unit’s manpower. When McKinsey & Company saw what I was doing they said my investigative process should be
“best practices”, and that no other bank had such a process that they were aware of.

Let me be clear, I’m not saying that Reg. E is bad, nor is it responsible for most of the fraud that exists today, but it makes a considerable contribution to client based fraud.

It needs to be amended to deal with today’s specific financial fraud threats.

Protecting the consumer’s rights is paramount; however, a more common-sense approach needs to be implemented.

Fraud and identity theft in this country are out of control to the point where sooner, or later it will affect the bottom line of banks worldwide, or the consumer will pay for the losses with bank fees. Is that good customer service?

How will changes in the Regulation help the consumer? It will help by reducing the financial institutions fraud exposure and losses; therefore, the bank saves money and this will stabilize or reduce their cost of doing business and trickle down to the consumer. It will significantly reduce client-based fraud and the possibility of terrorist financing.

In light of the new federal regulations coming into effect this year for cards, losses are even more important to the bottom line. This is an area that banks can recoup millions of dollars every year depending on their losses.

Some bankers say we can’t have the best of both worlds, I say we can, and I have proven it

Read this article on the website **Click Here**
Risk managers whose companies have trade secrets (inventions, methodologies, formulae, codes and even processes) face not only a growing threat of theft (especially cyber theft) but also odd quirks and exceptions in the law. By definition, a trade secret has to contain some unique set of pieces that gives their owners a competitive advantage but are also original. This means that even processes like customer data or marketing plans and forecasts can be defined under the umbrella of trade secrets.

But there is a problem.

Do you get protection under the law merely by registering a trademark, patent or copyright? No. Various legal cases have been ruled against trade secret owners solely because a company did not take steps or precautions to protect its secrets. This means you need to tell employees they cannot take trade secrets, and the protection within systems has to be tight. You also have to limit access to secrets to only those with a need to know.

In one case, *J.P. Healy & Son, Inc. v. James A. Murphy & Son, Inc.* 357 Mass. 728. 737-38 (1970), the decision of the court stated that "The essential characteristic of a trade secret [is] secrecy... individuals must be constantly admonished that a process is secret and must be kept so."

This odd rule means that unlike tangible assets, trade secrets can be stolen and the action defended on the basis that the company did not warn employees. If this were applied to tangible assets, the world would be even more chaotic than it is. For example, a thief could drive a car off the dealer lot and defend his action by saying, "The dealer left the keys under the floor mat, so I was justified in taking the car." The court would then rule that the dealer had not taken adequate precautions, so the thief is allowed to keep the car.

As odd as this is, it points out the difficulty of applying the law to intellectual property. It might not get any better as we move more
and more into the cyber world and place valuable trade secrets in the cloud. Could it be in the future than a trade secret their would argue that this by itself was rationale for a theft? If your cloud is not secure enough, are you exposing your trade secrets to anyone who can figure out how to steal them?

Read this article on the website Click Here
Bulgarian Competition Law is designed to protect and foster competition and free enterprise in economic activity. Over the years the law was repeatedly changed by the legislature to meet the requirements of economic life.

Bulgarian Competition law provides protection against agreements, decisions and concerted practices, abuse of monopolistic and dominant and all other acts and actions that can lead to the prevention, restriction or distortion of competition in the country and / or affect trade between Member – States the European Union as well as unfair competition. The Act regulates the control of concentrations between undertakings. This law regulates relations concerning the application of Art. 81 and 82 of the Treaty establishing the European Community including cooperation with the European Commission and national competition authorities of the Member – States of the European Union under Regulation (EC) 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Art. 81 and 82 of the Treaty establishing the European Community, hereinafter referred to as “Regulation (EC) 1/2003 ‘, and Regulation (EC) 139/2004 of 20 January 2004 on the control of concentrations between undertakings (Merger Regulation EC), hereinafter “Regulation (EC) 139/2004.”

Bulgarian Competition Act shall apply to:

- undertakings and associations of undertakings which operate in the Republic of Bulgaria or abroad, unless expressly or tacitly prevent, restrict, distort or may prevent, restrict or distort competition in the country;

- state bodies, including executive authorities and local government, if they expressly or tacitly prevent, restrict, distort or may prevent, restrict or distort competition in the country;
FRAUD, BUSINESS RISKS, LAW

- undertakings to which the state or municipality is assigned to perform the services of public interest, insofar as the application of the law is not law or in fact the tasks assigned to them, and competition in the country is not affected significantly;

- individuals who commit or facilitate the commission of an offense under this Act.

The Act created the Commission for Protection of Competition. The Commission is the national body of the Republic of Bulgaria, responsible for the implementation of Community law on competition.

The Act prohibits any agreements between undertakings, decisions by associations of undertakings and concerted practices of two or more undertakings which have as their object or effect the prevention, restriction or distortion of competition in the market, such as:

- directly or indirectly fixing prices or other trading conditions;

- share markets or sources of supply;

- limit or control production, marketing, technical development or investment.

- applying dissimilar conditions to identical contracts to certain partners, thereby placing them at a competitive disadvantage;

- making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations or additional contracts which by their nature or according to commercial usage have no connection with the subject of the main contract or its performance.

It is forbidden to conduct businesses with monopoly or dominant position as well two or more undertakings of dominant position, which may prevent, restrict or distort competition and affect the interests of consumers, such as:
- directly or indirectly imposing prices for the purchase or sale or other unfair trading conditions;

- limiting production, trade and technical development to the prejudice of consumers;

- applying dissimilar conditions to identical contracts to certain partners, thereby placing them at a competitive disadvantage;

- making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations or entering into additional contracts which by their nature or according to commercial usage have no connection with the subject of the main contract or its performance;

- unreasonable failure to supply goods or provide service to real or potential client to hinder the attainment of its business.

The Act prohibited any act or omission in the course of business which is contrary to good commercial practice and harms or may harm the interests of competitors.

Shall be prohibited to damage the reputation and credibility of the competitors and their products or services by stating or disseminating untrue information, as well as by presenting the facts in a distorted form. Shall be prohibited to mislead in relation to essential characteristics of goods or services on or use of the goods or the provision of services by alleging false statements or misrepresenting facts.

It bans misleading and unlawful comparative advertising.

Advertiser and advertising agency prepared the ad, are liable for misleading and unlawful comparative advertising.

The offering of goods or services, appearance, packaging, marking, name or other characteristics which mislead or might mislead as to the origin, producer, seller, manner and place of manufacture, source and manner of acquisition or use quantity, quality, nature, consumer characteristics and other essential characteristics of the product or service is prohibited.

**LIABILITY AND PENALTIES**
For breaking the law are provided penalties, some of which are:

- Commission imposed a penalty of up to 10 per cent of total turnover for the previous financial year of an undertaking or association of undertakings.

- Individuals contributed to the performance of violations under the Act if the act constitutes a crime shall be punished with fine from 500 to 50 000 BGN.

If you believe that your rights under this Act have been violated please contact us. We are ready to help you.

Read this article on the website [Click Here](#)
Occasionally the SEC and other regulators will castigate, actually punish, fraudulent events on Wall Street. Of course the real punishment is only meted out to individuals and small companies. Mega banks – the banking mafia – are largely immune.

Martha Stewart was convicted of insider trading in 2004 – a relatively small amount – and was sent to jail. It was an act of fraud alright, but it pales in comparison to the fraud of Wall Street banks.

Phil Falcone, a once high flying hedge fund manager, was just charged with fraud and it sounds like the regulators will throw him in jail for a very long time. Among other allegations, Mr. Falcone was charged with “granting favorable redemption and liquidity rights to certain strategically-important investors in exchange for those investors’ consent to restrict redemption rights of other fund investors” and “Falcone and two Harbinger investment managers through which Falcone operated manipulated the price and availability of a series of distressed high-yield bonds…”

Remember, like Martha Stewart, the government wants to throw Phil Falcone in jail and maybe he belongs there; but what about the mega banks?

Barclays was found guilty of MANIPULATION (like Falcone) and giving PREFERENTIAL TREATMENT to certain clients (like Falcone) but nobody is going to jail. Moreover, Barclay’s fraud was on a colossal scale, unlike Martha Stewart, and again I say: nobody is going to jail.

From the FSA’ breakdown of Barclays traders caught in the act of manipulation:

On Friday, 10 March 2006, two US dollar Derivatives Traders made email requests for a low three month US dollar LIBOR submission for the coming Monday:
i. Trader C stated “We have an unbelievably large set on Monday (the IMM). We need a really low 3m fix, it could potentially cost a fortune. Would really appreciate any help”;

ii. Trader B explained “I really need a very very low 3m fixing on Monday – preferably we get kicked out. We have about 80 yards [billion] fixing for the desk and each 0.1 [one basis point] lower in the fix is a huge help for us. So 4.90 or lower would be fantastic”. Trader B also indicated his preference that Barclays would be kicked out of the average calculation; and

iii. On Monday, 13 March 2006, the following email exchange took place:

Trader C: “The big day [has] arrived… My NYK are screaming at me about an unchanged 3m libor. As always, any help wd be greatly appreciated. What do you think you’ll go for 3m?”

Submitter: “I am going 90 although 91 is what I should be posting”.

Trader C: “[…] when I retire and write a book about this business your name will be written in golden letters […]”.

Submitter: “I would prefer this [to] not be in any book!”

And further…

Trader C requested low one month and three month US dollar LIBOR submissions at 10:52 am on 7 April 2006 (shortly before the submissions were due to be made); “If it’s not too late low 1m and 3m would be nice, but please feel free to say “no”… Coffees will be coming your way either way, just to say thank you for your help in the past few weeks”. A Submitter responded “Done…for you big boy”.

And further it goes…

On 6 August 2007, a Submitter even offered to submit a US dollar rate higher than that requested:
Trader F: “Pls set 3m libor as high as possible today”

Submitter: “Sure 5.37 okay?”

Trader F: “5.36 is fine”

And further…

On Thursday 14 December 2006, Trader F emailed a Submitter, requesting a low three month US dollar LIBOR submission for the following Monday, 18 December 2006; “For Monday we are very long 3m cash here in NY and would like the setting to be set as low as possible…thanks”. The Submitter instructed another Submitter to accommodate the request; “You heard the man” and confirmed to Trader F “[X] will take notice of what you say about a low 3 month”.

Two seconds later, that Submitter sent himself an electronic calendar reminder to make a low three month submission at 11 am on Monday 18 December 2006: “USD 3mth LIBOR DOWN”.

And further it goes…

For example, on 26 October 2006, an external trader made a request for a lower three month US dollar LIBOR submission. The external trader stated in an email to Trader G at Barclays “If it comes in unchanged I’m a dead man”. Trader G responded that he would “have a chat”. Barclays’ submission on that day for three month US dollar LIBOR was half a basis point lower than the day before, rather than being unchanged. The external trader thanked Trader G for Barclays’ LIBOR submission later that day: “Dude. I owe you big time! Come over one day after work and I’m opening a bottle of Bollinger”

And further…

Trader E communicated with traders at Panel Banks 1, 2 and 6 in advance of the IMM date. For example on 12 February 2007, Trader E stated in an instant message with a trader at Panel Bank 6:
“if you know how to keep a secret I’ll bring you in on it […] we’re going to push the cash downwards on the imm day […] if you breathe a word of this I’m not telling you anything else […]

I know my treasury’s firepower… which will push the cash downwards […] please keep it to yourself otherwise it won’t work”.

And further the FRAUD goes…

Various instant messages exchanged after the final benchmark rates were published on 19 March 2007 indicated that the traders involved considered that their strategy had been successful. Trader E commented to the external trader at Panel Bank 6 “this is the way you pull off deals like this chicken, don’t talk about it too much, 2 months of preparation […] the trick is you must not do this alone […] this is between you and me but really don’t tell ANYBODY”.

LIBOR is a major international interest rate used for rate calculations that may have affected you. Let’s see; if you had and ARM loan at any time from 2005 until today, or student loans, or car loans…or any damn loan…you may have been harmed by this outrageous and blatant FRAUDULENT activity! In fact, LIBOR sets the interest rate for $350 TRILLION in interest-rate sensitive products.

So what was the penalty you’re wondering? The usual for big banks: a small fine of $200 million and a “promise” to never do it again.

Why isn’t Phil Falcone being fined $1 million and why wasn’t Martha Stewart fined about $10,000? Oh yeah, they aren’t mega banks like Barclays, JPM, Shitibank, and Goldman Sachs.

If the government refuses to put one person in jail for this scandal, I personally hope Barclays is sued into permanent bankruptcy – never to rise again.

*Trade well and follow the trend, not the so-called “experts.”*

Read this article on the website [Click Here](#)
The referendum (19 March) on the constitutional reforms in Egypt was held in compliance with the state laws. Certain violations at a number of polling stations were reported but they were insignificant and could not affect the final outcome. Nearly 18.5 million voters (41.1% of those eligible 45 million Egyptians) turned out. Of these 77.2% (14.2 million) voted in favour of the reforms and with ca. 23% (4 million)- opposed. These results can be considered as a successful test for what the sentiments of the Egyptian society before and during the parliamentary elections (most probably in September this year) will be like.

Some preliminary estimates of the shares of the participating parties, movements and individual politicians in the votes were confirmed. The constitutional reforms were backed by the biggest opposition power “The Muslim brotherhood” /MB/ and its coalition partners the “Salafist, movement, “Al Jama’a Al-Islamiya”, the newly established moderate Islamic party “Al-Wasat” close to MB and others. The conservative National Democratic Party /NDP/ of the stepped-down President Hosni Mubarak also voted in favour of the reforms. Obviously the reasons for backing the reforms are different for the biggest political players although they have one common reason too – both political powers win by shortening the period until the elections by evading the cardinal problems or stated in other words by delaying the cardinal constitutional reforms. This actually leads to postponing of the essential constitutional changes.
MB retains its well built organizational structure in the country as well as its followers. It remains the only major oppositional force in the political sphere. The organization prefers the elections to be held sooner which will prevent the remainder of the opposition and the remnants of the previously ruling NDP from regrouping. Otherwise it is possible that an alternative player shows up which can cause a serious competition in the elections. There is some talk already about the planned formation of the political party “Freedom and Justice” with the purpose to broaden the support by the population for MB and for its entering the political life in Egypt. A prerequisite for the speedier legal formation of the party is the present constitution to remain in force rather than suspended.

NDP benefits from the approval of the constitutional reforms too. Giving its vote it relies on retaining its dwindling number of supporters and on rallying the party before the parliamentary elections. The enactment of an amended Constitution preserves the status quo to a certain extent thus extending time to the party for reorganizing itself, for expelling the discredited party members, for reinforcing its structures in the country and for the endorsing its image of a reformed party. Failing to convince the public in its new inception NDP can most probably share the destiny of many failed parties – to be officially dissolved and voices to this effect can already be heard in the political spheres.

The parties, movements and the politicians (the liberal “Al Wafd” party, the left “Al Tagammo” party, the 8.5 million Copts and the two main Presidential candidates – the Secretary General of the Arab League Mr. Amr Moussa and the former Director General of the International Atomic Energy Agency and opposition leader Mr. ElBaradei demand substantial constitutional and democratic reforms and not barely political cosmetics, voted “against”. The necessary extended time for the drafting of a new Constitution gives a chance to these parties and movements to have longer time to prepare for the elections, to complete its party structures and to receive their public endorsement in the Egypt political sphere.
The referendum clearly demonstrated that MB is the new political force in Egypt. Most probably it will dominate the newly elected Parliament and dictate further political changes in the country. The formation of the “Freedom and Justice” party within days can be expected. With the declared open doors for party members from the whole social spectrum in the country it will further expand the MB influence. The future foreign policy orientation of Egypt will depend on what the future behavior of the movement and of its concomitant party will be.
The spontaneous revolutions in the Arab countries resulted in the deposing of the despotic regimes in some of them, while in others /Jordan, Syria, Libya/ they grow in scale through armed clashes and mass peaceful protests aiming the final removal of the discredited rulers. This wave of discontent can possibly incite certain forces in some of these countries to redraw the borders in the region as they were determined with the participation of the European powers in 1916-1922. These borders were later shifted during the Iraq war /some ethnic enclaves arose/ and the Israeli withdrawal from Gaza. There HAMAS took control after parliamentary elections. With the signing of the Camp David Peace Accords between Israel and Egypt /March 1979/ the period of expectations of achieving a final lasting peace in the Middle East set in. Since then until the present moment the parties in the conflict /Israel, Egypt and the Palestinian Autonomy (PA)/ participate with varying persistency in negotiations recognizing that the eventual successful conclusion of the Israeli-Palestinian dialogue is the key for solving the problems. Currently, however, under the impact of the wind of changes preconditions for revising the foreign policy targets of the negotiating countries arise and the outline of additional difficulties emerges resulting from government changes.

The upheavals in the area were unexpected and they took the political strategists in Israel by surprise. The government missed its chance to respond in due time and in accordance with the changing environment. The prognostics assessment and the intentions for interactions in the new political reality were delayed for a long period of time. No matter what steps will be taken from now on it is important to realize that the region becomes subordinate to new political rules. This state of affairs requires new strategic thought and preemptive decision making and not merely following the events.

The peoples’ aspirations for reforms and democratic changes in the countries affected by the revolutions come into conflict with
the popularly constructed notion that these people are undeserving and immature and they are inapt to achieve their purpose. Obviously the mass disturbances vented certain amount of the accumulated pressure but unfortunately they can still not nominate stable political leaderships. Two possible scenarios for getting the processes under control are emerging in Egypt affected by the Revolution of 25 January- with the military or with the ascend of the radical Islamists of Muslim Brotherhood (MB) to power. By the first one the parting with the military is imminent as they are identified with the previous status quo and they are not anticipated to justify the expectation for reforms. In view of this the people’s attention logically turns to the second possibility – the representatives of MB /HAMAS in the Palestinian Autonomy, Hezbollah in Lebanon etc./. HAMAS is a vivid example of political metamorphosis by which the admittedly terrorist and supported by Iran Shiite organization was transformed into a political force. Judging by the dynamics of the developing processes it can be ascertained that is a matter of tactical evaluation by the radical Islamic movements /Egypt and Tunisia/ when the time for assuming power to set in. And what is more Israel especially has to live with the notion that the Islamic regime which will eventually come to power in Egypt will try to receive an international recognition. On account of this it can be expected that the new government will not denounce the peace treaty with Israel but will rather take action for its subversion. The analyses and assessments show that the troubles for the countries participating in the negotiations will begin with the replacement of the secular regimes by the rule of the radical Islamic movements. Despite of the Islamic diversity the individual subjects are united by the common ideas that the religious law (the Sharia) must be adopted in the countries and that the “infidels” must be fought.

One of the topics of the Israeli-Palestinian dialogue is the creation of an independent state Palestine with capital East Jerusalem. It can be expected that its decision can be abandoned for a very long time by eventual similar political development in the neighbouring Hashemite Kingdom. It has to be taken into consideration that Israel has its longest border with Jordan in
close proximity to which many Jews live. The eventual downfall of the King’s regime will affect the dialogue worse than Hosni Mubarak’s fall from power.

As a whole the Palestinians will feel more and more the support of Egypt including for averting the attacks on the Gaza strip. For the first time since many years a genuine satisfaction was felt at the official statement of the new Egyptian government on the last Israeli air attacks on the Gaza strip. It is caused mainly by the resolute tone of the new Foreign Minister of Egypt Mr. Nabil El-Arabi, despite that Egypt is currently occupied with its internal problems and has temporarily abandoned its relations with Israel. Simultaneously eventual military operations in Gaza will provoke reaction and protests in Cairo which will have to be addressed by the Supreme Council of the Armed Forces. The problem is that the rule is no longer in the hands of the convenient Hosni Mubarak and Omar Suleyman.

It can be anticipated that the Israeli-Palestinian dialogue faces new difficulties analyzing the current processes in the Middle East and the prospects for their development. Israel lost its moderate partners-mediators with the Palestinians in the persons of the former President Hosni Mubarak and the present Vice President Gen. Omar Suleyman.

The probability the power in Egypt to pass in the hands of the radical Islamists after the parliamentary elections in September this year is high. It is expected that this will result in a tougher policy towards Israel and in provoking either suitable real steps towards the solution of the controversial issues in the dialogue / the return of the Palestinian refugees, the creation of Palestinian state, releasing the Palestinian prisoners/ or in discontinuing the negotiations for an indefinite period of time.

Read this article on the website Click Here
Clarity in discussions of risk

Best questions, Debate & Opinions

Clarity in discussions of risk

Posted by Andre Mirabelli on May 30, 2011

A couple of distinctions I would like to see more attention paid to, so that it is always clear what is being addressed;

1. Ex ante prediction of risk (e.g. the probabilities assigned to possible future results)

vs.

Ex post evaluation of past risk (i.e. the experienced impact of actual past outcomes or implementations).

2. The uncontrollable risk that each various aspect of the world (market) creates for you, given that you have put yourself in a particular situation (If I do all this, how can I expect this particular aspect of the world to affect me?)

vs.

the controllable risk that each aspect of your decision process creates (created) in putting yourself into a particular situation, given that the world (market) does (did) what it does (did) (If the world as a whole acts like this, how can I expect this particular decision to change things for me?).

I believe that it can be helpful to understand the past impact of each clearly differentiated kind of our own controllable past decisions when we are trying to predict what uncontrollable things will happen to us upon making different future decisions. What can be properly measured can be better controlled and improved.

Read this article on the website Click Here
The value of healthy debate to risk managers

Posted by Michael C. Thomsett on July 14, 2011

The question of how to manage risks is a complex one. It is not cut-and-dried like we might want. It gets boggled down in budgetary disputes, political beliefs and loyalties, economics, and private agendas.

The best way to contend with the difference of opinion is through open and honest debate. There is no flaw in disagreeing with someone, but we can all learn from respectfully listening to others and understanding how and why their point of view is different. Taking absolute positions blinds all of us from being able to learn and grow, and so this debate is valuable to everyone.

For example, in recent blog posts I have made observations based on economics and especially on varying systems of economic control. The free market versus government oversight is one of my favorite topics. I do believe that when government tries to fix perceived or real problems within the private sector, it tends to over-regulate, operate inefficiently, and as often as not to make matters worse. This has led to a spirited but respectful debate, a trend I enjoy seeing because it enlightens all sides.

There are many appropriate government actions that offset private sector abuses. Some industries and individuals have exploited the system in a shameful manner and deserve to be investigated, fined and in some cases sent to prison. This does not mean that more regulation and more penalties are always the best solution.

Where is the balance? Surely it is possible to temper the balance between the desirability of free markets and the necessity of government regulation. Or is this only a dream? Well, at the very least we can all agree to debate issues and learn from one another. This makes all of us wiser and more effective. No one needs to be right or to "win" the debate; it is enough to enter into the dialogue.
The value of healthy debate to risk managers

Read this article on the website Click Here
What skills are most in demand in Risk Management now, either because they are in short supply, or there is excess demand?

Posted by Boris Agranovich on December 4, 2010

I'm looking for some market intelligence... what area is growing fast and in what geographies. Is it because there isn't enough talent, or there is excess demand?

I was asked many times this question and I just want to hear the real practitioners’ opinion so everyone can contribute and profit from the crowd sourcing.

My guess- IT related implementations, compliance, Basel III, ERM, counterparty risk, programming and Quant skills

Looking forward for your active participation.

Read this article on the website Click Here
How to identify Business Model Risk & Weaknesses?

Posted by Peter Deans on September 27, 2011

I am doing research for an upcoming article I am writing on Business Model risk. I would be interesting in hearing members' thoughts on the following:

1. Is this an activity that should only be confined to the Strategic Planning phase or is it a core activity of Risk Management?

2. How do you identify businesses that are performing strongly but that may have a Business Model that is fundamentally flawed?

3. What types of action can be taken to have Business Model risk debated. The rise of subprime products in retail and investment banking is of course one of the best Business Model risk case studies I can think of.

Read this article on the website [Click Here](#)
The effect on cultural adoption, of risk management, of production control

Recently, I have focused on risk production and control.

Reading through the various regulations and proposals, errors, in the market and credit risk production itself, fall into, and get a little lost within, the op risk side of life. My main issue with this is that far from being an economic capital driver, good risk production control is the central plank in establishing an adoptable risk culture in any firm.

My main fear is that the general, and understandable, focus on meeting the regulatory changes has been at the cost of moving forward with better risk controls.

Effectively, if the lack of risk as a cultural imperative within financial firms is a major contributor to the recent crisis, then its correction should be a major driver in the aftermath. It is difficult to see how there can be any serious adoption, or buy in, from the stakeholders of risk, if the numbers themselves cannot be trusted, or at least correct quickly, once errors have been detected.

From what I have read, most of the control functions are around the trading itself, with risk incentives being in the form of punative measures such as CVA or IRC (sticks rather than carrots). On the risk side itself, it has all been about the capital numbers (again, sticks over carrots), with CVA, IRC, Stressed VaR, DSR etc.

I have always felt that making the risk numbers useful from a strategic point of view, which means that they are genuinely useful in terms of planning, would put risk at the heart of a firm in a far more 'sticky way' than simply making it a capital issue (which leads, in part, to increasing product sophistication and model/complexity arbitrage). It does require, however, that the numbers are either correct, or quickly correctable, and therefore trusted.
As I said, this has been a main focus for me and my firm for a while. I would love to hear other folks' opinions.

Read this article on the website Click Here
I am working on a Thesis involving RM Maturity Model.

Found the RKSM model within CMMi and the M_o_R model.

Additionally I found some "commercial" Maturity Models.

Anyone who can give me some references or pointers?

Thanks,

Stef
Can anyone pls explain with examples about

1. Safety statistics
2. Safety planning control

Looking forward for early and detailed response

Thanks & Regards,

Annus

Read this article on the website Click Here
Difference between Elimination and Substitution in Risk reduction.

Posted by Annus uddin Khan on December 15, 2010

Can anyone tell me the difference between the risk elimination and risk substitution..

For example: if we remove the source of risk introduce new thing which has less or no risk as previous then what would we say? Is it elimination or is it substitution?

pls explain with practical examples

Thanks & Regards,

Annus

Read this article on the website Click Here
What is the recommended "fundamental" Risk Management training?

Posted by maynardo lalo on September 15, 2010

When I started handling Risk Management, I first took on its Disaster Recovery and Info Security aspects as an MIS manager. Later, I branched out into Business Continuity Planning as well. With my current role taking on Corporate Governance and Compliance as well, it helped that I was exposed in most parts to the practical application of these concepts. Needless to say though, am still looking out for an omnibus training that encompasses the totality of Risk Management. Appreciate then recommendations from the members. Thanks!

Read this article on the website Click Here
SUPPLY CHAIN

Supply chain

Finding those weakest links

Posted by Michael C. Thomsett on May 29, 2011

Many years ago I was working on a book ("Little Black Book of Project Management," Amacom Books -- http://tinyurl.com/3at72s7) and developed a format for flowcharting in which the processes move left to right. This enables the preparer to identify separate people, departments or teams ("areas of responsibility") in their own rows as well as time along the bottom and a drop-down for any documentation developed as part of the process. It also facilitates concurrent process lines, so you can see at a glance that multiple processes move along at the same time. The whole system of horizontal flowcharting is visually efficient and effective.

However, I discovered something far more valuable and it has application in supply chain risk management.

The most likely point in a process for a failure to occur is at any point where the process is transferred from one area of responsibility to another. These are the weak-links in the chain. For example, one department or team may be responsible for many steps before the next step passes on to another department, person or team. This is the point where failure most often occurs, in the form of slow-down or outright stops, errors, or miscommunication of steps and deadlines.

SCRM is made the most efficient, and risks reduced effectively, when internal controls are focused on these weak-link points. A complex SCRM program may be overwhelming when the sheer number of steps in the process makes monitoring impossible. But when you focus on the weak links, you will prevent and control the vast majority of potential failures.

Read this article on the website Click Here
Managing the supply chain via tax policy - a controversial topic

Supply chain risk management is based on a series of assumptions, of course. But among these is an often overlooked issue: national taxation and how that affects the distribution of the supply chain itself (and thus, risk).

The U.S., for example, once the strongest manufacturing country in the world, today has the second highest corporate tax rate among industrialized countries. The U.S. is losing its competitive edge as a result.

**OECD Corporate Tax Rates - Federal Plus Provincial/State, 2007 and 2008**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Japan</td>
<td>39.54</td>
<td>39.54</td>
<td>0.0</td>
</tr>
<tr>
<td>2</td>
<td>United States</td>
<td>39.25</td>
<td>39.26</td>
<td>0.0</td>
</tr>
<tr>
<td>3</td>
<td>France</td>
<td>34.43</td>
<td>34.43</td>
<td>0.0</td>
</tr>
<tr>
<td>4</td>
<td>Belgium</td>
<td>33.99</td>
<td>33.99</td>
<td>0.0</td>
</tr>
<tr>
<td>5</td>
<td>Canada</td>
<td>33.50</td>
<td>36.12</td>
<td>-2.6</td>
</tr>
<tr>
<td>6</td>
<td>Luxembourg</td>
<td>30.38</td>
<td>30.38</td>
<td>0.0</td>
</tr>
<tr>
<td>7</td>
<td>Germany</td>
<td>30.18</td>
<td>38.9</td>
<td>-8.7</td>
</tr>
<tr>
<td>8</td>
<td>Australia</td>
<td>30.00</td>
<td>30.0</td>
<td>0.0</td>
</tr>
<tr>
<td>9</td>
<td>New Zealand</td>
<td>30.00</td>
<td>33.0</td>
<td>-3.0</td>
</tr>
<tr>
<td>10</td>
<td>Spain</td>
<td>30.00</td>
<td>32.5</td>
<td>-2.5</td>
</tr>
<tr>
<td>11</td>
<td>Mexico</td>
<td>28.00</td>
<td>28.0</td>
<td>0.0</td>
</tr>
<tr>
<td>12</td>
<td>Norway</td>
<td>28.00</td>
<td>28.0</td>
<td>0.0</td>
</tr>
<tr>
<td>13</td>
<td>Sweden</td>
<td>28.00</td>
<td>28.0</td>
<td>0.0</td>
</tr>
<tr>
<td>14</td>
<td>United Kingdom</td>
<td>28.00</td>
<td>30.0</td>
<td>-2.0</td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td>Value 1</td>
<td>Value 2</td>
<td>Change</td>
</tr>
<tr>
<td>---</td>
<td>-----------------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>15</td>
<td>Italy</td>
<td>27.50</td>
<td>33.0</td>
<td>-5.5</td>
</tr>
<tr>
<td>16</td>
<td>Korea</td>
<td>27.50</td>
<td>27.5</td>
<td>0.0</td>
</tr>
<tr>
<td>17</td>
<td>Portugal</td>
<td>26.50</td>
<td>26.5</td>
<td>0.0</td>
</tr>
<tr>
<td>18</td>
<td>Finland</td>
<td>26.00</td>
<td>26.0</td>
<td>0.0</td>
</tr>
<tr>
<td>19</td>
<td>Netherlands</td>
<td>25.50</td>
<td>25.5</td>
<td>0.0</td>
</tr>
<tr>
<td>20</td>
<td>Austria</td>
<td>25.00</td>
<td>25.0</td>
<td>0.0</td>
</tr>
<tr>
<td>21</td>
<td>Denmark</td>
<td>25.00</td>
<td>25.0</td>
<td>0.0</td>
</tr>
<tr>
<td>22</td>
<td>Greece</td>
<td>25.00</td>
<td>25.0</td>
<td>0.0</td>
</tr>
<tr>
<td>23</td>
<td>Switzerland</td>
<td>21.17</td>
<td>21.32</td>
<td>-0.1</td>
</tr>
<tr>
<td>24</td>
<td>Czech Republic</td>
<td>21.00</td>
<td>24.0</td>
<td>-3.0</td>
</tr>
<tr>
<td>25</td>
<td>Hungary</td>
<td>20.00</td>
<td>20.0</td>
<td>0.0</td>
</tr>
<tr>
<td>26</td>
<td>Turkey</td>
<td>20.00</td>
<td>20.0</td>
<td>0.0</td>
</tr>
<tr>
<td>27</td>
<td>Poland</td>
<td>19.00</td>
<td>19.0</td>
<td>0.0</td>
</tr>
<tr>
<td>28</td>
<td>Slovak Republic</td>
<td>19.00</td>
<td>19.0</td>
<td>0.0</td>
</tr>
<tr>
<td>29</td>
<td>Iceland</td>
<td>15.00</td>
<td>18.0</td>
<td>-3.0</td>
</tr>
<tr>
<td>30</td>
<td>Ireland</td>
<td>12.50</td>
<td>12.5</td>
<td>0.0</td>
</tr>
<tr>
<td></td>
<td>OECD Average</td>
<td>26.6</td>
<td>27.6</td>
<td>-1.0</td>
</tr>
</tbody>
</table>

*Source: Organization for Economic Co-operation and Development (OECD)*

The problem here is related directly to supply chain risk management. If the taxing system is viewed as an economic punitive tool, then charging profitable corporations a high rate of tax on profits is satisfying in the short run. However, it has a profoundly negative impact over time. Organizations heavily taxed are likely to outsource a majority of manufacturing to countries charging lower taxes, and even to locate subsidiaries or entire companies in countries where taxing policies are less punitive.

So companies like Halliburton, Accenture, Ingersoll-Rand, Tyco, Foster Wheeler, Cooper Industries, Global Crossing, Noble Drilling, Seagate Technology and Nabors Industries -- once large
U.S.-based corporations -- all left the U.S. to set up shop in places like the UAE, Bermuda, and the Cayman Islands. Their primary motive was to escape high U.S. tax rates.

Several benefits would accrue to the U.S. if corporate tax rates were lowered, even down below 15%. The obvious would be an improved overall private sector environment and job growth. A secondary effect would be that the U.S. would get back the lost tax revenue and,ironically, perhaps even higher levels of revenue due to improved productivity and overall profits.

One overlooked benefit would be related to supply chain risk. If it became viable to maintain the supply chain closer to home, U.S.-based companies would be able to reduce and even eliminate many risks associated with the global nature of the supply chain.

This topic is controversial. Economic theories conflict and get mixed up with politics and political opinion, obscuring the truth about the economics of taxation policy. The idea of making one country's rates more favorable is not isolationist by any means. The current reliance of hundreds of U.S.-based companies on overseas manufacturing and production does not necessarily disappear just by reducing taxes. But the heavy hand of taxation has made the situation an unfair playing field, which is why many corporations have simply packed up and left for more competitive home bases.

Among the benefits of equalized tax rates would be improved economic conditions not only in the U.S. but also in many of those same countries currently participating on the supply side of the supply chain. With reducing global risk, all participants benefit. Punitive tax rates kill industry and raise prices to end users while increasing inflation. No one benefits when this happens. High corporate rates in the U.S. certainly have not done anything to counteract high deficit spending. The more revenues going in to the U.S. Treasury, the more Congress spends. How that that make sense?

Read this article on the website Click Here
Logistics, the monkey wrench in the supply chain machine

Posted by Michael C. Thomsett on June 15, 2011

If you know the kinds of things that can and do go wrong, why is supply chain risk management so complex, and why do risks keep popping up?

The answer is logistics. If the supply chain were a never-changing machine in which goods or services flowed in the same manner all of the time, it would be easy to manage. But logistics gets in the way. Supply chain is not static but an ever-changing, evolving, growing labyrinth of potential risks, with new and unplanned ones showing up, always at the worst place and time.

Supply chain management demands multitasking over planning, transportation, storage, security, and much more. And when something doesn't go right, it never reduces the effect but always increases it in the most negative way. Any supply chain, whether raw materials turned into product, or information moving through a complex of IT controls, is going to evolve into its own life cycle with issues and challenges no one can plan for 100%. However, while you cannot plan for specific risks, you can plan for the consequences of such risks if and when realized.

To plan for management of outcomes and mitigation of effects, remember:

1. You cannot control output of any process. However, quality of output in all processes is improved when ownership of risk extends throughout the entire length of the supply chain. The key to ensuring high quality output is to shun the philosophy that "it's not my job." To the extent that you can inspire subordinates to also adopt the more enlightened risk management approach, you improve output further.

2. Quality control should be more than buzzword. Programs such as Six Sigma can effectively control risk consequences, recognizing that such programs function on two levels. The first and obvious is the functional steps involved in a team...
approach to quality control. The second and equally important is the organizational culture which is vastly improved through Six Sigma practices.

3. Simple changes may often reduce and even eliminate the scope of losses. These may include steps like more frequent transportation of goods, but in smaller increments (a form of diversification), for example.

4. Improved processes not only reduce risk, but also improve profits. This is an effective argument in a budget committee meeting where risk management often is among the first programs to be reduced or eliminated. If the case is made in a compelling manner, the answer -- handling the underlying issues -- is the only logical response. This beats waiting to see and hoping nothing happens.

Read this article on the website Click Here
It often is the case that diversification is ineffective. Why? Because risks are not truly reduced in some instances. A few rules worth remembering when you attempt to diversify:

1. Know your suppliers. Steps like supplier and manufacturer audits and ratings are likely to be effective, and are necessary if you rely on overseas suppliers for a majority of the products moving through your supply chain. But how often are you in touch? Are you in the loop of the supply decision-making process? Many SCRM problems originate with poor communication.

2. Who are your supplier's own suppliers? Are you really diversified using several different suppliers? You are not if all of them rely on the same manufacturers, storage, transportation, and other subsidiaries; or if they are all subject to the same location-specific events, such as weather-related risks. Effective diversification is best set up in different circles of partnership and different geographic locations.

3. Bring key suppliers into the core organization. If suppliers feel left out of the internal workings of the supply chain and yet they provide a large portion of the goods moving through it, the entire system is unequal. A supplier only becomes a true stakeholder when there is enough at stake to make it worthwhile. This includes participation, even some top-tier management drawn from key suppliers. Is this really such a revolutionary idea, or just a form of enlightened management?
Is your trade disruption insurance good enough?

Posted by Michael C. Thomsett on June 10, 2011

Among the different classes of BI insurance, trade disruption may be easily overlooked (or difficult to get approval for, given the fact that potential losses might never occur). However, if your organization is involved with the global supply chain, the complexities only add risk to your movement of goods or services. Trade disruption truly is a very large threat that may come about in many ways.

Covered risks in trade disruption should move beyond the obvious transportation risks. This coverage may also include losses on the part of your critical suppliers, disruptions caused by weather, labor strikes and even piracy. The complex coverage may cross over into typical marine insurance coverage. The key to need for this coverage is found in increasing reliance on direct suppliers, with the risks accompanying this reliance. The potential losses may arise from so many causes, including supplier use of their own secondary manufacturers. If your suppliers outsource any critical parts of what they provide to you, your exposure is increased exponentially.

This means that even if you believe you have adequate trade disruption insurance, your coverage may only extend to direct losses and not to more likely secondary losses involving your suppliers and their own outsourced providers. The lapses in coverage may be even more severe. For example, typical trade disruption policies exclude losses arising from terrorism. Although it will cost more to revise coverage to include disruptions arising from terrorist acts, it might be necessary.

The point is this: Trade disruption insurance, just like all other forms, might cover only a limited number of direct perils but not more likely and more serious secondary perils. You can mitigate this exposed flank by diversifying your supply chain, increasing the scope of coverage, or working with suppliers to supplement your coverage with insurance of their own.

Read this article on the website [Click Here]
Supply chains are rarely simple, but more often consist of complex interactions and movement of materials. In the modern world, information also moves through the supply chain, making it even more complicated to control. Anticipating points of weak links is a challenge.

There are ways to know not exactly where failures are going to occur, but where they are most likely. These points in the supply chain are easy to find. Some ideas:

1. **Visible weak links.** Look for points where material (or information) passes between people, organizations, or other "areas of responsibility." Any time goods change hands, that is by definition a weak link in the supply chain. This is the most likely point of failure. So risk management efforts that are concentrated on these changeover locations will be more effective than a more generalized monitoring program.

2. **Lack of enforcement.** Also look for points where internal controls are not being enforced. If the controls are designed to avoid or reduce risk, they need to be enforced. But as we all know, controls don't enforce themselves. They demand monitoring.

3. **Right to audit.** If you have provided internal controls to outsourced manufacturers or suppliers, how do you know they are enforcing them? Part of your contract may include the right to audit and this should be followed through and practiced as well.

4. **Second-tier enforcement.** Do your suppliers subcontract to other suppliers or manufacturers? If they do, how do you know whether their controls are working? What about their weak links? To an extent, you have transferred responsibility for risk management to your supplier. But this does not mean they enforce it with their secondary sources.
5. **Quality control programs.** Create internal programs at all levels, including suppliers, to continually monitor and enforce controls. Base it on a well structured quality control program such as lean Six Sigma.

Read this article on the website [Click Here](#)
Insurance

Insurance in perspective – part of a bigger risk management program

Posted by Michael C. Thomsett on June 3, 2011

Insurance is an essential part of risk management, but it is not the entire picture. It is part of it. Many specific problems arise concerning coverage and this becomes a source of potentially large and unexpected losses.

The problems are well known:

1. Many losses that are not covered or that are uninsurable, may be assumed to be covered.

2. The level of coverage is not adequate for the entire loss that might occur.

3. Some insurable losses are under-insured or not among covered perils.

When current insurance coverage is audited critically, not only for comparison between cost and benefit, but also from the point of view of the supply chain and its risks, these common flaws may become more obvious; and that is the first step in correcting the problem. The hard sell after this is convincing the executive branch and those who control the budget that more insurance is essential -- especially if the budget committee's goal is to reduce insurance and not to increase it. Many executives (including risk managers) live with a false sense of security based on several perceptions. These include:

1. We do not need more insurance because we have not had a loss. We can get by with less.

2. A positive experience rating has reduced our insurance cost; we should enjoy the reduction and not step up coverage.
3. We can self-insure because the most likely losses are not going to be catastrophic. (Realistically, a catastrophe by definition cannot be anticipated but always comes as a surprise.)

4. As long as our premiums are equal to or outpaced by our claims, our insurance coverage is "profitable" and does not need to be increased.

The risk management task is formidable. For many decision-makers, insurance is a simple matter. You pay a premium for a level of coverage and that's what you get. They often are unaware of the effects of exclusions, limits, deductibles and co-pay clauses. This, of course, all exists even before awareness of the risks that are under-insured or excluded.

Read this article on the website [Click Here](#)
Financing risk: points for evaluation insurance (or, have you read your company's policy?)

Among the methods for dealing with risk, financing is the best-known but perhaps the least understood. The approach to financing risk (i.e., buying insurance) is not the last word in risk management. Many executives are not aware of the many considerations involved with picking the best insurance, or in determining which risks to cover or to self-insure.

The considerations begin with deciding what not to cover. You cannot insure against every possible loss. So those least likely and least costly risks are best carried as risk realities. Insurance should be used for the most likely and highest-costs catastrophic risks. But once you decide what to insure, how about these additional three considerations in your analysis:

1. **Exclusions.** All insurance includes a list of what is not covered. It is not safe to assume that everything is covered because it never is. Study the list of exclusions to make sure you're getting the insurance you need.

2. **Cost.** Simply needing insurance is not the end point, it is the beginning. A careful quantification of the coverage you have versus its cost determines what you need and what you can afford.

3. **Deductibles and co-pays.** The devil is in the details, and this is true in insurance policies more than anywhere else. Every form of casualty coverage includes a deductible and a co-pay. When you consider these weighed against the cost, you are better able to identify what you need and what you can afford.

Beyond this, the world of insurance analysis is very complex. For example, does your "standard" casualty insurance policy include a provision for experience rating? Incentives like this are very attractive for organizations taking a proactive loss reduction
Financing risk: points for evaluation insurance
(or, have you read your company's policy?)

position with risk. Policies cost less when they are designed to encourage safe practices.

It all comes down to the reality that you get what you pay for. But many organizations and executives don't have the coverage they think, because they have not gone to the trouble to reading the terms.

Read this article on the website Click Here
Seen on the Tube: How do Insurance Firms Justify Prices?

Posted by Rebecca Beard on March 7, 2012

How much have recent events affected our perception of risks? How much are insurance firms really using this to their advantage?

Like so many people, I was riding on the tube this morning when a passing advert shocked me so much that I had to take a picture. People looked at me, a little bewildered and like my actions were odd. I am a risk manager and an econometrician. I like numbers and probabilities. These prices made little sense to me: this is because they are nonsense.

According to this advert (also confirmed on the provider’s website), the price of insuring your next three day ski trip costs the same amount as covering the risk of being stranded by an ash cloud on the days you travel. Really? Is the risk of an ash cloud stopping air traffic on the two single days you travel the same as suffering any sort of accident or injury during a ski trip?

A quick research on the probabilities of events show that “for every 1000 people spending a day on the slopes, only 2 on average will sustain an
injury that requires ski patrol and/or medical attention” (Source: medical interventions statistics, ski-injury.com). This means that your risk of being injured during a three day skip trip is 0.60% (exactly: 99.8% to the power 3, not 0.2% x 3, but the difference here is so small it is lost in roundings).

According to the study Dr Graeme Swindles, from the University of Leeds School of Geography the chances of an ash cloud forming are incredibly slim: “Although in the past 1000 years, volcanic ash clouds reached northern Europe with average return interval of 56 years (plus or minus 9 years), this interval varied and can be shorter or longer. A minimum of 6 years and maximum of 115 years between events was recorded for the last 1,000 years.” (Source: “A 7000 yr perspective on volcanic ash clouds affecting northern Europe” by Graeme T. Swindles, Ian T. Lawson, Ivan P. Savov, Charles B. Connor and Gill Plunkett). This publication suggests that the risk of being stranded by an ash cloud on either of the two days you travel varies between 0.0048% minimum (for clouds every 115 years) and 0.09% maximum (for clouds every six years). On average, the risk is 0.01%, 60 times less than a ski injury over three days!

Human minds have a tendency to overestimate the future risk of recent events, even if these events are incredibly rare. Studies have shown, for instance, that after terrorist attacks people are ready to pay higher insurance premiums to cover for the risk of damages caused by terrorism rather than of damages for any cause (including terrorism). In cognitive science, it is called recency bias.

Basically, it appears that this insurer is using the impact of recent events to push overpriced insurance covers. When considering risks, do not trust your sole judgement, do not trust your perception on a situation and do not be influenced by events highlighted by the media. Instead, back test them with proven data, research and compare the real chances and quantify the probability of such an event occurring.

Ariane Chapelle, Director of Consulting, Manigent.
The Election Is Finally Over! It's time for Brokers and Employers to grasp and plan for the "Disruptive Change" with Innovative Plan Strategies and Designs!

The wasteful and negative election period is now over! PPACA/Obamacare is here to stay! Those Brokers and Employers who took a "Wait and See" position on making Insurance and Benefits decisions will now be forced into becoming Decision-Makers. Many factors will have an impact on these decisions! These include:

- Changes in the existing PPACA/Obamacare Reform will be Ongoing.
- Regulations and Guidelines on Federal and State Levels will Abound.
- State Regulations and Exchanges will Differ Substantially.
- How Essential Health Benefits (EHBs) are defined.
- A Tremendous Volume of Information must be Reviewed and Acted Upon.
- Awareness of Timelines and Penalties will Demand Tracking.
- Brokers and Employers will Suffer from Confusion Based on Conflicting Information.
- A Plethora of Self-Proclaimed "Experts" will come forward to guide Brokers and Employers Down Unfamiliar Paths - Listeners Beware!
- A New Set of Economic Measures must be Utilized by Brokers and Employers.
- Brokers' Commissions may be further Diminished.
- Brokers' Administrative demands by Carriers and Employers will Increase.
The remainder of this Blog will be dedicated to four specific areas of focus to provide Direction for Brokers and Employers:

4. What Brokers and Employers should be watching for in the coming months - 2013 and Beyond!

5. Insurance and Benefit Plan Strategies that Brokers and Employers should consider before Years End, in 2013, and in the Future.

6. Brokers will be forced to Create Affiliations and Partnerships for Delivering Plans, Programs, and Services to Employers, Employees, and Individuals.

7. Things to remember for 2013 and Beyond – For Evaluating Insurance and Benefit Plan Designs and Strategies! For Implementing Plans Programs, and Services! For Remaining in Compliance!

What Brokers and Employers should be watching for in the coming months - 2013 and Beyond!

- Self-proclaimed "Experts" with Advice, White Papers, Webinars, etc. - Free and at a Cost - with schemes for circumventing PPACA or with promises of outcomes to good to be true.

- New Guidelines and Regulations as they are rolled out by the Administration, the Treasury, Congress, and Agencies in regard to PPACA.

- Timelines for Employers, Employees, and Individuals to be in compliance with various sections of PPACA.

- Federally mandated "Base" Health Plan Coverages" - Bronze, Silver, Gold, and Platinum - under PPACA.

- State Regulations and the Structure of their Exchanges.

- Guidelines for Private Exchanges.

- Employer Group and Individual qualifications under PPACA.

- Penalties imposed on Employers, Employees, and Individuals who are not in compliance with PPACA?
The Role of "Navigators" in Educating and Enrolling qualified Employees and Individuals.

How "Navigators" will be compensated?

Medical Loss Ratios (MLR) and their impact on Commissions?

Changes in existing regulations, ie. Self-Funding, Section 125, Reimbursement Plans, Reporting, etc.

Changes in the Plans and Premiums offered by Carriers.

Insurance and Benefit Plan Strategies that Brokers and Employers should consider before Years End, in 2013, and in the Future.

The Focus should be on Containing Costs while remaining in Compliance.

The Goal should be Meeting the Needs of Employers and Employees.

The Designs will need to be adjusted as Federal and State Regulations Roll-Out.

Plan Strategies should act as the foundation for building a Sound Strategic Benefit Plan and consider including:

A) Create - or Participate in - a Private Exchange as permitted under PPACA. The Private Exchanges will become available by numerous entities in various forms. We suggest that the Private Exchange options include - but not require participation of the Brokers, Employers, and Employees:

- Accommodations for Federally and State mandated plans.
- Core Health Plan Choices - offering levels of Premiums, Co-Pays and Deductibles.
- HRA and HSA Options - to assist Employees and their Families in becoming better Consumers and potentially set aside Funds for the Future.
- High Deductible Health Plan Options - compatible with HRAs and HSAs.
INSURANCE

- Self-Funded Health Plan Options - to provide Employers and Employees Greater Flexibility of Choices and Potential Savings.

- Implementation of Section 125 of the IRSC - to reduce Taxation for Employees and Employers while making Qualified Plans more Affordable.

- Availability of Reimbursement Plans - including: Medical, Dependent Care, and Transportation/Parking.

- Voluntary Benefit Choices - to Meet the Needs and Price Points of Employees and their Families.

- Ancillary Benefit Plans - to Offset the Costs of Employees and their Families for Day-to-Day Lifestyle Events and Needs.

- Wellness Plans - to Encourage Healthier Lifestyles and Reduce the Costs of Health Care.

B) Utilize a Defined Contribution (DC) Employee Benefit Design Strategy. The DC strategy is essentially a Cafeteria Plan and Full Flex Plan on Steroids. DC Plans provide better Control to the Employer and more Choices for Employees and their Families. DC Plan designs should include the following:

- All of the above under (A.)

- The CFO and/or Financial Advisor(s) - for the Employer determine a fixed budget to be allocated to Employee Benefits - year-by-year. In addition, they allocate Benefit Dollar/Credits to Employees by Classifications - Without Discrimination.

- The Managers and/or HR Department - working with the Broker(s) - select a Menu of Benefit Choices to offer Employees and their Families.

- The Managers and/or HR Department - working with the Broker(s) - determine the methods, for and the providers of, Employee Benefit Education, Communication, Enrollment, and Data Management.
The CFO, Managers, and/or HR Department - working with the Broker(s) - determine the Technology required for Implementation and Tracking of the above. In recent years the capacities of Technology have become more Efficient and Cost-Effective.

C) **Begin a systemic shift to a Fee Based Compensation Model for Insurance and Benefit Broker/Advisors.** This would replace the traditional Commission Based Models. Brokers/Advisors would clearly represent the Employers, Employees, and Individuals:

- Brokers would have no perceived or real Conflict of Interest.
- Carriers would be enabled to more easily comply with MLR.
- Consumers - Employer, Employees, and Individuals - would gain greater representation in negotiating with Carriers and other Suppliers of Plans, Programs and Services.

**Broker Affiliations and Partnerships will become more important in Delivering Programs and Services to Employers, Employees, and Individuals. These Affiliations and Partnerships will include (some may be integrated):**

- TPAs - for Self-Funded Plans.
- TPAs - for Reimbursement Plans.
- TPAs - for Retirement Plans.
- CPAs - to assist with Tax Planning.
- Law Firms - to assist with Compliance Issues.
- Traditional Core Benefit Brokers working with Voluntary Benefit Brokers - to grasp the full spectrum of Benefits Choices.
- Defined Contribution Plan Design Specialists - to assist in Strategically Designing and Implementing the Strategy.
- Retirement Plan Specialists - for helping to integrate all Voluntary Employee Benefit Plans.
- Enrollment Company Specialists - for providing the Education, Communication and Enrollment to meet the Employer, Employee,
and Brokers' Needs and Financial Capacities. Types of Enrollment may include: Group Meetings, One-On-One, Call Centers, Kiosks, Internet Based, Paper Based, or an Integration of these Methods.

- Technology Companies providing Software or Cloud Based Services - to simplify and integrate all of the above Regulations; Strategies; Affiliations and Partnerships; Plans, Programs and, Services; and more.

**Things to remember for 2013 and Beyond – For Evaluating Insurance and Benefit Plan Designs and Strategies! For Implementing Plans Programs, and Services! For Remaining in Compliance!**

- There are no Experts on PPACA. There are people who have and are closely Monitoring the Changes, New Regulations, and New Guidelines.

- There are no Silver Bullets for avoiding the reach of PPACA... There are Strategies for expanding Employers' and Employees' Options and for Retaining some Control.

- It will take several years for the PPACA Regulations and Guidelines to Roll-Out - Keep Up-to-Date!

- Tax Laws, as the Federal and State Governments concern themselves with Revenues and Deficits - will become more burdensome - Keep Up-to-Date!

- Tax Reform will be proposed and possibly implemented - Keep Up-to-Date!

- All levels of the Insurance and Benefit Decision-Making Process -- Brokers,/Agents; Service Providers; Employers; Employees and their Families; and Individuals -- will have a high degree of confusion, skepticism, doubt, fear, etc.

- Because of the above, the Education, Communication, and Enrollment Process will become More Important and may Take More Time.

**As the above outlines, the time has come for Brokers and Employers to begin the process of Disruptive and Innovative Change brought on by the skyrocketing Costs of Health Care and Health Insurance.** These factors have been combined with
Health Care Reform and Changes in the traditional Employer based Benefits Delivery Systems. There will be no return to the Good Old Days!

Survival for Brokers in 2013 and Beyond will be based on their willingness to abandon Old Strategies and Models while accepting Change. It will be essential for Brokers to embrace and even spearhead New Strategies and Business Models to Survive. Brokers must become creatively involved in building new Plans, Programs and Services - as well as Delivery Systems to accommodate the above changes. 2013 will deliver Brokers and Employers many Challenges and Opportunities!

We invite you to Comment and add to this Discussion: Join our Linkedin Group, Insurance Forum; Visit our Website - Benefitplace.biz or Email - max@benefitplace.biz

Read this article on the website Click Here
The death of an industry? - four insurance and benefits industry problems and solutions!

Posted by Philip Eide on March 18, 2012

BenefitPlace.com (BP) and BPTradeShow.com (BPTS) are constantly monitoring social media, especially Linkedin, for trends in the Insurance and Benefits Industries. Among the Groups we monitor, the "Players" include

- Insurance Company Decision-Makers
- Wholesalers, MGAs, GAs, PAs, etc
- Brokers and Agents
- Service Providers, ie. Consultants, TPAs, Enrollment Cos., etc.

Four problems seem to be shared among these Industry "Players":

1. Reducing Cost of Marketing and Selling!
2. Expanding the Distribution Channels!
3. Shortening Selling Cycles!
4. Increasing Sales and Revenues (ROI)!

As we monitor the discussions about these problems, we note some common threads:

- The problem is Always Someone Else's Fault!
- It was Always Better in the Past!!
- A Focus on the Problem Rather Than Finding Solutions!
- An Unwillingness to Take Risks That Might Provide Solutions!
- An Unwillingness to Embrace Change!
- Anything New Can't Work!

We're going to go out on the "Proverbial Limb" with some Solutions to the above Problems fully realizing that the above "Common Threads" will negate anything we may propose:

1. Reducing Cost of Marketing and Selling - A dedicated shift to "Inbound" marketing from traditional "Outbound" models
could substantially reduce costs while producing measurable results! According to a recent HubSpot study the savings could be as much as 61%. - Inbound Leads Cost 61% Less Than Outbound [New Data].

2. Expanding the Distribution Channels! - With traditional commissions and renewals shrinking or disappearing, all parties must look at new forms of "Distribution Channels". One of these that has been extremely effective for other Industries is "Affiliate"Marketing"! **What is "Affiliate Marketing"?** According to **Blue Global Media:**

"Affiliate marketing is an advertising model that works especially well online. It allows advertisers, also known as merchants, to sell their products and services through affiliates, or publishers. Basically, affiliate marketing gives a business a virtual sales force of online salesman, while giving affiliates a way to make money online without producing their own products or services. In return for promoting an advertiser’s products, affiliates receive a commission based on sales."

BP and BPTS would suggest that all of the above "Players" could substantially expand their distribution channels and marketing capacities - while reducing their costs - by implementing an Affiliate Marketing Strategy! This could be part of, and not exclusive from, the "Inbound" Marketing Strategy!

3. **Shortening Selling Cycles** - Utilizing "Inbound" Strategies combined with "Affiliate" Marketing, the "Players" should monitor, collect, and distribute the "Qualified Prospects" to the "Producing Field Force" in the straightest line possible. **Eliminate the dependence on "Field Management"!** Top heavy Field Management is generally expensive, slow to move, ineffective, and often favors personal relationships over Producer Statistics!

4. **Increasing Sales and Revenues (ROI)** - These "Bottom-Line" items can be achieved with the implementation of the above "Strategies"! We are not suggesting throwing out the old and
bringing in the new. We are suggesting that the above can be implemented at a limited cost of time and money. Those parties who are heavily "invested" in perpetuating the old models and strategies are generally going to be least informed, generally negative, slow to make changes. They will react with the tenancies - Threads - outlined above:

- The problem is Always Someone Else's Fault!
- It was Always Better in the Past!!
- A Focus on the Problems Rather Than Finding Solutions!
- An Unwillingness to Take Risks That Might Provide Solutions!
- An Unwillingness to Embrace Change!
- Anything New Can't Work!

Let's put aside the "Doom and Gloom" that is pervasive in many Social Media discussions and the general media! There have always have been "Problems". Throughout the years, Industry survivors have been those who: focus on "Solutions", take measured "Risks", embrace "Change" and move "Quickly"

As I was coming to press with this BLOG, I received Wendall Potter's article on Huff Post titled, "Coming Soon: The End of Health Insurers As We Know Them -- By Self-Inflicted Wounds"! Mr. Potter points out, "The system doesn't work. It's broke today" He added: "The end of insurance companies, the way we've run the business in the past, is here." The article goes on, "...the Affordable Care Act -- which essentially will ban medical underwriting after 2014 as well as several anti-consumer practices -- has accelerated the time frame in which the industry's current business model bites the dust. But reform was only an accelerant." Huffington Post March 18,2012

At BP and BPTS we are integrally involved in instituting "Inbound" Marketing Strategies and "Affiliate" Marketing for ourselves, those who list on BenefitPlace.biz, and Exhibitors on BPTradeShow.com. For more information: Email - max@benefitplace.biz or Call - 216.577.5579

Read this article on the website Click Here
Investment Risk

Risks in accounting rules for less-informed investors

Posted by Michael C. Thomsett on August 26, 2011

In the on-going debate concerning the impact of GAAP transition over to IFRS accounting, much of the debate revolves around cost of compliance, adjustments in reported profits, and treatment of certain items (i.e., deferred taxes, goodwill and even capital asset valuation).

All of these issues are of great concern and importance, and the current SEC-imposed deadline of fiscal 2015 for full coordination might not be realistic given the enormity of the changes involved. However, within this debate, one issue has not been mentioned often. How does the transition affect risks for less-informed investors?

We may expect that an experienced analyst is going to be able to spot trend bumps and to recognize that these are caused by the newly integrated accounting methodology. However, less informed investors may face a new risk, that of misreading the trends. For anyone advising investors, and for those with limited interpretation experience, this is a noteworthy risk. One study of this potential problem, termed it "information asymmetry," which could be an issue for several years of transition between the two systems, especially if past results are not restated to ensure continuing accuracy in fundamental trends.

Read this article on the website Click Here

---

The risk of accounting manipulation

For years I have been concerned with the question: Can fundamental investors make value judgments based on financial statements?" Give the many different kinds of accounting "interpretations," how do you know that you're getting an accurate picture of operations?

Perhaps the most damaging form of manipulation is one described as "less" offensive. In other words, short of outright fraud, this year's transactions are simply arranged to smooth out what gets reported. Is this serious? Yes. Any kind of decision to manipulate earnings is deceptive and may lead to more serious forms of deception.

At first I considered that there were dozens of ways to manipulate, to cook the cooks. And then I found a book published in 2002 that articulated the problem into five broad categories. These are:

1. **Aggressive accounting** (choosing to rationalize the treatment of transactions in the most favorable manner, in some instances even beyond what GAAP recommends)

2. **Earnings management** (manipulating or timing revenues to meet predetermined earnings targets or analysts’ forecasts)

3. **Income smoothing** (adjusting reported earnings to create year-to-year consistency and growth trends even when actual results are more chaotic)

4. **Fraud** (misstatements or omissions with the purpose of deceiving investors and regulators)

5. **Creative accounting** (any decisions undertaken to improve desired outcomes in financial reports, including interpretation of the rules under GAAP to maximize profitability and working capital) (Mulford and Cominsky, 2002)
The risk of accounting manipulation

This came from the book (Mulford, Charles W. and Cominsky, Eugene E., “The Financial Numbers Game” (New York: John Wiley & Sons), 2002). It was very useful to be able to classify the various methods into five groups, and to then consider ways that accounting departments and auditors can contend with them.

As a risk issue, the danger is that once the deception door has been opened, it is very difficult to step back out. Cooking the books is tempting, of course, but it is like any other slippery slope. Once it starts, it is difficult to control.

Read this article on the website Click Here
How will the GAAP and IFRS merger affect trend analysis

All good ideas have risks. The creation of a uniform international accounting standard is going to be a positive matter, given the emergence of so many multi-national companies and the importance to investors to knowing the basis of financial statements. Even with the flaws in accounting interpretation, when everyone is basing their audited work on the same assumptions, it will be a good change.

However, before that can happen there will be the Big Transition. Are you ready for it?

The problems of training IT personnel, testing and implementation are mind-boggling. The new approach and issues for tax, internal audit and legal personnel is equally difficult. But perhaps the greatest challenge is going to be for fundamental analysts. Are past years’ results going to be restated on the newly uniform basis from 2015 onward? Or will we simply accept that the assumptions changed and have to be factored in?

It would not be a big deal, except that profitability calculates out differently under IFRS than under GAAP. Reported profits under IFRS are 6% to 8% higher than under GAAP (McLaughlin, K., “IFRS-GAAP convergence likely to mean major changes in U.S. accounting,” The RMA Journal, 91(5), 2009). This is a big difference, with profits as well as other ratios affected between one year and the next.

The changes are massive, and all publicly traded companies currently using GAAP in the U.S. and Canada are required to switch to the new IFRS standard by fiscal 2015. If organizations have not yet started working on the training phases of the switch, it could be a problem. Maybe the bigger problem is that the specifics are still being worked out, so no one really knows what we are switching to ...
The big topic in accounting circles these days is the upcoming mandatory conversion of GAAP to the international financial reporting standards (IFRS) used in Europe. Whereas GAAP is a rules-based system, the IFRS alternative is called principles-based. Even though this move seems to be counter to the changes instituted in the U.S. after the Enron era via Sarbanes-Oxley (SOX), many see this uniformity of global accounting as a positive move.

This may be true. With so many companies now operating globally, having a single set of assumptions for how transactions are treated, revenues and earnings booked, intangibles valued, and deferred tax liabilities recognized, makes sense. Having one universal system of accounting is logical and advantageous.

Even so, the transition will be painful. This is especially true because many organizations are not prepared to go through the testing, training, and data management changes that are going to be involved. The new accounting system is to be implemented by 2015 but in terms of conversions, this is right around the corner. Massive training and procedural changes are going to have to occur in internal auditing, tax, and accounting departments. The biggest changes, however, will be in IT. A period is going to be required for revisions to data handling and storage, so if an organization has not yet started, they need to scramble to avoid chaos in a couple of years.

The IT transition is not going to be a matter of simply changing how or when data are moved through the system. In order to get technical folks to make changes properly, they will need a period of training just to understand the issues. After this, a testing period is going to be required to ensure that new procedures are (a) error-free, (b) reconcilable to older methods, and (c) in conformity with the new rules.

These are massive changes. CFOs and risk officers need to begin now to set a fast track for the training phase of IT employees, as a
first step in meeting the SEC-imposed requirement for these new procedures.

Read this article on the website Click Here
Every portfolio manager deals with the ever-present threat of market risk. This, more than anything else, is the concern faced by anyone with capital in the market. It does not matter how much research you perform, how many models you use, or how far you back date your analysis. It still comes down to one problem: the value of your investments might decline.

This problem is so severe, especially given recent market weakness and price volatility, that some portfolio managers and individual investors are simply not buying stocks directly any more. They are keeping their money in low-yielding Treasury securities (whose yield may be lower than inflation, meaning the purchasing power of invested funds is declining) or relying on mutual fund managers (and remember, most mutual funds perform under market averages). Some resort to ETFs as an alternative to tradition funds, an easy way to diversify while maintaining liquidity, but an exchange of risk for often mundane returns. So what can you do?

A suggestion: Invest in high dividend-yielding stocks with an excellent track record of growing revenues and profits. Focus on strong, well-capitalized blue chips. Invest only in companies with low or declining debt ratio and a P/E ratio between 10 and 25. Finally, protect your portfolio with no-cost or low-cost option strategies. There are two of these that eliminate all market risk while keeping dividend yield in place. These are:

1. The protective collar. This is a strategy combining stock and option positions. For every 100 shares of stock held long, you sell one covered call and buy one long put. The cost of the put is paid for my the premium on the covered call. The ideal strike is slightly higher than your basis in the stock. If the stock price declines, the long put can be exercised to recapture the paper loss, or the put can be sold at a profit. If the stock price rises, your short call will be exercised and your stock is
called away at a profit. In either case, you earn a profit and never suffer a loss, but you continue earning dividends as long as you own the stock.

2. **Synthetic short stock.** This is very similar to the collar. You open a short call and a long put, so that the position performs best when stock price declines. However, if stock price rises, the short call is exercised. So the conservative version of this strategy is to make the short position a covered call. Here again, you earn dividends while you own the stock, and the no-cost offsetting option positions eliminate market risk.

Both strategies contain lost opportunity risk. If the stock price rises quickly, your long stock is called away and you miss out on profits you could have earned. If you are not willing to face this possibility, then the collar or synthetic positions are not for you. But if you want to protect your capital and exchange market risk for the chance of getting exercised (at a profit), these are sensible and conservative ideas. If you end up with a portfolio of modest stock gains and consistent dividend income, you are going to be far ahead of the average.

Read this article on the website [Click Here](#)
Any system for valuing a company or its profits should be sensible, conservative and based on hard data. In the past, many tricks such as reliance on pro forma statements, "forward looking" estimates, and EBITDA, exaggerated the value of companies, often as part of an estimate for pricing a company upon sale.

Rather than using liquidation value or negotiating a goodwill value to company stock, some argue that cash flow is more accurate than actually reported profits. For investors, this is a risky affair. EBITDA (earnings before interest, taxes, depreciation and amortization) is odd because it calculates "profit" as if some realities simply did not exist. For example, interest on current long-term debt is excluded, as is the expense for tax liabilities and more.

If EBITDA is used solely as a means for comparison between organizations, it may be a useful calculation as part of a value analysis. However, beyond that it has little value. The calculation was born in the 1980s when leveraged buy-out was common and when new investors were interested in a stream of cash and were not at all interested in long-term growth or value. Today, the calculation may be used simply to make earnings appear stronger than they are. This was the conclusion of one study questioning the motives behind calculating EBITDA (Jennings, M. M., "Ethics and non-gaap financial reporting," Internal Auditing, 18(6), 2003).

A variation to this, known as EBIT (excluding adjustments for depreciation and amortization) also may be used to exaggerate earnings and potential future earnings. The worst of all worlds is found when EBITDA or EBIT are applied as part of a pro forma analysis -- estimating future profits.

For purposes of side-by-side comparisons or analysis between organizations, GAAP and IFRS are imperfect, but they are at least consistent and far preferable over the possible exaggerations found in other methods.
Are you really conservative? -- 5 reasons you might not be

Many traders define themselves as conservative. But is this accurate? or does your trading style contradict the standards of "conservative" trading? Here are 5 ways to test how conservative you are in your trading and investing.

1. How do you investigate a company before you invest? Do you look at the long-term fundamental trend for key indicators, check annual statements and read current news about the company? Or do you actually invest on tips or advice without asking questions? Do you develop low-risk strategies for your portfolio?

2. Do you know the business the company is in? This might seems obvious but it is not. Many self-defined conservative investors or traders know the names but really don't know what product or service the company sells. To be truly conservative, you should have a sense of the sector the company is in, and how strong that sector is today. Stay up with the current financial news; personally, I like newsfeed as a source.

3. Where does this company stand compared to its competitors? Is the company the leader or a strong second? Or does it lag behind in terms of market share and profits? You want to find companies that compete successfully with other, similar companies. If you don't know, you are not investing in a conservative manner.

4. Has the company made a profit in recent years, and is the profit increasing each year? Why would you invest in a company whose revenues and earnings are leveled out or falling? or if the company is even losing money? A conservative principle includes a requirement of financial success.
5. **What is the health of key indicators?** Have you checked dividend yield, P/E range, or debt ratio? Is the dividend rising each year? Is the P/E consistently in a mid-range (often defined as between 10 and 25, for example)? Is the debt ratio level or falling, or is it growing each year? These are essential financial signals and true conservative strategies rely on them to choose companies as potential investments.

These five steps are necessary in order to qualify you as a true conservative investor. In fact, even conservatives should never settle for below-average returns on their investments. A very appealing definition of *conservative* is: *strategies or a series of strategies designed to reduce risk while increasing income.*

That is a goal worth setting and then putting into action.

Read this article on the website [Click Here](#)
What can be done to seal the cracks in the lending landscape?

Posted by Ian Rawlinson on March 28, 2012

It is a time of clichés for banks as they currently find themselves caught in a Catch-22, stuck between a rock and a hard place. In the UK, government initiatives such as ‘Project Merlin’ have been put in place to encourage banks to lend more freely. At the same time, new regulations or initiatives such as Basel III, Recovery and Resolution plans and leverage limits are coming to the fore, increasing the capital adequacy and liquidity requirements for banks around the world. So how do banks walk the fine line between lending requirements, managing risk and capital adequacy?

Financial institutions are being asked to lend more therefore exposing themselves to additional risk and at the same time hold more capital which can reduce returns on equity. One consequence will be the need to make returns on lending by the way of fees and charges, as banks look at other ways in which they can optimise capital. A recent Capco/Swiss Finance Institute survey of the private banking industry found that 52% of firms plan to adjust their pricing strategies to share increased overheads with their clients.

But before costs are increased, there needs to be a reassessment of their current risk frameworks. If banks focus on qualitative frameworks as well as their current quantitative models, they will be in a better position to determine whether the composition of their portfolio is adequate. Senior management also needs to understand the scope of their models and think of other ways in which they can plan and test for risks.

The bottom line is that many regulations have yet to be implemented and therefore tested. Only time will tell whether these reforms will further complicate matters for banks. Clever financial institutions will be those that develop more
comprehensive risk adjusted return-on-capital capabilities, to proactively manage current and future complexities in the lending market. Or to avoid closing the door before the horse has bolted, so to speak.

Read this article on the website Click Here
Since the financial crisis, the banking climate has changed considerably. What used to be an abundant landscape where most, if not all banking providers coexisted profitably, is gone.

Today, banks have been forced to operate in a drastically more competitive environment. Increased access to information, advances in technology and greater choice has given the consumer more freedom to ‘shop around’, placing them clearly in the driving seat.

The longstanding relationships banks once enjoyed with their customers are now under threat from greater, more diverse competition, as retailers with advanced customer profiling capabilities and new market entrants swoop in for market share. The result? Customer loyalty has virtually become obsolete.

Looking from the outside in, banks are also grappling with numerous internal challenges, as high profile failures have placed bank’s risk taking activities under heavy scrutiny. This has left bank boards, regulators and auditors calling for greater visibility, more transparency and better control over lending portfolios and associated risks. The dwindling returns of the banking industry leave little to no room for error. Banks have been left with no choice but to capitalize on market opportunities to safeguard future profitability. The commercial lending space is an area that offers significant opportunities, but are banks ready to win big here?

There are just three steps to success in the commercial lending market.

First, banks - gain true insight into the credit quality of their customers. The whole industry has been talking about customer centricity for years, but how many banks are walking to walk? There is no doubt about it, banks need to attract the best quality credits. That’s a must. It’s an imperative. Relationship Managers...
need to become the customers trusted advisor, increasing customer loyalty through timely, prompt, and convenient service, and they need to do that at a competitive price. Not only that, but if they do not execute each and every customer interaction flawlessly, customers will not only walk, but with social media at their fingertips and word of mouth at their lips, they will talk. Deeper knowledge of the customer is the cornerstone of strong, loyal and profitable customer relationships.

Banks also need to lower costs by implementing strategic initiatives to enhance operational efficiency. They can substantially reduce costs, improve long-term efficiency, and foster better customer responsiveness by incorporating higher degrees of automation, and most importantly, by streamlining processes throughout the commercial lending lifecycle.

Lastly, banks need to proactively manage their portfolio and ensure constant regulatory compliance. To do this they need to better integrate risk management into their strategic decision-making processes. This will give bank boards, senior management teams, along with the regulatory and audit communities, visibility, transparency, and control over the portfolio, and most important, a view into the associated risks.

So, to climb the ladder to success in commercial lending, banks must think customer, cost and risk – all of which are much labored points in today’s market, but equally are game changing assets to the future survival and profitability of any bank today.

Read this article on the website Click Here
Icesave the Real Story. Gerard van Vliet deposited his savings in an Icesave account and lost it within 6 weeks! It made him a risk expert and an angry 'wasp' for all authorities

Posted by Boris Agranovich on November 28, 2010

Gerard van Vliet, leader of over 250 savers who had more than €100,000 in the Icelandic savings bank Icesave when it collapsed 2 years ago, and Dadi Rafnsson investigative journalist from Iceland are working on a book about the Icesave-bankruptcy. Gerard is a member of the GlobalRisk community and he is interested to see your reaction to this discussion.

Gerard van Vliet himself is one of the victims of the collapse of Landsbanki branch Icesave. The Amersfoorter deposited a considerable sum for a project in Africa, in an account with the savings bank, shortly before it collapsed.

The Dutch state and Dutch deposit protection scheme eventually compensated savers for the first €100,000, the rest they had to ‘save’ in Iceland as part of the bankruptcy of Landsbanki, the owner of Icesave.

Van Vliet is busy with this issue already one and a half year. Meanwhile he is battling with politicians and regulators in both Reykjavik and The Hague, as well as with the general public, which stamped him and his group as “rich bastards”.

The protracted battle supplied van Vliet with a wealth of information on which he collaborated with the Icelandic investigative journalist Dadi Rafnsson in a book which is about to be finished. The book comes out in both Icelandic and Dutch, and describes the failure of Landsbanki from different perspectives.

Van Vliet: "There is an enormous mass of information in Iceland, England and the Netherlands for the book intended. In some
cases, anonymous sources, who do not want to be named. Partly because they would be branded as 'victims' in their environment, partly because they themselves as "whistleblower" feel unprotected."

"To understand how and why it is so easy that Icesave tragedy could happen, we look first to the circumstances in Iceland preceding the time of the collapse of Icesave, October 6, 2008. We are introduced to "The Dirty Thirty", the thirty people who were responsible for an unprecedented upturn in Iceland, at least on paper, and finally almost bankrupted that country. What were their motives, where they stood, how they are linked. "

Next to that van Vliet and Rafnsson make a trip to the obvious lessons already available, lessons that nobody wanted to see. Based on the large number of bankruptcies in the 80ties in America, now known as Savings & Loan crisis. Dozens went bankrupt by the greed of bankers.

The roots, the beginning of Icesave was in England, which started in October 2006. Promising, rapidly expanding at the unprecedented level of 5 billion pounds of savings and winning prize after prize as an innovative Internet bank.

Share with us the surprise if you read that in 2007 there were already serious criticisms of Icesave and Iceland. Add to that withdrawal of one billion pounds of savings at Icesave in the period February-April 2008 (just before on May 29, 2008 Icesave in the Netherlands was launched) and the scathing criticism in the press on the operation of Landsbanki, "says van Vliet.

Van Vliet raises further questions as "Why did the DNB (Dutch Central Bank-Dutch regulator) not intervene? Could a bank run really have been avoided?"

Attention is also paid for the period after the collapse of Icesave. Where the relentless struggle of the Minister of Finance Bos, according to the authors manipulative, "it's € 1.3 billion to recover from Icesave is central. The money advanced to Iceland because it needed the money for their own Deposit Guarantee Scheme (DGS), the money for which an agreement is still missing."
Icesave the Real Story. Gerard van Vliet deposited his savings in an Icesave account and lost it within 6 weeks! It made him a risk expert and an angry ‘wasp’ for all authorities.

The association of more than 250 Icesave savers victims battles to be recognised as “ordinary, hardworking savers” and not as the 'rich bastards'.

You can find their stories in the book as well as the stories of some Icelanders. The Icesavers also battle for attention, recognition and support in the media, but especially in politics. They unable to get a foothold in Iceland where each judge has a ‘third’ cousin who was involved in the Icesave troubles.

Read this article on the website Click Here
Things To Not Say To A Risk Manager

Posted by Boris Agranovich on December 14, 2010

Have you been in a situation where either a colleague, a client, a regulator, a vendor, an auditor or someone you report to asked you a question or say something that was completely out of line? Let us know here. The most common and interesting questions and phrases will become a new blog article.

Read this article on the website Click Here
I've been a market maker in stock and index options about 17 years. Grew up in the derivative cowboy-land. I build up my own company, took on some fine traders and did well. In 2002 I decided to do something completely different and after a while I joined a recruitment company and became a 'executive search consultant' or 'head-hunter', if you like. Specialism: treasury. Not my choice, but (the treasury part) the company's choice I worked 4. Really interesting though. Options, hedging, funding,... in the end all the same: how to invest your money with minimum risk and get the best results. In my time, I had to do my share of risk management. Actually, it was all I was doing. Recently I've became a partner in a 'recruitment company' (we call it 'boutique') specialised in Risk. So here I am. Did Risk all my live as a market maker. No rules, just save your ass everyday...Rules are everything, nowadays. Basel, Solvency, the works. Interesting, but difficult. In the end it's all the same: getting down the source. I am learning every day and at the end of every day it's like going back in time. Any ways: It's fun to bringing knowledge to needs. Still have to learn a lot, especially about Risk-business slang. People make it harder then it is. Rules must be as clear as the communication about it (and visa versa)

Read this article on the website [Click Here]