All rights reserved by the authors
To view our privacy policy, click the link below:

Privacy Policy
Contents

Copyrights 2
Contents 3
Introduction 5
ERM: Doing it, and doing it right 6
SME Development Bank (SDB) 9
*The Hamilton Plan: SME Development Bank (SDB)
*The Hamilton Plan: Ten Points
*Capital Formation Key to Success
*Community Bankers as Risk Managers and Distribution Conduits
ERM Software vs. SharePoint 17
*Technology
*Support
*Costs
*The Advantages of Logic Manager
RIMS Risk Maturity Model: ERM Approach and Process Management 20
*ERM Based Approach
*RIMS Risk Maturity Model: ERM Process Management
*Why is this important?
Why Are So Many Companies Missing the Point? ERM’s Role in Risk Prevention 24
Upgrade Your Business Through GRC Solutions 27
*Ownership of the tool:
*Security Issues:
*Monitoring and Communication of Data:
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERM Software – Selecting the Best Solution</td>
<td>30</td>
</tr>
<tr>
<td>*Does your solution support the best practices outlined by an accepted ERM Framework?</td>
<td></td>
</tr>
<tr>
<td>*Is your solution flexible enough to fit the unique and evolving responsibilities of your ERM program?</td>
<td></td>
</tr>
<tr>
<td>*Does your ERM solution provide the support necessary to ensure success?</td>
<td></td>
</tr>
<tr>
<td>The Cost of Reputation Risk</td>
<td>33</td>
</tr>
<tr>
<td>Report: Colleges &amp; Universities Lack ERM, Guidance</td>
<td>37</td>
</tr>
<tr>
<td>ERM Report: The Automobile Industry &amp; Integrated Risk Management</td>
<td>39</td>
</tr>
<tr>
<td>NYT: How to Buy ERM Software in 2014</td>
<td>42</td>
</tr>
<tr>
<td>SEC Reprioritizes ERM in 2014</td>
<td>44</td>
</tr>
<tr>
<td>Improve Internal Audit Planning with ERM</td>
<td>46</td>
</tr>
<tr>
<td>Scoping by Objectives</td>
<td></td>
</tr>
<tr>
<td>Scoping by Business Process</td>
<td></td>
</tr>
<tr>
<td>Scoping Resources</td>
<td></td>
</tr>
<tr>
<td>Risk Libraries</td>
<td></td>
</tr>
<tr>
<td>Risk Taxonomy</td>
<td></td>
</tr>
<tr>
<td>Identifying, Assessing and Managing Risks From an Enterprise Risk Management (ERM) Perspective</td>
<td>50</td>
</tr>
<tr>
<td>Development of Operational Risk Management Solutions in UK</td>
<td>56</td>
</tr>
</tbody>
</table>
Introduction

The fourth book in the Global Risk Series is dedicated to one of the most popular discussions among seasoned risk professionals - GRC vs ERM.

Is ERM more a methodology for managing the entire spectrum of risk while GRC is more a technology platform for managing governance and risk compliance?

Can GRC live with ERM without one contradicting the other?

Why do so many philosophical and methodological differences exist that make this debate of almost theological importance for Risk professionals?

Special thanks go to members who contributed to this report: Steven Minsky, James McCallum, Sophia Wright and Peter Chisambara
JEFFERY REYNOLDS’ article in ABA Banking Journal, “ERM: Getting it, and getting it right”, equates the definition of Enterprise Risk Management with happiness.

"Before you start with ERM, you have to define it. If it were only that easy to nail down the definition of ERM—but it is not…Defining ERM is like defining happiness. Happiness is not the same for me as it is for you. Nor is it the same for me today as it was 20 years ago. And what drives happiness today will likely not be what defines happiness in a year or two."

Although Reynolds makes key points about the "interconnectivity" of ERM and its misinterpretation as a check-the-box activity, ERM is not like happiness. ERM is an action. You either do it, or you don’t.

Organizations do not need to do Enterprise Risk Management the same way, focus on the same goals, or follow the same best practices. But those best practices – a root cause approach, the iterative steps of identify, mitigating, and monitoring – do not require discovery. They are known, and they can be implemented at any organization of any industry or size.
Consider GAAP, a set of accounting standards that can be used in any given jurisdiction. GAAP includes rules, standards, and conventions that assist in the creation of financial statements and help accountants do their job well. GAAP is to accounting what ISO, COSO, and other such frameworks are to ERM. Your accounting department uses a general ledger software to turn these best practices from a good idea into practice. The general ledger is to accountants what ERM software is for risk managers. It makes their work real, their results actionable, and ensures they follow best practice.

Reynolds argues that the process of moving through a discovery phase and discussion of risk creates value because ERM becomes, like happiness, a mindset that can drive strategic decision making.

The problem with relying on the discovery process is that the very value that Reynolds’s recognizes in the process cannot be made actionable without tools that make the “interconnectivity or risk” transparent for risk managers and executives alike.

Have you ever been in a meeting with a fantastic exchange of ideas, but watched helplessly as those ideas floated off the second each stakeholder stepped out of the room?
ERM software is designed to capture those ideas by linking what your organization is doing, the controls, metrics, policies and so forth, directly to the risks and goals being identified. Without that link between good ideas and concrete activities, a mindset is just a mindset, and boards make decisions based on metrics, not mindsets.

The “interconnectivity or risk” that Reynolds correctly identifies as the value or ERM cannot effectively exist as a mindset, it requires a taxonomy. In trying to define happiness, Reynolds says that people “seek the counsel of experts and ‘gurus’… They attend seminars, buy books, and hear testimonials.” He’s right.

Those activities don’t create happiness, nor would they generate value for an ERM program. The value is made in executing the steps of an ERM process.

Utilizing the correct tools to connect those results to the strategic goals of your organization.

ERM Software is much more than dashboards and communication.
The Hamilton Plan: SME Development Bank (SDB)

Over the Labor Day Weekend Sum2 announced The Hamilton Plan.

The Hamilton Plan is a ten point program to foster the development of manufacturing in the United States by tapping the entrepreneurial energy of small and mid-size enterprises (SME). The plan's 10 points address sustainable business models, GRC best practices, capital formation initiatives, SME banking, labor union stakeholder empowerment, association syndication, cooperative formation, support for public education and cooperative learning.

This is an introduction to The Hamilton Plan, why it's needed and the call for the creation of an SME Development Bank (SDB) to facilitate capital formation to achieve the goals of the program.
The Hamilton Plan, named after the first Secretary of the Treasury of the United States, proposes a ten point program to develop small and mid-size enterprise (SME) manufactures. The Hamilton Plan invites business owners and executives, industry associations, chambers of commerce, banks, capital market participants, labor unions, academia, non-profit organizations and governmental institutions to join forces in a concerted effort to support the reestablishment of the manufacturing infrastructure of the United States.

The vital national interest can be served by institutions representing business, labor, local communities and government to join together to foster optimal conditions to incubate and develop SME manufactures. SMEs are a natural strength of the US economy. SME represent largest most vibrant sector of the economy and by combining the entrepreneurial drive and creative energy of SME's with the pressing need for innovative manufactures; America can reestablish its ascendancy as a preeminent power in the global economy. The Hamilton Plan is designed to provide incentives and encourage the formation of support clusters to develop SME manufacturing.
The Hamilton Plan: Ten Points

1. Adoption of World Business Council Standards for Sustainable Business
2. Establish Incubators for Targeted Growth Industries
3. Adopt Sound Governance, Risk, Compliance Practices (GRC)
4. Formation of SME Development Bank / Capital Formation Initiatives
5. Partnership Lyceums for Government / Business / Academic Institutions
6. Labor Unions as Preferred Stakeholder / Association Syndication Unions
7. Establish Cooperatives for Technology / Licensing / Commodities / Energy
8. Superfund for Progressive Tax Code / Universal Health &amp; Benefits / Infrastructure/ Brownfield Remediation and Reclamation
9. Expand Public Education Funding &amp; SME COOP Program
10. Support Millennium Development Goals

Capital Formation Key to Success

The Plan in its entirety is designed to respond to the compounding economic and political crisis that is confronting the United States. The credit crisis, energy dependence, industrial stasis, trade deficits, geo-political instabilities, aging infrastructure and climate change are the result of long term systemic problems that government and industry has failed to address effectively. The Hamilton Plan advocates the adoption of the program to squarely address these pressing issues with the full understanding that it will require the concerted cooperation of all stakeholders to assure the continued development, security and prosperity of America.
The Hamilton Plan requires concerted focus of investment capital to fund development and to make sure that assets are allocated to channels that will assure optimal returns and that equity participation of stakeholders is protected and rewarded. The establishment of an SME Development Bank (SDB) is a structured investment vehicle and corporate institution that will focus, manage and administer capital formation initiatives to incubate and develop SME manufactures.

At its core, The Hamilton Plan seeks to preserve the free flow of investment capital to finance national economic development and empower SME manufactures. The Hamilton Plan is not a substitution nor in any way seeks to supplant the American free market system.

The Plan is designed to unleash, pool and focus investment capital. The Plan leverages regulatory capital, compliance and governance. The Plan seeks to achieve strategic economic goals, build wealth and prosperity in US and realize broader goals and objectives to assure sustainable economic growth, ecological balance and global competitiveness.

**SME Development Bank (SDB)**
The SDB would be chartered to assure that capital is deployed to meet appropriate program projects and assure effective stewardship of shareholders capital. The SDB would be the repository for economic and regulatory capital. It would maintain capital adequacy ratios in conformance with Basel II directives. The SDB would serve as a fiduciary to distribute capital through local community banking channels. SDB governance would assure that program objectives, ownership equity, credit requirements, capital allocations, shareholder rights and income distributions are made to SDB shareholders.

Government funding of the SDB would consist of share purchases financed by capital from a national development Superfund. The Superfund would receive tax receipts from a progressive national tax program, budget allocations, licensing and royalty receipts, dividend reinvestment's and capital gains proceeds from the sale of assets.

Shareholders in the SDB would be community banks, institutional fund managers, state/local/federal government, private equity firms, business owners, company management, associations, labor unions, employees, academic institutions, non-profits organizations.
Different forms of capital would be recognized and used to purchase shares in the SDB. For example, local governments can purchase shares in the SDB with tax credits or land grants or infrastructure improvement projects; labor can purchase shares with sweat equity, academic institutions with intellectual capital etc.

Securitization of SDB shares can be created to trade on public exchanges. Any secondary market listings would occur after underlying assets have been properly seasoned. Shares in the SDB would offer terms of extended time frames for investment lockup and share redemption.

**Community Bankers as Risk Managers and Distribution Conduits**

Community Banks have a critical role as an SDB equity partner. The community bank is the primary channel by which equity and credit capital is provided to the SME. They are front line risk managers and advisors for portfolio companies. Community banks are astute relationship managers. Community banks understand local market conditions and can link assets and service providers to build support clusters and expanded value chains for SMEs.
Community Banks have a critical role as an SDB equity partner. The community bank is the primary channel by which equity and credit capital is provided to the SME. They are front line risk managers and advisors for portfolio companies. Community banks are astute relationship managers. Community banks understand local market conditions and can link assets and service providers to build support clusters and expanded value chains for SMEs. Community bankers will help SMEs focus on capital allocation strategies and support efforts in encourage growth and profitability. They will provide help in the following areas:

- Corporate Governance
- Risk Management
- Business Promotion, Acceleration and Development
- Corporate Advisory Services
- Information Services
- Performance Evaluation Services

Community banks must continue fulfill capital requirements for retail banking and other lines of business in accordance with regulatory requirements of its governing agency. State regulatory agencies relating to SME banking regulation, enforcement and inspection would conform to a unified national banking regulatory agency.
Community banks will share in the equity appreciation of the SME and any distributions, dividends or corporate actions the Board of the SDB effects. The differentiation of credit and equity capital participation will be accounted for at the SDB level. Administrators for hedge funds and other Alternative Investment Vehicles have developed sophisticated partnership and shareholding accounting capabilities that can address questions of share class ownership, tranche construction and attributes, asset valuation, distributions and returns.

The community bank in working in conjunction with the SDB will help SME's effectively manage risk, improve stakeholder communication, implement effective corporate governance that create sustainable business practices to assure long term profitability and growth.

The Hamilton Plan lays the foundation for SMEs to seize market opportunities. SMEs in partnership with community bankers must assess products and markets, business functions and critical success factors. Sufficiently capitalized by the SDB, the SME and local bankers will execute an action plan to support the corporate mission in line with the larger goals of The Hamilton Plan to build wealth for its shareholders and assure the future prosperity of America.

Risk: manufacturing, small and mid-size business, global competitiveness, middle class, national prosperity

Read this article on the website Click Here
ERM Software vs. SharePoint

Posted by Steven Minsky on August 4, 2014 at 11:02pm

Once SharePoint has taken root in a company, there’s a tendency to try to use it for everything. The mega-popular platform can accomplish many use cases, from social networking to document management.

It’s no wonder then that Risk Managers have been asked to build their programs on SharePoint - and live and die with the consequences. If your organization is considering SharePoint for ERM or other governance activity, or you’re considering moving your program off SharePoint all together, consider the following requirements and their effect on your ERM program’s growth.

Technology

SharePoint relies on a huge variety of technology. For the platform to run smoothly, everything has to be in sync or you’ll risk mishandling, or even deleting, critical data.
Consider that a common SharePoint set up relies on:

- Microsoft
- Structured Query Language (SQL) database(s)
- Internet Information Server (IIS)
- Active Directory
- Domain Name System (DNS)
- Enterprise networking
- Incoming and outgoing email servers

You’ll not only need IT personnel with expertise in these areas, but they’ll need a working understanding of ERM and what you’re trying to accomplish in order to build your platform successfully.

**Support**

SharePoint system administration is a big undertaking. ERM programs are typically “tacked on” to an already existing infrastructure, which may use an already established taxonomy (not a risk taxonomy, but a SharePoint naming convention that was probably created without much consideration for ERM).

Moreover, because SharePoint systems are built from the ground up, bugs and errors can be hidden deep in the infrastructure of the system. Troubleshooting any SharePoint outages take time and relies on internal IT department. Consider how often your IT team seems understaffed and over-worked in an ever expanding web of enterprise systems.
How likely is it that they’ll get to your support with get to your support ticket in a timely fashion?

Costs
Asking what SharePoint will cost is like estimating the cost of a house. While you might have an idea of the initial costs, the costs of maintaining and operating the system must be accounted for the get the total cost of ownership (TCO).

The costs of implementing SharePoint range wildly, especially for use cases as unique and broad reaching as Enterprise Risk Management.

Finally, if you’d like to stay up to date with existing technology, upgrading to newer versions of SharePoint can require the purchase of entirely new infrastructure.

LogicManager’s SaaS offering includes quarterly upgrades, where we introduce automatically the newest best practices that have been suggested by our customers at no additional cost and with no involvement from your IT personnel. LogicManager also provides continual training and support from both a business and IT perspective, both dedicated to your success as a risk manager. Finally, our pricing is transparent. No hidden fees and no minimum licensing let you evolve your program over time, with your dedicated business analysts there every step of the way to solve challenges and relay success stories from similar customers.
RIMS Risk Maturity Model: ERM Approach and Process Management

Posted by Steven Minsky on June 6, 2014 at 5:12pm

Last week, we introduced the latest findings from studies of the RIMS Risk Maturity Model (RMM). In an effort to explain the model and results of the study more fully, it’s beneficial to break the RMM into each of its attributes,

This week we’ll examine the first two attributes of an effective ERM program, ERM Based Approach and ERM Process Management.

ERM Based Approach

The focus of this attribute is to move organizations from an old, obsolete style of governance to a more holistic, integrated approach. Old-style governance is focused on regulatory compliance and silo specific risk management. The problem with this approach is it leaves the organization exposed to risk that isn’t governed by regulatory mandates, as well as cross functional risk that may be systemic to the company.
We see examples of failures in this approach all the time. West Virginia’s water contamination crisis was caused by a series of risks with inadequate controls – the chemical tank was not adequately surveyed, the employees were not directed to immediately report the leak, even the water filtration organization wrongly estimated that it could filter the chemicals out. None of these entities were at fault from a regulatory perspective, but they were still on the hook for millions in remediation (the chemical plant filed for Chapter 11 bankruptcy in January).

An ERM approach moves organizations past regulatory concerns, which are only a subset of the overall risk universe. This requires a number of activities that the Risk Maturity Model identifies as drivers of ERM Maturity – tone from the top, assimilation into front line activities, risk ownership – which when combined result in a more risk-aware enterprise.

**RIMS Risk Maturity Model: ERM Process Management**

With a new governance mindset in place, organizations can move to applying a risk-based process framework of Identify, Assess, Evaluate, Mitigate and Monitor within each business process. The Risk Maturity Model assesses the degree to which these activities are pervasive inside business processes.
Many executives misinterpret these processes as unique to ERM, when in fact the steps are iterative, constantly reoccurring within organizations but without any defined process or standardizations.

The key to ERM Process management is to create a common language and structure so areas can better transfer knowledge to each other where beneficial. This is done by integrating these framework steps into the business in a way that provides accountability, repeatability, and adequate reporting. A great example is the Vendor Management Governance function. Vendor Management is frequently tasked with identifying critical vendors, assessing their risk (e.g. “due diligence”) and then managing through mitigation (contracts, insurance certificates, etc.) and monitoring (shipping times, order completion).

The problem is Vendor Management, like other functions, is operating independently with too little information exchanged between Vendor Management and other governance functions.

Why is this important?

Strategic Imperatives are by nature cross-functional, but are rarely linked to processes and activities on the front line.
When not linked, risks to corporate objectives are either not addressed or treated differently by the business processes. This alignment is a critical driver of ERM maturity. Organizations that can effectively communicate goals, not just at the corporate level, but down to the front lines, are better equipped to achieve results and elevate concerns.
Why are so many companies missing the point? ERM’s Role in Risk Prevention

Posted by Steven Minsky on July 21, 2014 at 5:00pm

Regardless of guilt or innocence, FedEx’s recent indictment has reminded us that in today’s world of complex global interactions and increased regulations, organizations must have a strong handle on interrelated risk, business processes, and relationships.

This past week, FedEx made headlines for knowingly assisting illegal online pharmacies, according to the U.S. Federal Government. The company is being charged with conspiracy to distribute controlled substances and drug trafficking, as reports claim the shipping company willfully delivered unprescribed medications for over a decade.

Whether or not management and the Board of Directors were aware of the situation is a major factor in the case but nevertheless, FedEx has been indicted on a violation of the Controlled Substance Act.
Just over a year ago, FedEx’s competitor UPS found itself in a similar situation. UPS admitted to knowingly distributing controlled substances through illegal means, and they agreed “to establish a compliance program designed to ensure such customers won’t be able to use its services to illegally distribute drugs.”

Unfortunately, FedEx failed to take preventative steps and is now caught in a legal battle, facing possible fines over $800 million. Although such a compliance program may seem standard practice, FedEx is not alone with its lack of governance.

Many companies are far behind in establishing effective controls and processes relating to risk management. Linking policies and procedures that are already in place to the specific compliance and regulatory standards they support, uncovers business process gaps and allows for efficient mitigation activities. Without transparency into compliance gaps and existing oversight, events such as those experienced by FedEx and UPS are all but inevitable.

To ensure full transparency, it is critical to take things a step further and create an enterprise-wide governance program. Compliance management only goes so far on its own; integrating other existing governance areas such as risk, audit, and business continuity planning (BCP) drastically increases the value of compliance efforts.
To ensure full transparency, it is critical to take things a step further and create an enterprise-wide governance program. Compliance management only goes so far on its own; integrating other existing governance areas such as risk, audit, and business continuity planning (BCP) drastically increases the value of compliance efforts. Coordinating and sharing overlapping information between these functions ensures that all risks are identified and remain uncovered. In other words, creating a true enterprise risk management (ERM).

Damage control and press release statements can only go so far once an incident, like FedEx’s, occurs. The repercussions can be nearly impossible to bounce back from, regardless of a company’s size or financial standing. Taking a reactive approach versus a proactive, companies are left facing consequences instead of preventing surprises in the form of effective enterprise risk management.
Risks Management is an old topic that has existed since time immemorial. In today's economic world, it must be more organized so as to effectively implement its strategies. There are a number of challenges associated with the Governance, Risk and Compliance implementations. The primary step for any Enterprises must be to prevent, prepare and respond to those issues.

Effective application of GRC helps the organization to oversee and automate the operational processes. The Board of Directors and Management Committee must develop the awareness of the risk environment to counteract act it proficiently.

So what do you mean by effective implementation of GRC Solutions?

It has been observed when an organization is in a transition state, new risks emerge. It is critical to manage the risks associated with this transition usually related to activities such as:

- Developing transitional care models
- Data Sharing
- Agreement like prayer contracts
- Establishing provider networks
Integrating GRC solution tools enables an organization to minimize the redundant activities, escalate the automation processes and generate accurate data. These tools help the organization to reduce costs related to operations. It is vital for an organization to understand the objective and goals of integrating these GRC tools. Thus implementation of GRC tools commences with the planning process and is successful when the organization has achieved the optimized and efficient functioning of the GRC tool.

Often critical issues are encountered during the maintenance of GRC tool. Some of them are:

**Ownership of the tool:**

A particular department must take charge of the tool and the problems and support associated with it. Department like IT department usually supports the GRC tool and helps in timely risk management.

**Security Issues:**

Often organizations may face security breaches or cyber threats. Periodic maintenance of this tool is necessary where every activity can be monitored, recorded and retained.
Monitoring and Communication of Data:

Risk managers and employees must regularly report to a higher authority about their daily activities and work progress.

These tools and solutions may require appropriate execution and maintenance and yet they remain one of the most powerful risk management tools. It is only through implementation of these tools at a proper time and experience that organizations adopt risk management tools specific to their business.
As organizations turn to Enterprise Risk Management (ERM) Software to automate and enhance aspects of their ERM Programs, it’s time to take a critical look at the ERM and GRC marketplace to determine where gaps exist between the current offerings and the needs of risk managers.

Many GRC tools on the market today offer a separate ERM module at an additional cost. If the goal of enterprise risk management is to take traditionally silo’d information and communicate it with a single framework, does it make sense to offer ERM as a part, or module, of a platform?

Risk Managers must be wary when evaluating ERM software, and there are a few questions they should ask of all vendors.

**Does your solution support the best practices outlined by an accepted ERM Framework?**

The answer from an enterprise risk perspective should be an unqualified yes.
There are considerable resources available to risk managers (i.e. the RIMS Risk Maturity Model) that can provide a framework an ERM program, and if the ERM solution in question does not explicitly adhere to one or more of these standards, it’s likely that you’ll find yourself at a roadblock only a year or two down the road.

ERM programs forced to operate with tools not designed for true Enterprise Risk Management become quickly frustrated with their results; and worse, their executives and leadership become disenfranchised with the entire concept of ERM, putting their jobs in jeopardy.

**Is your solution flexible enough to fit the unique and evolving responsibilities of your ERM program?**

Enterprise Risk Managers have been tasked with the enormous responsibility of providing transparency and insight into their organization's risk universe. In order to accomplish that goal, an ERM software must be cross-functional and capable of aggregating silo’d information dynamically. Ask to see information aggregated by strategic goal, geographic location, or by a risk category currently in use by your company.

As your program grows, chances are your responsibilities will grow to compliance, policy management, business continuity, or other key function.
Any solution should be flexible enough to tackle these functions within the confines of your ERM framework. Many GRC Software solutions consider these roles to be separate. Look for an integrated tool that doesn’t charge extra for the modules you need, and keep in mind that your responsibilities today might not be the same as they are a year down the road. Your ERM solution should grow with your program, not define or limit it.

**Does your ERM solution provide the support necessary to ensure success?**

Many ERM programs are just beginning to evaluate software. Having worked hard to build your business case, set aside a budget, and evaluate solutions, the worst case scenario would be selecting an ERM Software that could take months, even years, to implement effectively. Risk Managers cannot afford a lengthy implementation timeframe while they work towards the milestones that will justify their solution. In addition, your solution should provide support tailored to your needs. Has your account representative supported the ERM programs of other organizations? Can they pass along best practices and build an implementation schedule around your milestones? And finally, can they do it in less than 90 days.
I came across a great presentation on Reputation Risk from Martin Davies of Causal Capital. It outlined the many dimensions of this onerous corporate threat.

It offered a definition, a list of risk factors, its impact on a company’s financial condition and proposed frameworks to mitigate its effects.

In the pantheon of risk factors, reputational risk is the classic riddle wrapped in a mystery. Its obtuse nature is due in part because it can spring from a multitude of internal and external factors. This makes predicting the occurrence of a reputational risk event difficult to assess and near impossible to quantify making ROI mitigation funding decisions a perplexing task.

Reputation risk seems to loom as a phantom menace that inhabits the dismal swamp of innumerable asymmetric risk factors. Its appearance is rare but potentially catastrophic in nature because it strikes at the heart of brand value and corporate integrity.
The dissolution of Arthur Andersen due to its failures to detect fraudulent business and accounting practices at Waste Management, Worldcom and Enron destroyed the firms reputation for honesty and integrity. Though some argue the cause of this spectacular corporate collapse was due to the contradictions of an attestation/consultancy business model, AA’s pattern of high profile failures in its attestation business made it impossible to continue in business as a firm with unimpeachable standards for audit and accountancy excellence.

Though corporate dissolution is the worst case scenario resulting from a catastrophic reputational risk event, larger firms with the financial wherewithal and organizational resource to underwrite corporate resilience strategies are best positioned to overcome the severe shocks of a reputation risk event. Mitigation initiatives must be more than a PR exercise in damage control. Senior management must take ownership of the event and implement a strategy that allocates resources to the problem to assure stakeholders that an optimal return on capital employed will be realized to the benefit of a sustainable enterprise.

Though reputational risk seems to arise from a kisomet of asymmetrical factors, which are difficult to foresee and nearly impossible to plan for due to the limitations of linear causation and factor biases of quantitative based risk models;
reputational risk is best addressed by striving for GRC (governance, risk compliance) excellence throughout the corporate enterprise.

This is particularly important for SME’s who lack an expansive balance sheet, financial reserves and organizational resources to ride out and overcome the profound impact of a reputational risk event.

Quantification of reputation risk is difficult to measure. The cost of mitigation initiatives and the expected loss realized from a reputational risk event must be funded through the GRC culture of the enterprise. The above slide caught my attention because it graphically displays the impact of a reputational risk event on the equity value of a publically traded company. Though equity exchanges are good barometers to determine monetary impact of a risk event, the managers of privately owned firms are beholden to a different set of expectations of closely held corporate stakeholders.

Amorphous performance standards of idiosyncratic investors, the close coupling of corporate goodwill, shareholder identification, corporate identity and product branding concentrates and magnifies the intensity of reputation risk.
SMEs mitigate reputational risk factors by developing a vigilant GRC culture that encourages the engagement of all employees in the mission of the enterprise. In so doing, all company stakeholders are deputized as vigilant risk managers; all wholly invested in the protection of corporate goodwill and the creation of long term sustainable value of an extended enterprise.

Sum2 believe this to be the case as well. Our clients engage risk as a daily cost of doing business. We design risk management products for small business managers that empower them to lower the odds and consequences of damaging risk events while positioning themselves to be the beneficiaries of opportunities changing market conditions produce.
Colleges and Universities are some of the most at risk institutions when it comes to high profiles failures in risk management.

Reputational risk – and remaining off the homepage of CNN – requires an active approach to managing enterprise governance, and most universities are unsure where to start. An Association of Governing Boards of Universities and Colleges (AGB) report finds:

“After five years of change and upheaval, why is it that governing boards of colleges and universities continue to consider risk on a largely ad hoc basis? The findings from a recent survey... indicate a modest increase in the use of risk assessment in high-level decision making over the past five years, but they also show that boards and administrators are not yet substantially committed to this process.”
The AGB report, entitled “A Wake-up Call: Enterprise Risk Management at Colleges and Universi...,” explores this disconnect more fully while making the following recommendations:

- Make Risk Management a Priority
- Implement a sustained ERM effort by Senior Administration
- Engage the Governing Board in Risk Monitoring
- Discuss institutional Risks Frequently and Regularly
- Share Information to Meet Obligations
- Evaluate the Institutions Work on an Institutional Basis

LogicManager applauds the AGB’s commitment to informing Colleges and Universities about risk management. In order to evaluate the current state of ERM within your institution of higher learning, colleges should have a board or senior administrative member complete the RIMS Risk Maturity Model (RMM) with their dedicated risk management team. The RMM will evaluate the current state of your ERM program, while providing a roadmap for improvement and grading your program according to the best practices of COSO & ISO frameworks.

Finally, risk management software provides a backbone for risk monitoring by ensuring accountability through risk ownership, transparency by aggregating and sharing risk intelligence, and the ability to manage and elevate concerns before they manifest themselves in negative media attention and loss events.

Read this article on the website Click Here
In the past few weeks, we’ve seen major automobile companies face huge product recalls due to safety errors, creating negative media attention and certain financial penalties.

As a result, automakers are dealing with a damaged reputation and loss of customer trust. At the center of Toyota, Nissan and General Motor’s incidents are two key failures: lack of internal communication and poor enterprise risk management.

Within an organization such as Toyota or General Motors, there are countless departments and employees who have an impact on the final products and their safety. Without proper communication and transparency across these various internal silos, key information can get lost and potential risks can go unnoticed.
Let’s look at General Motor’s recent safety recall as a case study. General Motors began to recall millions of vehicles after nearly a decade of safety and production flaws; globally sold vehicles were equipped with defective ignition switches. This tragedy has recently launched worldwide media frenzy, both Federal and internal investigations, huge fines, and public scrutiny.

The question that remains is how did this safety defect slip through the cracks and become a globally dispersed product? The answer, poor risk management and cross-silo coordination. Identifying, mitigating and monitoring risk on a comprehensive, enterprise wide level would have opened the lines of communication necessary to avoid the blind spots that led to such a large scale safety failure.

Fox News reported the incident stating that “GM has heavily layered and highly compartmentalized management and product design structures. Problems like the ignition switch can be discovered by GM engineers—as the result of customer complaints or tragic accidents—but go unnoticed by other units and senior leadership.”

Engaging leadership, managers and users across departments and levels is a critical element of enterprise risk management.
Without communication between an engineer, a health and safety manager, and the key departmental senior management at various stages of the risk management process, crucial information gets lost between these highly compartmentalized silos.

An ignition switch defect is a quality issue to engineering, but poses much larger risks to customer safety that must be communicated and escalated appropriately.

As a result of unsuccessfully managing risks; General Motors and these other carmakers are now facing a range of negative consequences – adverse reputational impact, consumer skepticism, financial loss and legal liabilities. Applying an ERM framework that integrates business areas is the first step at ensuring risk is communicated effectively.
In previous blogs, I've covered the differences between ERM and GRC offerings. One critical difference I'd like to explore more fully is the concept of Software-as-a-Service, especially as it pertains to the IT departments and legal councils charged with approving your ERM or GRC solution. Due to Software-as-a-Service's relatively recent entry into the Business to Business marketplace, it's not uncommon for risk managers to be concerned, even fear, how solutions that are not exclusively hosted on servers that they control will be perceived internally.

What needs to be highlighted is the enormous burden these groups are under in their organization by operating with decade old evaluation protocol, when as long as the proper due diligence is taken, SaaS is not only a secure solution, but an enormous benefit from the standpoint of organizational agility and flexibility.

Consider Michael Shear and Annie Lowry's recent article from the New York Times, "In Tech Buying, U.S. Still Stuck in Last Century." The article critiques the procurement process used by government agencies and large companies, especially the manner in which they prioritize long, drawn out legal proceedings with familiar vendors over technological innovators at the forefront of their discipline.
Organizations must "move away from an old-fashioned method of technology development that relies on a single, large vendor to develop technology in years-long contracts." In an age of constantly changing technology, taking on long contracts with enormous exit burdens is akin to running down the curtain on your department. Moreover, the innovation necessary to tackle complex problems, like Enterprise Risk Management, isn't found at giant, multinational institutions like IBM and SAP.

So in your evaluation of GRC or ERM software, what requirements can you place on a vendor to ensure your organization isn't stuck with archaic technology in a contract you can't terminate? The answer is Software-as-a-Service.

True SaaS vendors will not lock you in to long term contracts, and because of the way the infrastructure is managed, your implementation is reduced to less than 5 business days, so you'll be able to evaluate quickly whether the solution will suit your needs. Because the solution is hosted by the vendor, you'll be working with the latest improvements and updates without having to pay for maintenance, upgrades, or additional licensing. That's a significant cost savings, a competitive advantage, and peace of mind that the vendor will do everything possible to satisfy your unique requirements.
SEC Reprioritizes ERM in 2014

The Security and Exchange Commission announced its examination priorities for the New Year, and Enterprise Risk Management heads the list.

The priorities, selected by Senior Staff from the National Examination Program, aim to address areas of weakness that threaten fair, orderly, and efficient markets.

On the subject of Enterprise Risk Management, the NEP states that it will continue to meet with boards and high level senior management to discuss the firm’s Enterprise Risk Management process, especially as it pertains to identifying legal, compliance, financial, and operational risks.

This initiative is designed to: (i) evaluate firms’ control environment and “tone at the top,” (ii) understand firms’ approach to conflict and risk management, and (iii) initiate a dialogue on key risks and regulatory requirements.

The SEC’s renewed focus comes on the heels of 2013, a year that featured a bevy of high profile failures in risk management, such as the Edward Snowden NSA leaks, European horse meat scandal, Barney’s and Macy’s shop-and-frisk incident, Carnival Cruise Line’s generator fire, and culminating with Target’s credit card heist and the security breach of over 70 million customer records.
Also of note is the language used in the Commission’s briefing. Too often, enterprise risk management is seen as a static or silo’d practice, but the SEC specifically identifies dialogue as a critical component of any ERM program. The SEC is further demonstrating the need for organizations to be proactive in their risk management practices, and the days of maintaining an out-of-sight out-of-mind approach to risk management have been replaced by regulations designed to prosecute boards and leadership that fail to adequately address their ERM process.
Choosing the right areas to audit based on risk, or scoping, is the most important aspect of an audit management program. ERM provides five steps to ensure your audit program is truly risk based.

The key to adding value in the internal audit process is to first determine where the biggest contributors are to the business success, also known as a risk based approach. Too often internal audits get scheduled based on a rotational basis, gut feelings or suspicions or orders from management.

**Scoping by Objectives:**

The best way to move your audit plan towards a risk based approach is to work backwards – starting with goals, to the processes that deliver on these goals, and then to the risk, controls and monitoring within the business processes that deliver on these objectives. An ERM software system has a risk taxonomy that enables internal auditors to simply select a goal from a list and pull up an aggregated collection of related business process risks, controls and tests across all areas of the enterprise.
Scoping by Business Process:

An ERM software system will allow you to have a risk assessment of the inherent weaknesses in each sub-process, allowing you to prioritize which of these risk, control and test combinations are truly key. This scoping dramatically reduces the low risk, low impact audit content in your annual audit plans. You’ll also have access to the risk assessments completed by the risk owners themselves, allowing audit to validate their assessments against your defined criteria.

Scoping Resources:

Connecting the most important assets to the business processes that contribute most to each strategic objective will create a risked based or prioritized short list of the people, physical assets, IT assets and vendor partners that support your corporate objectives. Typically, it is not just one vendor that causes a failure, but a collection of vendors and other resources that result in critical damage. Auditing resources in isolation is both too time consuming and too narrowly focused, missing the critical dependencies between controls and their contribution to corporate strategy. ERM systems make it easy to aggregate individual resource assessments with business process and vendor assessments, prioritizing aspects of your organizations to points of failure that require auditing.
Risk Libraries:

What are the key risks for each area to be audited? Having a robust risk library that is mapped to specific business processes, industry specific challenges, and is root cause based will guide internal auditors to identify and concentrate on the high inherent and residual risks within an audit plan. Why root cause based? Because a root cause approach makes it easy for auditors to match risks to controls, and to determine the effectiveness of a control over a risk. For example, the control over fraud will be different depending on the source of fraud, be it employees, contractors, systems, or unknown external rings.

Risk Taxonomy:

To have a risk based approach to internal audit, you need a simple and practical framework that takes complex material, breaks it down, and makes it easy for everyone in the organization to contribute to their control environment. Having a standardized set of criteria that is rationalized, aligned, and scaled to be universally applicable makes risk information available on an apples to apples basis. A Risk Taxonomy enabled approach arms the auditor with structured data and the tools to do objective process and resource based scoping.
As the last line of defense, its audit’s job to uncover deficiencies that are not being appropriately mitigated. Ensuring that your control environment is adequate and that risks to the board are well managed isn't only best practice, but is now required by the Institute of Internal Auditors (IIA). The effectiveness of your audit program is largely based on not just how you audit, but what you choose to audit next.
Identifying, Assessing and Managing Risks From an Enterprise Risk Management (ERM) Perspective

In his book, The Black Swan: The Impact of the Highly Improbable, Nassim Nicholas Taleb defines “Black Swans” as random and rare events that underlie our lives and business, are nearly impossible to predict and and have a huge impact when they materialize. According to Taleb, “Black Swans being unpredictable, we need to adjust to their existence, rather than naively try to predict them.”

In the past several years, many large-scale events (similar in nature to Black Swans) have manifested and changed the course of many businesses. Examples of these events include increased food and product safety issues; energy supply volatility; global financial instability; geopolitical instability; natural disasters etc. These events have had significant impact not only on the organizations located in the borders where they occurred, but also on various parties across geographical borders, industries and sectors.

Because of this unprecedented change in the business environment and risk landscape,
organizations need to take a new look at their risk management processes and the allocation of resources to ensure that emerging risks are effectively identified, assessed, managed and monitored at all levels of the organization i.e. from strategic planning to day-to-day operational processes.

Although many organizations have put in place risk management processes to identify, assess and manage enterprise risks, their programs are repeatedly failing to identify emerging risks relevant to the organization; assess their impact and interconnectedness with other risks and mitigate them. This failure has implications for the organization’s strategy and objectives. It is therefore important that the organization’s board and senior management continuously scan the business environment for changes that could impact strategy execution and the achievement of business objectives.

A systematic approach to risk identification is achieved by first considering what risks the organization is facing on the macro and micro levels. Macro-risk identification involves the identification of major risks that may have significant impact, financial and otherwise, on the organization by using techniques such as industry analysis, competitor analysis, country analysis and market/environmental analysis. Micro-risk identification involves identifying sub-risks within the major risk classes that can usually be prevented by introducing effective risk control measures.
Risk inspections, HAZOP studies, failure mode and effect analysis (FMEA), fault tree analysis (FTA), hazard indices, safety audits, legislation and codes of practice, research and risk sourcing can all be used to identify risks and their sources at a micro level.

In a fast-paced and changing business environment which is always presenting opportunities and threats, the organization needs to build a dynamic ERM model, be proactive and resilient. Lessons are still being learnt from the 2008 Global Financial Crisis (GFC) which started first in the US and spread overnight to other developed and developing economies. What began as a crisis only within the banking sector immediately spread over to other non-banking industries, for example, the automotive industry. This GFC revealed the shortcomings in the risk programs of many financial and non-financial institutions. Organizations that were once thought of as “too big to fail” have disappeared while others have come out stronger.

Since then, supported by a stronger risk management culture, organizations across industries, sectors and national borders have attempted to strengthen their risk management programs by using techniques such as risk assessment, scenario analysis, event simulations and stress testing as a basis for determining response strategies that are aligned with the organization’s strategies, objectives, risk appetite and tolerance.
Today, risks are very much interconnected and go beyond enterprises, industries and national borders. Businesses no longer conduct business locally. Globalization has made it easier for organizations to seek opportunities across national borders either through direct market entry or through joint ventures and collaboration with foreign partners.

Although benefits can be accrued from collaboration, because of these interactions, the organization is also exposed to a wide range of risks which in turn has increased the complexities in managing risks.

Effectively applying ERM principles can help the business address risks that may appear unknown but have a huge impact when they materialize. By implementing ERM and building a strong risk management culture throughout the organization, business leaders are able to:

- Identify emerging risks relevant to the organization’s strategy and objectives by carefully scanning and analyzing all the relevant risk factors.
- Assess the significance of different risks to the business and stakeholders, their interconnectedness with other risks and implication to the business.
- Determine risk response strategies as well as consider collaboration with external parties to mitigate the risks and possibly even capture opportunities.
- Regularly monitor emerging risks through the effective use of qualitative and quantitative indicators.
In a global economy where opportunities are hunted across national borders and industries, risks spread equally very much. It is therefore important for boards and senior managers to ensure that the organization’s risk tolerances are not exceeded. Proactively monitoring risks and analyzing trends and the underlying relationships between risks helps organizations avoid significant losses and seize opportunities. By applying ERM to emerging risks, the board and management are able to reveal to investors and other stakeholders the organization’s agility to detect and respond to large-scale risks.

Risks affecting the organization’s business performance can be known, unknown and unknowable. Where the risks are known, their causes, probability of occurrence and likely impacts are well defined. These risks can therefore be measured and managed because they have manifested previously. Unknown risks are well defined but impossible to assign probabilities as to the occurrence of specific events e.g. acts of terrorism. Unknowable risks have not yet manifested and understanding of these is more of a speculative event. Understanding this distinction of risks is important. It helps with the allocation and reallocation of resources to help foresee risks that are currently being ignored.
Identifying, assessing and managing risks relevant to the organization should form part of its strategic planning and performance management processes. This also requires the organization to strengthen its ERM capabilities and skills to ensure adequate risk oversight and management. In addition to identifying risks relative to its key objectives, the organization also needs to embrace and manage risks throughout the value chain. Each relationship within the value chain not only does it imply new opportunities, but also risks. If one of the relationships fails, this results in consequences for all the relationship partners. Thus, it is important to understand the risks faced by each partner when identifying and evaluating risks. Through historical data and forward-looking analysis, the organization will be able to go beyond known risks and expose what may seem to be unknown risks.

In today’s complex and rapidly changing environment where an organization can thrive or disappear overnight, effectively applying ERM principles and building a strong risk culture to identify, assess and manage enterprise risks is important for executing strategy, driving business performance and meeting various stakeholder expectations.
Operational risk management (ORM) is one of the components that fall under Enterprise Risk Management Solutions. People, process, system or external events are the direct causes of operational risks.

In the early 2000s a number of companies in UK fell prey to operational risk as a result of internal and external fraudulent actions. And with the 2008 financial crisis most of the business in UK had their attention towards operational risk management solutions.

Then was the evolution of ORM software solutions. Many technology-based companies developed ORM software that facilitated internal audit as well.

With time, operational risk management software was equipped as a complete package with features like managing operations, conducting financial audits, data integrity and more.
Further advancements were made in ORM software solutions in UK when companies started realizing the significance of workflow, work style and organizational culture. After which ORM framework and ORM software were customized to suit the employees and work system. It was well integrated into the business operations that it served as a part of everyday routine process.

Now ORM platforms also function as a GRC guide (governance, risk and compliance) to the organizations and its employees.

With the installation of ORM software many operations are made easy like:

- Identifying and mitigating of operational risk
- Aiding risk visibility
- Facilitating risk assessment
- Maintaining transparency throughout all the departments of the organization
- Creating a reliable network of connections within an organization
- Performing internal and financial audits
- Having a check upon regulatory policies and compliance
- Secured access to centralized data
- Integrating communication and information
- Easing managerial efforts

Read this article on the website Click Here