Lessons Not Learned: The Role of Operational Risk in Rogue Trading

Serious lapses in operational risk control have been at the heart of the major trading scandals of the past two decades, from the Kidder fiasco in 1994 through the UBS meltdown last year.

By Amy Poster and Elizabeth Southworth

The financial services industry is proving to have a perennially short memory. Close at the heels of the Societe Generale trading scandal where a lone trader, Jerome Kerviel, managed to lose $7.2 billion in unauthorized European Index Future trades, UBS, in 2011, reported a similar scenario. In UBS' case, another lone trader, Kweku Adoboli, escaped the firm's risk management radar, losing $2.3 billion on fraudulent Delta 1 and exchange-traded funds (ETF) transactions.

Most striking is that over the last two decades, there have been repeated cases of rogue trading befalling many of the largest financial institutions. Despite sophisticated risk management governance and infrastructures, continued lapses in trading surveillance were apparent at many of these firms. As our Rogue Trading Hall of Fame indicates (see Table 1, page 22), this had a catastropic impact on several firms.

Kidder Peabody never recovered from the Joe Jett episode in 1994, and went into bankruptcy shortly thereafter. Barings Bank, the oldest merchant bank in London dating back to 1762, collapsed in 1995 after Nick Leeson hit the bank with a $1.4 billion loss on unauthorized futures and options trades on Nikkei 225 and Japanese government bonds. Daiwa Bank's New York branch shut down operations in 1995, and bank senior executives were subsequently slapped with a $340 million fine, as well as multiple felony and conspiracy charges to defraud the US Federal Reserve Bank.

However, AIG's credit default swaps scandal was probably the most devastating of all trading imbroglios. In what appears to have been a unit above any of AIG's risk management supervision, Joseph Cassano, head of AIG Financial Products (AIGFP) in London, was allowed to assume enormous risk by providing credit protection to many financial institutions in the form of credit default swaps (CDS). As the 2008 subprime mortgage crisis came to a head, AIGFP suffered enormous losses on their CDS trading, prompting credit agencies to downgrade AIG's credit rating.

The loss of its AAA credit rating threw the parent, AIG, into a severe liquidity crisis, effectively bankrupting the company. What ensued was a government bailout to the tune of $85.5 billion, as AIG was deemed critical to the US financial system or "too big to fail."

So, how were these individuals able to remain undetected (and seemingly unsupervised) for many years, without attracting the attention of both mid- and senior-level management? Tragically, these trading scandals left firms like Kidder Peabody, Barings Bank and Daiwa Bank as road kill.

This article explores key aspects of operational risk control that are often neglected and the limitations of quantitative risk measures like value-at-risk (VaR), stress testing and model validation. Although these tools are essential to a firm's risk governance program, a holistic enterprise risk management approach is critical.

Based on the history of rogue trading scandals, it is clearer than ever that effective trading surveillance cannot be achieved without sustained, regular dialogue between risk managers, traders and management. It is most critical to provide constructive challenges, to ask tough questions and to escalate issues up the management chain if responses from trading are unsatisfactory. While the Dodd/Frank Act and Basel III may provide reporting transparency, especially for derivative products, clearing through exchanges and transitioning from old to new reporting platforms can present a different set of operational risks.

Table 1: Rogue Trading Hall of Fame

Year	Company	Trader	Auditor	Years to Discovery	Source of Loss	Problem Type	Risk Classification	Trading Losses ($B)	Final Result	Auditor Sanction
1994	Kidder Peabody	Joseph Jett	KPMG	2	False profits on US Treasury forward trades.	Flaw in Kidder Peabody's computer systems. System incorrectly valued forward traded trades as immediately settled.	Operational/IT Systems	0.35	Kidder Peabody Bankruptcy.	
1995	Barings Bank	Nick Leeson	Deloitte and Touche	3	Unauthorized speculative position on A) futures linked to Nikkei 225 and Japanese government bonds; and B) options on Nikkei index.	A) Trader was allowed to execute AND settle his own trades; B) unchecked error account. Error accounts used to correct mistakes in trading.	Operational	1.40	Collapse of Barings Bank.	Deloitte and Touche found guilty of negligence in its audit by UK court. Red flag that Barings posted more margin to Singapore futures exchange than it had received from customer accounts.
1995	Daiwa Bank	Toshihide Iguchi	Showa Ota (part of Ernst and Young)	11	Unauthorized US Treasury bond trading.	Falsifying subcustody account statements held at Bankers Trust. (Note: Iguchi's did not relinquish back-office responsibilities with his promotion to trader.)	Operational	1.10	A) Daiwa end of US Operations; B) $340mm fine; C) 16 counts of Federal felonies; D) 2 counts of conspiracy to defraud US and Federal Reserve bank; E) 1 count misprision of a felony; F) 10 counts of falsifying bank records; G) 2 counts of wire fraud and; H) 1 count of obstructing a bank examination.	
1996	Morgan Grenfell Asset Management	Peter Young	KPMG	1	Shares-investments in unlisted companies.	A) Shell companies in Luxembourg to hide dealings in unlisted companies, mainly in Scandinavia; B) breach of rules in investing more than 10% in unlisted stocks.	Operational/Legal and Compliance — Lack of oversight on cross border transactions/legal entities.	0.66	Eventual sale to Deutsche Bank.	
1997	UBS	Ramy Goldstein	Ernst and Young	6	Inadequately hedged equity derivative trades.	A) Independence from the bankor company risk control process; B) conflicts of interest and overlapping of responsibilities in UBS' risk management efforts.	Operational/Legal and Compliance	0.68	Merger with Swiss Bank Corporation (SBC).	
2002	Allfirst Financial/Allied Irish Bank	John Rusnak	Ernst and Young	2	FX Options and bets on Japanese yen.	A) Booking bogus trades with Asian counterparties; B) forged trade confirmations.	Operational	0.75	Allfirst Financial sold to M&T Bank.	
2008	Societe Generale	Jerome Kerviel	Ernst and Young	3	European Index Futures.	Unhedged futures contracts covered with bogus forward trades.	Operational	7.22	Net loss reported for one quarter.	
2008	AIGFP	Joseph Cassano	Price Waterhouse Coopers (PwC)	n/a	Credit Default Swaps (CDS).	Unhedged CDS.	Adverse external events-subprime mortgage crisis/credit ratings downgrade.	85.50 *	AIG Bankruptcy, US Treasury/NY Fed bailout; continuing majority ownership by US Government.	
2011	UBS	Kweku Adoboli	Ernst and Young	3	Delta 1 and Equities ETF.	Unmonitored "failed to deliver trades."	Operational	2.30	UBS CEO resignation and management shakeup.	

Sources: *Baltimore Sun, Bilanz, New York Times, The Independent, Wall Street Journal, Wall Street & Technology*
* Total bailout amount to rescue AIG, "Too Big To Fail" status.

Operational Black Holes: Costs and Effects

History has shown that the majority of trading debacles were attributable to serious lapses in operational risk control. The day-to-day operations of a global bank involve thousands of transactions in multiple products and currencies across multiple regions and legal entities. This complex web of operational processes makes it vulnerable to breakdowns and, in extreme cases, to fraud.

In at least two recent instances (Adoboli at UBS and Kerviel at SocGen), the prior back-office experience of the fraudsters provided them with the intimate knowledge of how to exploit their firms' operational vulnerabilities to their advantage. With the exception of Joe Jett and Kidder Peabody, all the cases of

rogue trading occurred in a regional or remote office, far from the oversight of stronger audit, compliance and risk teams.

Table 2 (see below) provides a summary of common types of operational breakdowns.

These "black holes" are often overseen by mostly junior back-office staff and considered part of the daily tedious back-office reconciliation procedures. Given the disparity in compensation and education between front office and operations staff, it is not hard to understand how traders can intimidate operations staff into submission.

For example, in the case of John Rusnak of Allfirst Financial Inc. in Baltimore, Maryland, a subsidiary of Allied Irish Bank, an independent investigation revealed that Mr. Rusnak often berated back-office staff, when questioned, and became verbally abusive when pressed for information.[1] The last straw came when he failed to produce confirms from Asian counterparties under pressure from a more diligent and senior operations manager. These aggressive tactics allowed Mr. Rusnak to accumulate $750 million of trading losses, over a two-year period leading to the eventual sale of Allfirst Financial to a regional competitor.

Table 2: Operational Risk Black Holes

Type	Ops Risk Issue	Result	Department Responsible
Erroneous Adjustments	Adjustments made in error may "fix" a "true break," therefore hiding a bogus trade.	Undetected trading exposure.	Operations
Poor Reconciliation due diligence	All too often, when resolving breaks, operations might "take the traders word for it" instead of taking the time to fully research the cause of the break.	Undetected trading exposure.	Operations/Accounting
Incomplete FOBO Reconciliations	Relevant accounts missing from the reconciliation.	Positions sitting in unmonitored accounts.	Operations and IT
"As of" Trades	Multiple "as of" trades can be a signal that a trader is creating positions "after the fact."	Inaccurate trade position reporting; fraudulent trades creation.	Risk and Compliance
Cancelled Trades	Multiple cancellations can be a signal that a trader is booking bogus trades.	Concealing bogus trades by cancelling them before they fail or are "don't know" (DK'd) by a counterparty.	Risk and Compliance
Failed Trades	A counterparty may not be aware of the trade or is unable to deliver on the trade.	Unresolved/uncorrected trades resolution, increasing exposure and penalties over time.	Back Office
Confirmations	Confirmations with counterparties may not be matched or sent out at all.	Heightens the risk of failed trades or bogus trades.	Middle Office
Poor Technology Monitoring	Technology breakdowns such as imperfect back-office feeds, or logic as to what accounts appear on which reconciliations, can hide exposure.	Trades may be missing in a back-office batch or rejected due to data integrity issues. This may not be caught resulting in a costly error and increased hidden exposure.	IT

Traders can book bogus trades in an array of different account types to conceal losses. Nick Leeson, who used the "5 eights error" account to hide trade losses, was a prime example.

"Parking Trades" — Miscellaneous Trading and Trading-Related Accounts

Firms that maintain various miscellaneous trading and trading-related accounts also have vulnerable spots in their operational process chain. Table 3 (see page 24) provides a list of trading-related accounts and the potential risks when not monitored thoroughly.

In addition to proprietary accounts and customer accounts, firms also use other types of accounts to conduct business. These accounts are necessary to segregate customer funds, balance legal entities and legally transfer funds and securities between business units. When not monitored properly, they can create accounting and operational misrepresentations leading to undetected losses.

Traders can book bogus trades in an array of different account types to conceal these losses. Nick Leeson, who used the "5 eights" error account to hide trade losses, was a prime example.[2] It was widely reported that Leeson originally used the error account to book an erroneous sale of options contracts by one of his colleagues, and then, over time, increasingly utilized the account to book more bad trades. Leeson saddled Barings Bank with a $1.4 billion loss, leading to the bank's eventual closing, after more than two centuries of illustrious existence.

Meanwhile, over an 11-year period, Daiwa Bank's Toshihide Iguchi mismanaged customer custody accounts and sub-custody accounts held at Bankers Trust through unauthorized sales of US Treasury bonds in these accounts. As losses mounted, and with customers continuously requiring interest payments on securities held in custody by Daiwa, Iguchi began falsifying sub-custody bank statements with bogus trades and accounting entries. In the end, Daiwa not only had to repay $377 million to the customer accounts that Iguchi had looted but also had to shut down its US operations, pay an additional $340 million in fines and plead guilty to felony and conspiracy charges to defraud the US Federal Reserve.[3]

Table 3: Miscellaneous Accounts

Account Type	Definition	Potential Risk
Intercompany	Facilitates a transfer of securities of cash between separate legal entities.	A trade may sit in an intercompany account of one entity and never be transferred to the opposing intercompany of the other entity.
Error	Used to book erroneous transactions.	A trader can book bogus trades into this account to hide losses.
Omnibus	Typically, an account used between futures merchants where transactions for multiple clients are held at one futures merchant until they are booked into the relevant client accounts at another futures merchant.	If not reconciled and monitored properly, trades could sit in the omnibus account, exposing one or both of the futures merchants to risk.
Client Facilitation	Principal account used to book executions for a client – executions which are then allocated to that client's account.	Bogus executions can be booked into these accounts and never get allocated.
Custody Account	Customer account held by an institution, but managed by custodian.	Lax monitoring can result in bogus trades executed away from customer instructions.

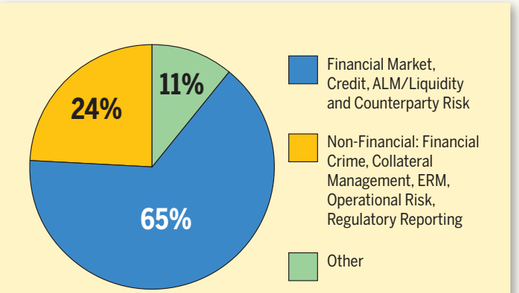
Operational Impact of Mergers: Processes and IT

Past and recent mergers between financial institutions present new areas of operational risks and leave firms vulnerable to rogue trading activities. Post merger infrastructure fragmentation makes managing overall risk and exposure a daunting task. Consolidation of different business units, operations and IT infrastructures can take years to complete. Areas where added operational risk can reside include front-to-back-office reconciliations, overall counterparty risk and proprietary and client exposure reporting.

As business demands continue to drive firms to place priority on purchasing and developing new technologies, consolidating legacy systems invariably takes a back seat. Application fragmentation across various business units makes aggregating risk and exposure on a firmwide basis a difficult task. For example, aggregating exposures to the same product or counterparties across business units, geographical jurisdictions and legal entities could be damaging if a firm fails to integrate new and legacy systems. Recent mergers (e.g., Wells Fargo acquiring Wachovia and Bank of America acquiring Merrill Lynch) exemplify the huge challenge of integrating not only people, but processes and technologies.

The continuing overall trend in risk technology investment spending remains heavily biased towards financial risk management (market, credit, ALM/liquidity and counterparty) versus non financial (AML, financial crime, collateral management, ERM, operational risk and compliance, and regulatory reporting).[4] Graph 1 (below) shows most recent spending estimates to be at about 65% for financial vs. 24% for non-financial and 11% for others.

Graph 1: 2012 Risk Management IT Spending Estimates



Source: Celent, "Strength Under Fire in Risk Management: New Realities, Technology Imperatives and Investment Spending," by Cubillas Ding, February 21, 2012.

Gartner, an IT consulting firm, believes new regulations may further accelerate mergers in the financial services sector.[5] Basel III and the Dodd-Frank Act, due to their new restrictions on proprietary trading activities and higher capital requirements, will impact the viability of smaller institutions. As further consolidations take place, acquiring institutions face the challenge of integrating more applications, offices, products and employees. An attendant result will be new and increased operational risks emerging from these integration activities.

Limitations to Quantitative Measures of Risk

Beginning in the late 1980s, a new standard for measuring market risk had gained traction within the risk community: VaR. This new approach evolved in the last 20 years to be a leading benchmark, and became the cornerstone of risk management in most all of the largest financial institutions.

VaR's popularity had been largely driven by its capability to provide a singular quantitative measure of loss over a specified time horizon and to assign, in dollar terms, the loss of a portfolio's value.[6] However, although VaR will continue to be a mainstay in risk metrics, its limitations have become widely known, with Long Term Capital Management (LTCM) as its

unfortunate poster child.

In 1998, LTCM's well-chronicled meltdown exposed the limitations of VaR modeling and inadequacies of historical probabilities in predicting the future. Because Russia defaulted on its domestic (rather than foreign) debt, something that had never occurred before, LTCM's VaR models assigned a probability of zero and incorrectly calculated the losses of this event. The miscalculation threw LTCM into a liquidity crisis, eventually leading to a bailout by a private consortium of banks and financial institutions.

Stress testing is another methodology used to monitor risk concentrations across business units and relevant risk categories.[7] In addition, stress testing allows risk aggregation that enables firms to test dependencies within risk categories. There are two broad categories employed in stress testing: scenario analysis and sensitivity testing. Scenario analysis, a forward-looking approach that tests hypothetical "could be" events, is a useful tool for a more active and dynamic risk management approach.

Similar to VaR, this approach has significant limitations. One of the key flaws in stress testing is the assumption that a firm's risk exposure is static during the stress period; this assumption might lead a firm to gauge the impact and immediacy of new exposures inaccurately. The recent case of AIGFP offers a good example of why this assumption is flawed. From July to September 2008, the sudden worsening of the subprime mortgage crisis and extreme market volatility severely handicapped AIGFP's ability to exit CDS trades and quickly react to changing market conditions.

For many firms, stress tests that comprehensively measure broad risk categories across business units are generally only undertaken on a limited basis.[8] This limits the ability in developing scenarios to capture non-linearities in complex products, as well as to identify plausible scenario events with financial and operational implications.[9]

Model validation is another important approach for identifying risks in complex products. For liquid assets where there are directly observable prices in the marketplace, pricing is an easy exercise. But with the exponential growth of derivatives and structured products, prices for these assets cannot be directly observed and need to be inferred from related instruments or "proxy."

The process of pricing, known as "marking to model," is dependent on mathematical algorithms combined with subjective judgments.[10] The subjective component, most commonly the choice of the best proxy instrument as a model input, exposes the valuation process to error estimation. However, since many complex instruments "trade by appointment," coming up with the most appropriate proxy is extremely challenging.

Basel III ... is largely focused on guarding against systemic risk and the repeat of the "too big to fail" scenario.

Dodd/Frank Act and Basel III

Although new regulatory initiatives (specifically, the Dodd Frank Act and Basel III) may enhance reporting and transparency in the markets, adoption for financial institutions across the board will be a formidable task. Both compliance and operational requirements are substantial.

On Dodd/Frank alone, there are 400 mandated rules, and only 93 (or a meager 23%) had been finalized as of January 2012.[11] Moreover, participants in derivatives markets in the US have been left with many operational ambiguities as a result of jurisdictional bifurcation between the two main regulatory agencies, the Securities and Exchange Commission (SEC) and Commodity Futures Trade Commission (CFTC), over derivatives products. Some examples where increased operational due diligence will be required for derivatives reporting are in the areas of collateral segregation, cross-border transactions and pre (legacy) versus post (new) Dodd/Frank Act margin requirement reporting.

Basel III, which targets increased capital requirements for the biggest financial institutions, is largely focused on guarding against systemic risk and the repeat of the "too big to fail" scenario. While Basel III addresses liquidity and leverage issues that were found to be drivers in the failures of several institutions during the crisis, further regulatory coverage is extended through the imposition of new capital charges for stressed credit valuation adjustment VaR (CVA VaR) and correlation between financial intermediaries.[12] CVA VaR, which provides an added layer of risk protection to institutions and the financial system on top of market VaR, zeroes in on managing counterparty risk especially concentrated over a number of large institutional dealers.

However, similar to Dodd/Frank, Basel III can only provide a structural framework for firms to manage risk. When dealing with illiquid products, like illiquid CDS' that cannot be cleared, institutions still have to manage risk through traditional reserves and exposure limits.[13]

Closing Thoughts

People risk and human behaviors were at the heart of operational risk that was evident in the largest trading scandals. In nearly every case, the problems lay in failed internal controls and systems and a distorted focus on profits at the expense of appropriate due diligence by mid- and senior-level management. Because these scandals were not mostly driven by external events, new broad regulatory initiatives like Dodd/Frank and Basel III may have little impact on discouraging future rogue trading activities.

People risk and human behaviors were at the heart of operational risk that was evident in the largest trading scandals.

While critical in assessing market, liquidity and credit risk issues, quantitative measures of risk — like VaR, stress testing and model validation — still need to be integrated with operational risk monitoring for a holistic enterprise risk management approach. Past and present merger activities among institutions pose additional challenges in risk aggregation and assimilating legacy systems, especially since investment spending for operational risk technology remains a relatively small part of budgets.

Unless operational risk is at the center of strategic and operational decisions, firms will continue to be vulnerable, despite the presence of enhanced risk analytics and regulatory reform. Most importantly, there can be no substitute for regular and sustained dialogue between risk officers and trading management in order to maintain effective trading surveillance. A robust risk governance process requires a mechanism for personnel, up and down the management chain, to escalate trading or security breaches without fear of economic penalty or retribution. Risk management must exist as the core value of an organization, embedded in its day-to-day operations.

FOOTNOTES

1. "The Risk of Rogues," Louis J. Slifker Jr., *Internal Auditor Magazine*, December 2008.
2. In Chinese numerology, 8 is considered a lucky number.
3. "Daiwa Bank Admits Guilt in Cover Up," Peter Truell, *The New York Times*, February 29, 1996.
4. "Strength Under Fire in Risk Management: New Realities, Technology Imperatives, and Investment Spending," Cubillas Ding, Celent Report, February 21, 2012.
5. "Market Trends: Financial Services Consolidation Poses Both Opportunities and Threats for Technology and Service Providers, North America, 2011," Kristine Pfeiler, March 2011, Gartner Inc. See http://www.gartner.com/id=1567414.
6. "Evaluation of VaR Models Using Historical Data," Darryll Hendricks, Federal Reserve Bank of NY Economic Policy Review, April 1996 (pg. 39).
7. "Cross Sectoral Review of Group Wide identification and Management of Risk Concentrations," The Joint Forum, Basel Committee of Banking Supervision, April 2008 (pg. 25).
8. Ibid, pg. 27.
9. Ibid, pg. 27.
10. "Model Validation: Theory, Practice, and Perspectives," Zeliade Systems whitepapers, May 2011 (pg. 1).
11. "Over Regulated America, The Home of Laizzez Faire is Being Suffocated by Excessive and Badly Written Regulation," *The Economist*, February 28, 2012.
12. "Basel III and Systemic Risk," David Kelley, *Derivatives Week*, September 19, 2011 (pg 10).
13. Ibid, pg. 11.

Amy Poster is a strategic adviser for non-investment activities at Iron Harbor Capital Management. Previously, she worked as a senior advisor in the US Department of Treasury's Office of the Special Inspector General-TARP (SIGTARP), where she was responsible for the development and oversight of US Treasury's Public Private Investment Program (PPIP) and led critical audits of TARP recipients and spearheaded interagency enforcement investigations. Prior to SIGTARP, she was Valuation and Risk Controller for Global Credit Products at Credit Suisse, focusing on pricing, model validation and risk governance. She also led the set up and post-launch risk management of several credit and distressed funds for Credit Suisse's Alternative Capital Division.

Elizabeth Southworth has more than 15 years of capital markets experience, with deep expertise in global equities, derivatives and commodities. She recently served as a strategic operations advisor to the Bolsa Nacional Agropecuaria in Bogota, Colombia, where she advised them on the selection and implementation of an electronic trading infrastructure. Previously, she worked at Bear Stearns for 10 years, holding progressively senior roles in international operations, middle office and institutional trading. During her time at Bear Stearns, she was also responsible for the implementation and oversight of their global equities order management platform.

RETROSPECTIVE