Dissecting the JPMorgan whale: a post-mortem

Patrick McConnell
Macquarie University Applied Finance Centre, Level 3, 10 Spring Street, Sydney, NSW 2000, Australia; email: pjmcconnell@computer.org

(Received December 17, 2013; accepted January 21, 2014)

In many respects, the “London whale” scandal at JPMorgan Chase is similar to other “rogue trading” events, in that a group of traders took large, speculative positions in complex derivative securities that went wrong, resulting in over US$6 billion of trading losses to the firm. As in other rogue trading cases, there were desperate attempts to cover up the losses until they became too big to ignore and eventually had to be recognized in the financial accounts of the bank. However, the whale case, so-called because of the sheer size of the trading positions involved, differs in several important respects from other rogue trading cases, not least because the sheer size and riskiness of the positions were well-known to many executives within JPMorgan, a firm that prided itself on having advanced risk management capabilities and systems. The role of Model Risk in this scandal, while not the primary cause, is important in that at least part of the impetus to take huge positions was due to incorrect risk modeling. Various external and internal inquiries into the events have concluded that critical risk management processes in the bank broke down, not only in the Chief Investment Office, the division in which the losses occurred, but across the bank. In particular, deficiencies in the firm’s Model Development and Approval processes allowed traders to trade while underestimating the risks that they were running. Under Basel II regulations, losses due to process failure are classified as operational risk losses and hence this case demonstrates a significant failure of operational risk management in JPMorgan. This paper dissects the whale scandal from an operational risk perspective using the late Professor Barry Turner’s framework for analyzing organizational disasters. The paper also makes suggestions as to how model risk may be managed to prevent similar losses in future.

1 INTRODUCTION

All models are wrong, but some are useful. Box and Draper (1987)

This paper looks at the failures of risk management that became known as the “whale” scandal, which resulted in trading losses at JPMorgan Chase in the firm’s Chief
Investment Office (CIO), within a framework created by Turner (1976) for analyzing the “development of disasters”. Before analyzing the events leading to the losses using Turner’s framework the events are summarized and a few key concepts explained.

As recommended by Turner (1976), information in this paper is taken predominantly from the reports of official inquiries into the losses, in particular the independent report to the US Congress by the Permanent Subcommittee of Investigations (PSI 2013), the report of an internal “management task force” (JPMorgan 2013) and a report by one of the firm’s regulators, the Commodity Futures Trading Commission (CFTC 2013). In addition, official annual reports and key disclosures by JPMorgan are referenced (JPMorgan 2011, 2012a,c). Together these reports run to almost 2000 pages of evidence, exhibits and transcripts of emails and telephone conversations and so, as a matter of necessity, the selection of material to illustrate key points in this paper is somewhat subjective.

1.1 Summary: the whale losses

It is difficult to condense such a complex case into a few bullet points but, in summary, the events played out over the first five months of 2012, within the CIO division of JPMorgan. Surprisingly, given the size of the resulting losses, the events were triggered by an attempt to reduce risk in anticipation of new regulations designed to increase capital requirements on large banks such as JPMorgan (Basel Committee on Banking Supervision 2010). The trading group within CIO did not waver from their goal but, in trying to execute the reduction strategy in their so-called synthetic credit portfolio (SCP), actually took on a massive amount of additional risk. Far from being rash, the acquisition of this risk was part of a deliberate strategy, known to and agreed with senior management, which badly misfired.

Backing out of trading positions, as demanded by JPMorgan’s management, is rarely without costs. These were initially estimated by CIO traders in this case to be around US$400 million, a not insubstantial loss for a division that had been profitable throughout its short life (PSI 2013). Furthermore, executing the reductions in the SCP over time also created risks in that the portfolio was subject to substantial losses if traders were caught with temporarily unhedged positions as they were unwinding the portfolio. This actually occurred in January 2012 with the bankruptcy of Eastman Kodak, which cost the bank some US$50 million (PSI 2013). Caught between a rock (closing out their positions) and a hard place (potential losses), the CIO traders developed a complex strategy to manage the risk reduction over a long period of time by not only selling down positions but also buying hedges against the risks that remained. Unfortunately this strategy, which was ill-understood but nonetheless sanctioned by CIO management, created more risk than it hedged. In practice, CIO
traders had to purchase massive amounts of securities to hedge the remaining risk. These purchases became known as the “London whale trades” because of their sheer size (PSI 2013; JPMorgan 2013; CFTC 2013).

Before the whale case, JPMorgan had an enviable reputation in the industry as a good risk manager (PSI 2013), and had put in place state-of-the-art risk management processes and systems, in particular management of trading risk using so-called value-at-risk (VaR) models and limits. However, the CIO traders firmly believed that the bank’s standard VaR model overstated the risks they were taking in the SCP by under-estimating the “correlations” between its components. CIO traders and management aggressively petitioned the firm’s risk management function to approve a new VaR model that supposedly modeled the risks better (JPMorgan 2013; PSI 2013). Unfortunately, the new model did indeed reduce the VaR estimate but, as was discovered after a few months, it was doing so incorrectly. By the time of that discovery, however, the CIO had taken on massive risks, through the whale trades, which, by staying within their division’s VaR limits, were flying below the bank’s risk management radar (PSI 2013). Desperate to escape detection until the risks could be reduced, the CIO traders and management began to understate the risks by “marking to market” the portfolio with optimistic rather than realistic prices.

By the time the extent of the risks in the failed strategy was discovered in May 2012, the expected losses had risen to some US$6 billion (PSI 2013). The usual firing of the culprits and resignations of key managers followed and the bank and its regulators began their investigations into the failures of risk management that permitted, first, the complex and ultimately disastrous strategy to proceed and, second, the spectacular failure of supposedly world-class risk management and model development processes.

The internal task force into the events leading up to losses concluded that the problems were due, in large part, to deficiencies in risk management in the bank, in particular the CIO, as identified by the CEO:

CIO, particularly the Synthetic Credit Portfolio, should have gotten more scrutiny from both senior management, and I include myself in that, and the firm-wide Risk control function.... Make sure that people on risk committees are always asking questions, sharing information, and that you have very, very granular limits when you're taking risk.... In the rest of the company we have those disciplines in place. We didn’t have it here.

... These were egregious mistakes. They were self-inflicted, we were accountable and what happened violates our own standards and principles by how we want to operate the company. This is not how we want to run a business. [Emphasis added.]

JPMorgan (2013)
The PSI report to the US Congress on the losses agreed with the firm’s own assessment:

The Subcommittee’s investigation has determined that, over the course of the first quarter of 2012, JPMorgan Chase’s Chief Investment Office used its synthetic credit portfolio (SCP) to engage in high risk derivatives trading; mismarked the SCP book to hide hundreds of millions of dollars of losses; disregarded multiple internal indicators of increasing risk; manipulated models; dodged OCC oversight; and misinformed investors, regulators, and the public about the nature of its risky derivatives trading.  

[Emphasis added.]

Employing an analysis framework developed by Turner (1976), this paper identifies some of the warning signs of the impending disaster that were ignored by JPMorgan’s management. Similarities with other cases of operational risk disasters are highlighted and deficiencies in management controls are identified. Before doing so, however, some of the key trading organizations, trading strategies and processes are described.

1.2 Chief Investment Office

Set up in 2005, the CIO is part of JPMorgan’s central corporate/private equity division. On the face of it, the mandate of the CIO was simple, “to manage the bank’s excess deposits” (PSI 2013), mainly the cash difference between money placed with the bank by depositors (and retained for liquidity purposes) and money loaned to customers. For a bank the size of JPMorgan, this excess is not insubstantial, of the order of US$350 billion in 2012 (PSI 2013). While many banks invest these excess funds in relatively risk-free investments, such as government securities, JPMorgan attempted to be more proactive in investing a portion of these reserves in high-return securities and were successful in doing so for a number of years. For example, while income from CIO was not split out from the rest of the corporate division in annual reports, it was reported that the profit from just one position in the synthetic credit portfolio (SCP) was of the order of US$400 million as a result of American Airlines declaring bankruptcy in late 2011 (PSI 2013). It was in this SCP portfolio that substantial losses were to occur in the first quarter of 2012.

By 2011, the CIO was headed up by an experienced executive, Ina Drew, and operated out of several locations, in particular New York and London, employing a staff of over 400, including 140 traders (PSI 2013).

1.3 Synthetic credit portfolio

In 2006, the CIO were given permission to trade in so-called synthetic credit derivatives, such as credit default swaps (CDSs) and “indexes” based on those derivatives (PSI 2013). A CDS is a “derivative” that is traded “over the counter” (OTC), ie, directly...
between two parties, and is effectively a bet on the creditworthiness of the “underlying” firm, for example, IBM or Boeing. In a CDS transaction, one party will, for upfront and usually periodic fees, “buy protection” against a downgrade or default of the underlying firm. If the underlying firm were to default, the other party, the seller of the protection, would have to reimburse the buyer any income due from the underlying firm under the swap, operating in much the same way as a “financial option” (Crouhy et al 2006).

A credit index is an artificial/synthetic derivative security that consists of a pre-defined mix of CDSs (or similar derivatives). The concept is analogous to stock market indexes such as the S&P 500, which consists of a “basket” of shares on the New York Stock Exchange (NYSE) or NASDAQ, the composition of the basket being dependent on the market capitalization of the firms involved. Just as an investor can trade in futures and options on the S&P 500 index and the underlying shares, investors in a credit index can invest in the index and its constituents. As noted above, however, trading of credit indexes is not done on an exchange but OTC, directly between parties. In such trades, the buyer is said to be “short risk” on the index while the seller is “long risk” (PSI 2013).

From 2007 until the end of 2011, the size of the SCP portfolio managed by CIO grew by a factor of over 12 from some US$4 billion to over US$50 billion of notional value1 of these structured credit products. (PSI 2013). And in growing, the SCP had been profitable in each of those years. The head trader for the SCP was Bruno Iksil, who operated out of the London office, reporting to the Head of Credit and Equity Trading, Javier Martin-Artajo, who reported to the International Chief Investment Officer, Achilles Macris, who in turn reported to Ina Drew in New York. Although this chain of command appears to be long, in practice these executives were – as illustrated by the communications published by the PSI – in constant contact with each other by email and telephone. These managers and traders were not neophytes but highly experienced trading professionals, whose expertise was rewarded with annual remuneration higher than comparable senior positions in the JPMorgan Investment Bank (PSI 2013, Exhibit 1h).

1.4 Credit indexes

The Markit Group Ltd, a global financial information provider, dominates the market for “credit indexes”, creating and administering multiple indexes, in much the same way that Standard & Poor’s (S&P) dominates the market for administering stock market indexes (Markit 2013). The company have, through acquisition, become the

---

1 It should be noted that the “notional” amount of a derivatives trade refers to the “face” or paper value of the underlying securities not the “current market” value of the trade, which is usually much less.
administrators of two main families of credit index: CDX, which is a family covering North American firms; and iTraxx, which covers international firms. As part of its administration of these indexes, Markit calculates index values and publishes daily index prices on its website (PSI 2013). In addition to these indexes, Markit have also created so-called credit index tranches, which allow investors to invest in particular subsets of an index, such as a so-called equity tranche, which will suffer losses immediately if any firm in the basket were to default (PSI 2013).

The concept is best explained by an example such as the IG9 index (IG9 2007), which was heavily traded by the CIO (PSI 2013). The IG9 index, part of the CDX family, consists of 125 investment-grade (IG) US firms with equal weighting (ie, each makes up 0.8% of the index); these companies are considered unlikely to fail.2 Issued in 2007, IG9 was the ninth issue of the Markit IG series and could be traded, by parties entering a swap agreement referencing IG9, in various maturities, eg, IG9 10-year would be a swap that matured in 2017, ie, ten years after IG9 was created. A trader who is "long" IG9 is betting that the index will rise over the period, receiving income from the seller, but if a credit event was to occur, such as if one of the constituent firms were to default, the “long” party would have to make up the shortfall to the “short” party. It should be noted that not all indexes are based on investment-grade companies, but there was an active market in CDS and indexes in high yield (HY) or less credit worthy firms (PSI 2013). At the end of 2011, buyers of protection were banks, such as JPMorgan, that were hedging against a downturn in the US economy. On the other hand, sellers tended to be hedge funds speculating on the default of specific firms.

As would be expected from a portfolio that was supposedly acting as a hedge against companies defaulting in an economic downturn, the SCP was predominantly “short risk” on HY indexes and tranches at the end of 2011, but also had some hedging (ie, “long risk”) positions in IG indexes (PSI 2013). However, the management of the bank and CIO felt that the US economy was improving and that the SCP could naturally move to a “risk neutral position [and] that macro credit protection was therefore less necessary” (PSI 2013).

Before describing the events of 2012 that led to JPMorgan’s losses, it is worth noting here that estimating the risk of default in a portfolio of CDS, credit indexes and credit index tranches, is a very complex undertaking not least because the same underlying firm could be represented in multiple CDS, multiple indexes and tranches in varying mixes and different levels of risk, eg, equity/nonequity tranches. In addition, there is a degree of correlation between firms in an index that is difficult to estimate; for

---

2 It should be noted that despite the fact that the constituents were investment grade, at the time of the whale case, there were only 121 firms in the IG9 index, as a number of large firms, such as Washington Mutual, had defaulted during the global financial crisis (GFC).
example, the creditworthiness of automobile companies will tend to rise and fall, if not in lockstep, then in roughly the same direction.

1.5 Market risk management at JPMorgan

JPMorgan popularized the concept of VaR for managing the “market risk” in portfolios of cash and derivative instruments (Jorion 2006). JPMorgan described the VaR of a portfolio as representing “an estimate of the maximum expected mark-to-market loss over a specified time period, generally one day, at a stated confidence level, assuming historical market conditions” (JPMorgan 2013). This definition is widely used in the industry and also for regulatory purposes, with, for example, Basel II regulations requiring a so-called ten-day holding period, rather than one day, for the purposes of calculating market related risk weighted assets (RWAs) for regulatory capital purposes (Basel Committee on Banking Supervision 2004, Paragraph 718).

Although the concept of VaR has been criticized as being insufficient for managing risks in complex portfolios, not least because it is not a “coherent measure” of risk (Artzner et al 1999), it nonetheless remains a widely used “risk metric” for management purposes (Jorion 2006). Despite its pitfalls, such as its difficulty in handling extreme events (Taleb 2007), VaR, as part of a robust risk management framework, does have the advantage that the results are intuitive and easy to explain to non-technical executives. To paraphrase the words of the famous statistician E. P. Box, the VaR model is wrong but nonetheless is useful (Box et al 1987).

However, to be useful in managing risk, it has long been recognized that VaR had to be embedded within a framework that comprises comprehensive and robust processes for: data collection; VaR model development; VaR limit setting and monitoring; proactive management of limit excesses; independent price validation; “backtesting” of models; stress testing; independent model review, and independent auditing of all of these processes (Federal Reserve 2011). A breakdown of any of these processes can lead to significant losses, as shown in the AIB and NAB cases (McConnell 2003, 2005). And, as in those cases, the bulk of the losses incurred were a result of deficient market risk management, eg, taking risky positions, but the breakdown of the control processes were failures of operational risk management.

The process of estimating VaR for any portfolio involves breaking down each unique “trading position” in the portfolio into its component “risk factors” and then computing the potential losses at a predetermined confidence interval (eg, 99.9%) for each factor, from consideration of the price and volatility history of each factor. The contribution of each risk factor in each position is aggregated using relatively simple formulas that stem from the Nobel-winning work of Harry Markowitz on modern portfolio theory (Markowitz 1971). The aggregate value is then reduced by formulas
that recognized the “correlations” between risk factors; for example, not all stocks will react in exactly the same way to an announcement of a base interest rate change.

This paper is not the place to describe the intricacies of various approaches to calculating VaR (such as variance–covariance or Monte Carlo simulation) and their respective benefits and disadvantages as these are adequately covered by, among others, Jorion (2006) and Crouhy et al (2006). However, it should be noted that these approaches are very well-developed and well-understood and it is possible to purchase off-the-shelf software packages that can be tailored relatively easily to a specific portfolio, provided that it consists of trading positions which are based on risk factors that have a “rich” history of prices and stable market behaviors. Beyond that, portfolios that are based on risk factors that do not have such a long price history in heavily traded markets, such as the SCP, become more problematic to assess using VaR techniques. If a difficulty in assessing VaR is combined with breakdowns in market risk management processes, the potential for significant losses can arise.

As noted above, one of the key reasons for large banks to develop market risk management models, such as those based on VaR, is to satisfy the requirement of the so-called Basel II regulations (Basel Committee on Banking Supervision 2004) which requires banks to set aside capital to cover, inter alia, the RWAs attributable to a firm’s market positions. Basel II permits the use of a so-called internal model based on VaR which “will be conditional upon the explicit approval of the bank’s supervisory authority” (Basel Committee on Banking Supervision 2004, Paragraph 718). JPMorgan had such approval for its internal “Basel I model” from its primary regulator, the Office of the Comptroller of the Currency (OCC) (JPMorgan 2013; PSI 2013). To use such a model, regulators require a comprehensive set of so-called quantitative standards which include “external validation” of the model(s) used and “stress testing”, in addition to “qualitative standards” such as creation of an independent risk management organization (Basel Committee on Banking Supervision 2004).

At this point it should be noted that JPMorgan, as the originator and promoter of value-at-risk, has had an enviable record in market risk management, putting in place a comprehensive and heretofore robust market risk management framework. In particular, the bank had a created an independent function called Model Risk and Development, reporting to the firm’s Chief Risk Officer (CRO), who is responsible for validating all important models in the firm, in particular VaR models. The firm also had a process for setting and monitoring VaR limits across the firm and independent auditing of those processes. On the face of it, and certainly for most of the firm, in particular the JPMorgan Investment Banking division, which incurred most market risk, these processes did, and still do, appear to work well. That these well-established processes broke down in the CIO is the subject of Section 4. As the internal report into the so-called whale losses concluded, the blame for the breakdown was widespread:
The firm did not ensure that the controls and oversight of CIO evolved commensurately with the increased complexity and risks of CIO’s activities. As a result, significant risk management weaknesses developed within CIO that allowed the traders to pursue their flawed and risky trading strategies. On this point, the task force has concluded that senior firm management’s view of CIO had not evolved to reflect the increasingly complex and risky strategies CIO was pursuing in the Synthetic Credit Portfolio; instead, they continued to view CIO as the manager of a stable, high-quality, fixed-income portfolio. [Emphasis added.]

JPMorgan (2013)

In other words, management did not adjust their approach to managing the risks in the SCP until it was too late, because they did not completely understand the complexity of the risks being taken. This has echoes in other rogue trading cases, such as AIB, NAB and Société Générale, where management considered the particular businesses to be low-risk.

2 ANALYSIS OF DISASTERS

2.1 Turner’s framework for disasters

In an often-cited work in decision literature, Turner (1976) examined the official reports of a number of “disasters” from an organizational perspective. The disasters analyzed by Turner resulted in considerable loss of life and so cannot be compared to the failures of management that occurred at financial institutions. However, Turner considered that discussion of such disasters offers “a paradigm for discussion of less tragic but equally important organizational and inter-organizational failures of foresight”, such as significant financial losses at a major public company. Turner identified a number of “stages” in the “development of a disaster” and “features” that appear to be common to them, which are summarized in Table 1 on the next page.

Turner’s framework proves a useful tool for analyzing the whale case (and others) because, as with the disasters that Turner studied, a number of official inquiries were conducted into the events leading up to the losses, the results of which were published by JPMorgan and its regulators.

In his framework, Turner concentrates on the stages of “initial beliefs” and “incubation period” because he argued that it was before the “onset” of disasters that the significant organizational failures tended to occur. In an observation that is important for banking regulators and management, Turner pointed out that:

Disasters, other than those arising from natural forces, are not created overnight. It is rare that an individual, by virtue of a single error, can create a disastrous outcome in an area believed to be relatively secure. To achieve such a transformation he or she needs the unwitting assistance offered by access to the resources … of large organisations, and time.

Turner (1976)
TABLE 1  Common features in the development of a disaster.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Features common to disasters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Initial beliefs and norms</td>
<td>Failure to comply with existing regulations</td>
</tr>
<tr>
<td>Culturally accepted beliefs and precautionary norms and procedures</td>
<td></td>
</tr>
<tr>
<td>2. Incubation period</td>
<td>(a) Rigidities of belief</td>
</tr>
<tr>
<td>The accumulation of an unnoticed set of events which are at odds with the accepted beliefs</td>
<td>(b) Decoy phenomena</td>
</tr>
<tr>
<td>(c) Disregard for complaints from outsiders</td>
<td>(d) Information difficulties and noise</td>
</tr>
<tr>
<td>(e) The involvement of strangers</td>
<td>(f) Failure to comply with discredited or out-of-date regulations</td>
</tr>
<tr>
<td>(g) Minimizing emergent danger</td>
<td></td>
</tr>
<tr>
<td>3. Precipitating event</td>
<td>The event that brings the issue to public attention</td>
</tr>
<tr>
<td>4. Onset</td>
<td>The immediate consequences of the collapse of “cultural precautions” becomes apparent</td>
</tr>
<tr>
<td>5. Rescue and salvage</td>
<td>The immediate post collapse situation when rescue attempts begin</td>
</tr>
<tr>
<td>6. Full cultural adjustment</td>
<td>The establishment of a new level of precautions</td>
</tr>
<tr>
<td>An inquiry is carried out and beliefs are adjusted</td>
<td></td>
</tr>
</tbody>
</table>

Source: Turner (1976, Tables 1 and 2, pp. 381, 391).

As it transpired, JPMorgan was one of those “large organizations” that had the resources to create an organizational disaster.

2.2 Financial disasters

There have been a number of well-publicized “financial disasters” that have been attributed to deficient operational risk management, in particular the losses due to
“rogue traders” which caused the collapse of Barings bank and significant losses at National Australia Bank (NAB), as documented by Board of Banking Supervision (1995), Crouhy et al (2006) and APRA (2004). McConnell (2003, 2010) also described losses due to rogue trading at Allied Irish Bank (AIB) and ANZ Bank in terms of the Turner framework.

In January 2008, Société Générale SA, France’s second-biggest bank, announced that a relatively junior trader, Jerome Kerviel, had lost €4.9 billion (US$7.4 billion) by taking positions on European stock market indexes and then falsifying documents and emails to pretend the bets were hedged (Economist 2008). Kerviel was initially arrested claiming, and continuing to claim even after conviction, that the bank was aware of his actions and hence had condoned them. Under pressure from the French financial regulator, the Banking Commission of the Banque de France, Société Générale set up a formal inquiry to investigate the events leading up to the losses (SOCGEN 2008). While the inquiry continued to refer to the events as a “fraud”, the report gives details of a litany of failed opportunities to detect the trading anomalies over a prolonged period of time, many attributable to the fact that, while control staff did raise issues with the trader and his superiors, they did not follow up on answers/excuses that were given for the “red flags” being raised. The conclusion was that the procedures in place were sufficient to indicate the possibility of a problem but the risk management processes failed to bring it to management’s attention.

In September 2011, UBS AG, the large Swiss bank, announced that it had discovered a significant loss, of around US$2.3 billion due to unauthorized trading by a trader, Kweku Adoboli, on the exchange-traded funds (ETF) desk in its investment banking division in London (FINMA 2012). In November 2012, Adoboli was found guilty of “fraud by abuse of position” and sentenced to seven years, half of which was to be served in jail (Keith 2012). The judge in the trial gave an excellent summary of what had happened when sentencing Adoboli:

In the last few months before your arrest, you amassed huge positions when trading on behalf of the bank, well beyond your risk limits, and you did not protect the bank from the risk of loss by hedging your trades. I accept that you started to do that in order to maximise the profits which the bank would make from your trading, and the effect which being regarded as a star trader would have on your bonus and your prospects for advancement within the bank was a secondary consideration only. Nor do I doubt that you were persuaded, despite your view that the market would fall, to trade on the basis that the market would rally. But the fact is that the market did fall. Your unhedged trading well beyond your risk limits resulted in the bank being exposed to the risk of enormous losses – at one stage to the risk of losses amounting to an unbelievable $11.8bn. And you then took larger and larger positions in a desperate attempt to recoup those losses. Throughout all that, you concealed what you were doing by booking fictitious hedging trades to give the back office the impression that your
trades were hedged when they were not. Once your positions had been unwound, the actual losses which your trading caused still came to a colossal $2.25bn. [Emphasis added.]

Keith (2012)

Concurrent with the trial, the UK and Swiss regulators undertook a joint investigation which resulted in a fine of £29.7 million by the UK Financial Services Authority (FSA), and the Swiss regulator, FINMA, also “imposed until further notice a range of preventive supervisory measures, designed to limit the operational risk exposure of UBS until able to give evidence that the operational control environment of its Investment Bank is working effectively” (FINMA 2012; FSA 2012). Both regulators identified serious failings in the bank’s risk management and control environment (FINMA 2012) and failure to manage limit breaches (FSA 2012) and poor supervision by senior executives (FINMA 2012).

However, precisely the same reasons were proffered in other cases of large-scale and well-publicized losses due to fraudulent trading, such as Barings, Allied Irish Bank, and National Australia Bank, Société Générale and UBS. So, given the wide publicity given to these other losses, there is no real excuse for the control failures that occurred at JPMorgan in the whale case. In its report into the NAB failure, the Australian Prudential Regulation Authority (APRA) highlights the importance of in-depth analysis of organizational disasters, “the wisdom of hindsight provides a valuable platform from which to learn lessons for the future” (APRA 2004). The analysis in this paper attempts to contribute to an understanding of the events at JPMorgan that caused a loss of over US$6 billion using Turner’s framework.

3 JPMorgan: DEVELOPMENT OF A DISASTER

3.1 Initial beliefs and norms

Turner (1976) argues that a disaster or “cultural collapse” takes place because of “some inaccuracy or inadequacy in the accepted norms and beliefs” of a firm. Organizational disasters build up gradually over time and the signs should be apparent to management. Instead, the warning signs go unnoticed or ignored because of “cultural rigidity” which manifests itself in erroneous assumptions and reluctance to face unpalatable outcomes (Turner 1976).

Until 2011, the SCP was only a small part of the overall portfolio of CIO’s investment securities – some US$50 billion out of US$350 billion overall. In turn, CIO’s positions paled into insignificance compared with the bank’s overall assets of some US$2.3 trillion. SCP was considered fairly small beer. In fact, SCP was deemed so insignificant that it was not reported as a separate line item within CIO in income or risk reports to the firm’s banking regulator, the OCC (PSI 2013). And it was not until
May 2012, when losses were mounting, that separate figures were reported, and the losses in those reports shocked the regulators.

In her testimony to the PSI, the head of CIO and previously head of the bank’s Treasury function, Ina Drew, was proud of the fact that CIO managed a very diversified portfolio, including the US$13 billion employee retirement plan, “engaged in all of these activities as part of what we viewed as prudent and normal-course asset-liability management for a large financial institution such as JPMorgan Chase” (PSI 2013). She was also proud that the CIO function had helped to keep JPMorgan afloat during the GFC, contributing “about $23 billion to the company’s earnings from 2007 through 2011, helping to offset business losses incurred during that difficult period of time” (PSI 2013). The PSI (2013) also noted that “as CEO, Jamie Dimon developed a reputation as a ‘risk-averse manager who demands regular and exhaustive reviews of every corner of the bank’” and that “during the financial crisis, government officials, investors, and depositors alike viewed JPMorgan Chase as a safe harbor in the storm” (PSI 2013).

And it was not only the CIO management that had a high opinion of their capabilities. Even after the first sets of losses were reported to the bank’s regulator, the OCC, and derided by the CEO as a “tempest in a teapot”, the head of the regulatory group in the OCC was prepared to be somewhat forgiving, because JPMorgan, unlike other banks, had, after all, survived the GFC, and “at end of day they are good at financial risk mngt [sic]. But they are human and will make mistakes (big loan losses, trading losses, litigation, etc.).” (PSI 2013).

The original rationale for the SCP was not as a proprietary trading desk but as management claimed “as insurance or a “hedge” against credit risks confronting the bank” and many inside the bank, such as the CFO, continued to consider it to be so even as losses mounted (PSI 2013). Sometime between 2007 and 2012, the SCP had, in the words of the CEO, “morphed into something that, rather than protect the firm, created new and potentially larger risks” or in the words of an OCC examiner a “make-believe voodoo magic ‘composite hedge’” (PSI 2013).

As was evident in other cases of significant losses, such as NAB and Société Générale, the business area that created the losses, here CIO, was considered relatively minor in the grand scheme of things and was considered to be managed well by top-class executives. This was not necessarily complacency but more a belief that there was a robust and proven risk management framework in place that would pick up any problems before they grew too big. However, the internal task force that investigated the losses at JPMorgan observed that

Senior firm management’s view of CIO had not evolved to reflect the increasingly complex and risky strategies CIO was pursuing in the Synthetic Credit Portfolio; instead, they continued to view CIO as the manager of a stable, high-quality, fixed-income portfolio. As a result, they were less focused on CIO relative to client-facing...
businesses, and did not do enough to verify that CIO was well managed or that the firm was fully applying its various risk and other controls to the Synthetic Credit Portfolio’s activities. [Emphasis added.]

JPMorgan (2013)

Consistent with its perception as a low-risk hedging operation, the CIO division did not have a full-time, dedicated CRO until 2012, when a new CRO was appointed just as the whale crisis was emerging and while the CRO was still “learning the ropes” (PSI 2013). The CIO’s own divisional risk committee had a low profile, meeting only three times in 2011, and then not until late March 2012, when losses were beginning to rise. Consisting of internal CIO staff, the division’s risk committee did not have a formal charter and the JPMorgan task force noted that “had there been senior traders or risk managers from outside CIO or had the CIO Risk Committee met more often, the process might have been used to more pointedly vet the traders’ strategies in the first quarter of 2012” (PSI 2013).

But even if the risk committee had been more proactive, there is little evidence that it would have made the difference suggested by the task force as the responsibilities of the CIO risk managers were ill-defined and constrained. The head of market risk for CIO told the PSI that his “role as a risk manager was descriptive, rather than prescriptive … [acting] as a ‘middleman’ who ‘coordinated’ between the risk modelers and the traders and managers to ensure that the risk metrics were properly calculated and disseminated to decision makers” (PSI 2013). In particular, he said that he did not have the authority to enforce risk limits nor to “challenge trading strategies” (PSI 2013). In short, just as it became important to be proactive, risk management was low key and side lined.

3.2 The incubation period

Turner (1976) identified several “features” that he found were common to disasters from organizational rigidity to individual failure to appreciate danger. He argued that disasters tend to occur not as a result of some sudden event, but as a consequence of an accumulation of organizational and individual faults that cause a problem, which could have been contained, to grow into a catastrophe. Turner argues that “small scale disasters can be produced rapidly, but large scale disasters can only be produced if time and resources are devoted to them”. During the incubation period of a disaster, Turner points out that there is a steady accumulation of events that are at odds with the norms of the organization but go unnoticed because their importance is not fully appreciated. It is the gradual acceptance of such events that blinds management to potential problems.

As the focus of this paper relates to the incubation of the causes of the whale losses, discussion is postponed until the next section while the remaining stages in the Turner model are described in brief.
3.3 The onset

Turner identifies two distinct stages that bring a disaster to the public’s attention: the “precipitating event”, which grabs the attention of the public; and the “onset”, or immediate consequences of the event.

3.3.1 The precipitating event

On May 11, 2012, JPMorgan announced an investors’ conference call to discuss the recent filing of its first quarter income report to the Securities and Exchange Commission (SEC). This so-called 10-Q report (JPMorgan 2012a) contained the first public admission by the bank that there were problems in the CIO.

Since March 31, 2012, CIO has had significant mark-to-market losses in its synthetic credit portfolio, and this portfolio has proven to be riskier, more volatile and less effective as an economic hedge than the firm previously believed.

JPMorgan (2012a)

Although the admission was newsworthy, there had been rumors of problems with what had been termed the “London whale” for some weeks. In early April, financial news outlets had reported that CIO traders had been amassing trading positions that were so large they were driving price movements in the CDS market and that hedge funds were betting against these positions (Burne 2012). During a conference call to discuss JPMorgan’s first quarter earnings a few days later, the CEO was quizzed about, among other issues, the whale rumors and Dimon made a dismissive comment that was later to haunt him, “it’s a complete tempest in a teapot” (PSI 2013).

3.3.2 The onset

Despite the CEO’s somewhat off-hand characterization of the whale controversy, bells were beginning to ring very loudly inside CIO and JPMorgan in general. Exhibit 1i of the PSI report into the losses is a time line of events that shows that the SCP suffered losses of some US$169 million in January and February and an internal review estimated potential losses of some US$6.6 billion (PSI 2013, Exhibit 1i). By the end of March 2012, first quarter losses for the SCP had grown to US$719 million. By mid-April, SCP losses for the year-to-date had risen to some US$1.3 billion (PSI 2013, Exhibit 1i) and on April 12 the bank filed an 8-K (notification of material change) to the SEC but did not expand on the CIO problems (JPMorgan 2012b). In late April, JPMorgan management met with the bank’s regulator, OCC, to discuss VaR limit breaches but insisted that all would be well with the SCP. Just two weeks later, the bank informed the OCC of losses in the SCP of US$1.6 billion, although losses were estimated internally at that time to be over US$2.3 billion (PSI 2013, Exhibit 1i).
On May 10, 2012, JPMorgan filed its first quarter 10-Q report, disclosing losses for the quarter of almost US$800 million in CIO and for the first time disclosing problems with the SCP portfolio and its increased VaR (JPMorgan 2012a, Q1). During the investor call following the quarterly filing, the CEO disclosed additional losses of US$2 billion for the year-to-date and for the first time disclosed problems with the CIO’s VaR model (PSI 2013, Exhibit 1i).

Events moved quickly after the call. The bank set up an internal “management task force”, headed by a previous CFO, with the remit to answer three questions “what happened”, “how did it happen” and “where is the firm now?” (JPMorgan 2013). As is typical in such events, there was immediate and significant management upheaval. All of the CIO management hierarchy from head trader, Bruno Iksil, upward were fired or, as in the case of Ina Drew, resigned. Other employees were fired or resigned in the aftermath, including Julien Grout, a trader in the SCP group (PSI 2013).

In September 2012, the Permanent Subcommittee on Investigations in the US Senate initiated a formal investigation into the Whale losses, which, over a period of nine months, interrogated many of the key players and in March 2013 produced a comprehensive report running to over 900 pages of commentary and exhibits, including many internal emails and reports from the bank (PSI 2013). This congressional report and that of the JPMorgan task force, released in January 2013, are used for the details in this paper, as recommended by Turner (1976).

3.4 After the event

Turner (1976) identifies two final stages that are common in an organizational disaster. In the immediate aftermath there is the “rescue and salvage” of anything of value left from the disaster and finally there is a “cultural adjustment”, which attempts to learn lessons from the unhappy events. Again, these stages were apparent in the Whale case.

3.4.1 Rescue and salvage

The task force report was not a whitewash but concluded that “responsibility for the flaws that allowed the losses to occur lies primarily with CIO management but also with senior firm management [original emphasis]” (JPMorgan 2013). The report also concluded that certain senior executives were directly responsible.

(1) Head of CIO, Ina Drew, for multiple failures in ensuring the CIO trading strategies were understood and controlled

(2) Head of firm-wide risk, Barry Zubrow, for failures of the CIO risk organization, in particular “the CIO Risk organization was not equipped to properly risk-manage the portfolio during the first quarter of 2012, and it performed...
ineffectively as the portfolio grew in size, complexity and riskiness during that period [emphasis added].

(3) The CFO, Douglas Braunstein, for weaknesses in financial controls, in particular the “CIO finance organization’s failure to have asked more questions or to have sought additional information about the evolution of the portfolio during the first quarter of 2012 [emphasis added]” (JPMorgan 2013).

The JPMorgan task force also criticized the bank’s CEO, Jamie Dimon, for relying too heavily on divisional management and not recognizing deficiencies in the CIO organization sooner but acknowledged his prompt actions when the crisis became evident (JPMorgan 2013). The task force made a sizeable number of key observations on the causes of the losses, in particular:

(1) The trading strategies that were designed in an effort to achieve the various priorities were poorly conceived and not fully understood by CIO management and other CIO personnel who might have been in a position to manage the risks of the Synthetic Credit Portfolio effectively.

(2) CIO personnel at all levels failed to adequately respond to and escalate (including to senior firm management and the Board) concerns that were raised at various points during the trading.

(3) Certain of the traders did not show the full extent of the Synthetic Credit Portfolio’s losses.

(4) CIO provided to senior firm management excessively optimistic and inadequately analyzed estimates of the Synthetic Credit Portfolio’s future performance.

(5) CIO Risk Management lacked the personnel and structure necessary to manage the risks of the Synthetic Credit Portfolio.

(6) The CIO Risk function had been historically understaffed, and some of the CIO risk personnel lacked the requisite skills.

(7) The CIO Risk Committee met only infrequently, and its regular attendees did not include personnel from outside CIO. As a result, the CIO Risk Committee did not effectively perform its intended role as a forum for constructive challenge of practices, strategies and controls.

(8) Furthermore, at least some CIO risk managers did not consider themselves sufficiently independent from CIO’s business operations and did not feel empowered to ask hard questions, criticize trading strategies or escalate their concerns in an effective manner to firm-wide Risk Management.

(9) The risk limits applicable to CIO were not sufficiently granular. The absence of granular limits played a role in allowing the flawed trading strategies to proceed in the first quarter, especially as the positions grew in size.
Approval and implementation of the new CIO VaR model for the Synthetic Credit Portfolio in late January 2012 were flawed, and the model as implemented understated the risks presented by the trades in the first quarter of 2012. [Emphasis added.] JPMorgan (2013)

It should be noted that many of these criticisms are the same as those identified by other official inquiries into significant trading losses, such as NAB (APRA 2004), AIB (Ludwig 2002), Société Générale (SOCGEN 2008) and UBS (FINMA 2012).

Following the PSI investigation, the Commodity Futures Trading Commission (CFTC), charged JPMorgan under the new Dodd–Frank legislation with “manipulative conduct”, in particular “employing a manipulative device in connection with the Bank’s trading of certain credit default swaps” (CFTC 2013). Under Basel II regulations, such a regulatory fine can be mapped directly onto the Basel II Operational Risk Loss Event Type classification in the category of “Clients, Products and Business Practices”, in particular “Market Manipulation” in the level 2 category “Improper Business or Market Practices” (Basel Committee on Banking Supervision 2004, Annex 7).

At the time of writing, the US Department of Justice (DOJ) has charged two CIO employees, Javier Martin-Artajo and Julian Grout, with falsifying financial records, which relates to the mispricing of SCP positions to disguise losses, which allegedly took place in March and April 2012 (SEC 2013). Prior to those charges, the DOJ entered into a nonprosecution agreement with the CIO head trader, Bruno Iksil, in return for cooperation (DOJ 2013). To date these, relatively minor, charges are the only prosecutions in the whale case.

3.4.2 Cultural adjustment

Turner (1976) points out that, after the dust settles, it is possible to carry out a “more leisurely and less superficial assessment” of the events leading up to a disaster, with the goal of learning lessons from it and ultimately closing the circle by adjusting the erroneous beliefs and norms that lead to the failure. In its report into the NAB affair, the Australian regulator, APRA, is in strong agreement with Turner’s viewpoint:

APRA believes that cultural change must be driven from the top … the cultural issues thrown up need to be treated with the same attention and seriousness. [Emphasis added.] APRA (2004)

The task force recommended a number of “remedial measures”, including

(1) appointing a “new, experienced CIO leadership team”,

(2) substantially reducing “the 2012 incentive compensation for a number of employees and … also reducing the 2012 incentive compensation pool for all of CIO”.

Journal of Operational Risk 9(2)
(3) introducing new governance measures to integrate CIO with the rest of the bank, in particular JPMIB,

(4) overhauling the risk organization in CIO, in particular its reporting lines directly to the firm’s Chief Risk Officer,

(5) implementing new more granular risk limits for CIO, and

(6) undertaking a “comprehensive self-assessment of the entire risk organization [including] working to improve model development, review, approval, and monitoring” (JPMorgan 2013).

As these “cultural adjustments” (Turner 1976) were only instituted some months before this paper was written it is not possible to determine whether the “remedial measures” have as yet worked.

Beyond JPMorgan’s cultural adjustments, the industry is also changing. In December 2013, all of the five US banking regulators, including JPMorgan’s regulators, the OCC and Federal Reserve, agreed the “Final Rules to implement the ‘Volker Rule’”, which, inter alia, prohibits proprietary trading by the regulated banks (OCC et al 2013). While the so-called Volker Rule was proposed as part of the Dodd–Frank legislation following the GFC (Dodd–Frank 2010), and permits market-making and hedging activity, the emergence of the whale scandal contributed to specific tightening in the area of documentation of hedging activity, which was aimed at controlling trading in functions such as the CIO and improving monitoring of risk limits (OCC et al 2013). The rules also formalize existing and introduce new measures of market risk and more intrusive limit monitoring (OCC et al 2013). Again it is too early to identify the changes to banking culture that will arise from these new regulations, but it is already obvious that more intrusive risk management is likely in future.

4 THE CAUSES OF THE WHALE LOSSES

4.1 The incubation period

As noted above, Turner (1976) considered the “incubation period” to be important when analyzing disasters as it is actions prior to the “onset of the event” that ultimately determine the scale of the organizational disaster. During the incubation period of a disaster, Turner (1976) points out that there is a steady accumulation of events that are at odds with the norms of the organization but go unnoticed because their importance is not fully appreciated. Turner identifies the “incubation period” as the stage where the “failures of foresight” that lead to the eventual disaster occur and he describes a number of key features, summarized in Table 1 on page 68, that are common to the disasters that he studied. These features are discussed below in the context of the whale case.
Notwithstanding the long build-up to organizational disasters, one of the common features of “rogue trading” cases, such as Barings, AIB, NAB, Société Générale and UBS, is that, once problems arise, events spiral out of control very quickly and attempts to rectify the situation fail to reverse it. At that point, the rogue trader(s) often try to mask the losses in the hope that they can fix the problem. In cases such as Barings and NAB, the initial problems were caused by external events outside of the control of the traders, such as the Kobe earthquake in the case of Barings (Blunden and Thirwell 2010), or the change in interest rates following the G7 meeting in September 2003 in the case of NAB (APRA 2004).

In the whale case, however, the problems were wholly home-made, and not caused directly by external factors. For CIO, 2011 was a very good year, with increased profits and a growing but controlled portfolio of securities totalling some US$57 billion (JPMorgan 2013). At the end of 2011, the senior management of the bank decided to reduce its overall RWAs in order to increase their regulatory capital in anticipation of anticipated new regulations, colloquially known as Basel III (Basel Committee on Banking Supervision 2010). Like other businesses, CIO were asked to reduce their RWAs and hence their risks and regulatory capital (JPMorgan 2013).

In trading, there are two major methods of reducing market risks in a portfolio of securities: (a) sell down all or part of the portfolio; and/or (b) buy securities that “hedge”, ie, offset the risk, of the remaining portion of the portfolio. For example, to reduce risk in a share portfolio, an investor can sell shares or alternatively can buy options that protect against a fall in share prices. In what turned out to be, with hindsight, a disastrous strategy, the CIO traders decided to take the second approach and went on a massive spree of selling protection to offset the “short risks” in the SCP at that time. These were the so-called London whale trades (JPMorgan 2013).

However, this decision was not taken lightly in CIO as the risks were obvious, but the traders were faced with what were, in retrospect, three conflicting priorities:

1. reduce RWAs by reducing the SCP’s VaR;
2. minimize the losses in doing so; and
3. minimize the potential losses due to company defaults while doing so.

The PSI reports the suggestion by the head trader, Bruno Iksil, to his superior that they should just “take the pain fast” and “let it go” (PSI 2013) but CIO management were reluctant to do so. For example, Drew asked the traders “to see if it was possible to reduce RWAs without holding a ‘fire sale’” (PSI 2013). In January 2012, the risks of unwinding the SCP became evident, when as a result of unwinding some short positions but not matching with long positions, the SCP suffered a loss of some US$40 million when Eastman Kodak defaulted (PSI 2013). In addition, a general
strengthening of the US economy at the start of 2012 was making the SCP short positions lose money. Something had to be done.

In January 2012, the CIO traders and managers developed a number of strategic options/scenarios for reducing RWAs, all of which would produce a sizeable loss, some more than others. At that point it was recognized that one of the major contributors to reducing the RWAs could be to use a new VaR model, which, unlike the standard model, “properly” recognized the correlations in the SCP. In fact, it was estimated that the new model could on its own reduce the RWAs by potentially up to 50% (PSI 2013), leaving the traders to work out the remainder. The traders suggested that the remainder of the RWAs could be removed by “opportunistic risk reduction”, which meant that “risk could be reduced in a way that minimized execution costs, and that the risk reduction did not have to be completed quickly, but could occur over time” (PSI 2013). This was also characterized by a senior CIO executive as making “the trades that make sense” (PSI 2013).

This mixed scenario – new VaR model plus opportunistic trading – was the one that the CIO traders embarked upon from the end of January although there was no evidence that it was ever formally approved by CIO management. The new trading strategy was complex and, as the PSI noted, “the CIO traders were confronted with a series of complex objectives: to stem the losses in its credit portfolio, reduce the SCP’s RWAs, and maintain default protection to take advantage of any large corporate defaults” (PSI 2013). This was a difficult balancing act that, in practice, proved impossible to sustain. In executing the strategy, the CIO traders decided to reverse their natural market positioning and “go long”, ie, to sell rather than buy protection. The rationale for this change of tactics was that “going long” would collect premium income, so-called carry, which could be used to offset losses in the traditional short positions and to buy even more protection:

In short, the CIO traders began accumulating long credit derivatives – selling credit protection – in a mistaken effort to address all of the CIO’s problems at once: to offset losses by producing carry, reduce RWAs, add appreciating positions to the portfolio during the market rally, and allow the CIO to maintain default protection.

But the market was not letting the CIO keep all of these balls in the air at the same time. In practice, the premiums that CIO were collecting through selling protection did not keep up with the losses that were occurring in their short positions, and a vicious circle began of selling more and more protection – to effectively stay still. This mismatch in hedging was partially due to the fact that, because of the volumes of trading needed to close the gap, the CIO were having difficulty finding buyers at reasonable prices. Before long the sheer size of the CIO trading became obvious to the market, which consisted of only fourteen or so significant participants, and the whale
trades became newsworthy. In March 2012, the CIO accounted for 50% of trading in the IG9 index, all the time losing money on every trade (PSI 2013). By mid-March 2012, the SCP was losing money every day, with losses year-to-date totalling some US$500 million.

At this point, the CIO traders felt they had no option but to

“defend their positions” which meant going even more long in what the OCC called
“doubling down” on the SCP’s already losing trading strategy.

PSI (2013)

But the end was near and, on March 23, Drew ordered the traders to “put the phones down” and to stop trading (PSI 2013). The “going long” strategy had failed.

However, while putting the phones down would have stopped the positions from growing, it did not in fact stop the losses in the SCP portfolio, now grown to a massive US$157 billion or by a factor of 300% in just three months (PSI 2013). The now-frozen positions were losing money every day as the market moved against CIO and there was little that the traders could do to stem the flow of red ink (PSI 2013). On the day that the order to stop trading was given, March 23, the SCP experienced losses estimated to be between US$300 million and US$600 million (PSI 2013), but we might question why the range of estimates was so wide: 100%. It is, of course, a result of which “prices” were used to “mark to market” the portfolio. In this case, as a CIO trader explained in an email to managers, using the “best [ie, most advantageous] ‘bid–ask’ price would yield a loss of US$300 million on the portfolio, as against US$600 million ‘from the mids’ [ie, mid-points of the bid–ask spread]” (PSI 2013).

In financial markets, including credit derivatives, trades are normally quoted on a “bid–ask spread” where a buyer will pay the “bid” price and a seller will sell at the “ask”, the difference between bid and ask prices being the “spread”, which is a measure of the liquidity in the market, in that highly traded markets tend to have tighter bid–ask spreads. The “mid”, or mid-point, is the arithmetic mean of the bid and ask prices (Crouhy et al 2006). Generally accepted accounting principles (GAAP) require banks to value their trading positions each day using prices that are “most representative of fair value in the circumstances” (PSI 2013). While the “mid” of the latest “bid–ask spread” is most often used for this purpose, it is not mandated because there are circumstances that may necessitate a different value, such as traders’ belief that the mid is no longer relevant to their trading intent.

In practice, traders use their subjective judgement to “mark” their positions each day, usually, but not always, at the mid. This, of course, gives rise to the possibility that traders may use prices that increase their profits or alternatively reduce their losses. To counteract this possible mispricing, banks have created independent functions that check the prices used by traders to value their positions against independent sources for reasonableness. JPMorgan had created just such a function, the CIO Valuation

Journal of Operational Risk 9(2)
Control Group (VCG), whose role was to “independently test the front-office [ie, trading] marks at each month end and to determine necessary adjustments” (PSI 2013). The VCG reported through the CIO finance function up to the Chief Financial Officer.

In February and March 2012, while losses were exploding, the CIO traders had taken the decision to “mark away from the mid” because they had convinced themselves that the market was behaving irrationally “we can show that we are not at mids but on realistic level [sic]” (PISI 2013). Although the CIO traders only marked the portfolio slightly away from the mid (of the order of 1 basis point or one hundredth of 1%), the difference was nonetheless significant because of the sheer size of the SCP portfolio. By the end of March, the so-called lag or the aggregate difference between losses calculated using mid-prices and the prices used by traders was in the region of US$600 million and US$800 million (PSI 2013). In other words, traders were systematically under-reporting their losses. It was this under-reporting of losses in the first quarter reports to the SEC that led to criminal charges against CIO traders and managers (SEC 2013).

As noted by in the firm’s internal report, the CIO trading strategies were not subjected to robust challenge:

The firm expected them [senior CO management and traders] to subject CIO trading strategies to rigorous analysis and questioning prior to implementation, and to understand the risks inherent in the trading strategies. Here, they did not, and instead put in place the trading strategy without fully understanding what risks were being taken on, particularly in light of the size of the positions being built over the course of the first quarter of 2012. [Emphasis added.]

JPMorgan (2013)

In normal circumstances, the risks in this rapidly growing portfolio would have been detected by the firm’s VaR limit monitoring, and evasive action taken, were it not for the fact that CIO had in January 2012 introduced a new VaR model, which had the effect of hiding the increasing risk. This flawed model is described later but the model helped to create a “perfect storm” in which risks were rising rapidly but were not showing up on VaR reports. By the time that the perfect storm had blown over, the damage was enormous.

The question then arises: if such a situation was clearly unacceptable, why did JPMorgan’s management (generally recognized as competent) not detect and fix the problem before it got out of hand? Turner (1976) suggests some reasons.

4.1.1 Rigidity of belief

Turner (1976) points out that all organizations develop a culture that relates the tasks that individuals perform to the goals of the firm and that success stems from the
effectiveness of that culture. The other side of this coin, however, is that, in attempting to create an all-pervasive culture, managers may well become blind to potential problems.

As noted above, senior executives at JPMorgan were convinced that CIO was a relatively risk-free business that was being well-managed by exceptional professionals. This confidence was shared by CIO management and traders. In fact, CIO traders were convinced that the business was being overly conservative and that they could increase their profitability while still maintaining a low-risk profile. CIO traders were convinced that the firm’s standard VaR model was not recognising all the benefits of diversification in their credit derivatives portfolio. As described above, the VaR formulas allow a deduction for correlation, but the CIO traders were convinced that the existing correlation rules were too conservative and not benefitting the SCP enough. So they argued for the development of a new model that would handle correlations better from their perspective (JPMorgan 2013).

The existing so-called Basel I linear sensitivity model was designed to capture the risks arising from changing “credit spreads” in the portfolio but was “limited in the way that it estimated correlation risk: that is, the risk that defaults of the components within the index would correlate” (JPMorgan 2013). This discrepancy became significant as the SCP portfolio grew and in particular as traders increased the number of “index tranches” which by their nature were highly correlated with the rest of the portfolio. In August 2011, one of the CIO traders ordered the development of a new VaR model engaging a highly experienced and expert modeller, Patrick Hagan, from the central CIO quantitative team. Hagan is a quantitative expert and joint inventor of a widely used interest rate derivatives formula, the stochastic alpha beta rho (SABR) model (Hagan et al 2002). The modeler was also convinced that the correlation methodology in the existing VaR model was too conservative and, in November 2011, presented a new model to the firm’s independent model review team for approval that did indeed reduce the VaR for the SCP portfolio (JPMorgan 2013).

The central model review team performed a standard “backtest” on this new so-called Basel 2.5 model but used historical data of only two months for the test, because they were told that was the only data available (JPMorgan 2013). Nonetheless, after many exchanges of information and pressure to approve, the new model was approved and went live in late January 2012. This approval was in spite of some outstanding issues, not least the fact the model consisted of multiple Excel spreadsheets where data had to be manually “cut and pasted” to produce the results required. As part of the approval process, several actions to improve the model were agreed, but, in fact, the changes were never implemented (JPMorgan 2013).

However, the new model reduced the VaR for the SCP portfolio and traders began to trade up to the old VaR limits (JPMorgan 2013). Despite the fact that a number of VaR limits excesses had been recorded using the old model just prior to acceptance
of the new one, VaR limits were not exceeded with the new model. The hurried and unquestioning acceptance of a model that reduced the estimated VaR as anticipated by traders and modelers is an example of “confidence bias” or the ready acceptance of data that confirms one’s position to the exclusion of contradictory data (Kahneman 2012). In other words, CIO found what they were looking for and did no further searching for potential problems.

The new Basel 2.5 model was used until May 2012 when, after large losses in the SCP portfolio and a number of exceptions that arose during the model’s operation, a review of the model was ordered by the head of the central model review group (MRG). The review found a number of serious errors in the model, in particular spreadsheet errors that had the effect of reducing estimations of the volatility of correlations and hence the VaR (JPMorgan 2013). The decision was taken to revert to the standard model used by the JPMorgan Investment Banking division and immediately a significantly different picture of the risk in the SCP emerged. As Box et al (1987) noted, “remember that all models are wrong; the practical question is how wrong do they have to be to not be useful?” Obviously, the new Basel 2.5 model was “too wrong” to be useful.

In analyzing the events leading to the losses, the PSI reconstructed the levels of CIO VaR for the period using both the old and the new models and they found a significant difference between the model results (PSI 2013, Exhibit 1e). The PSI analysis showed that the CIO VaR limit of US$100 million was exceeded in late January 2012 but with the new model the VaR was immediately reduced to around US$80 million until it again reached the limit in late April. However, using the old model, the VaR limit was consistently exceeded from January 2012, touching almost US$200 million in April 2012; that is, the difference between the two models’ results was greater than the VaR limit itself. It is probable that, if the models were run in parallel for a period, the differences would have rung alarm bells sooner and possibly averted the losses. It is important to note the effect of the spike in VaR in late January 2012, which first broke the CIO VaR limit. This excess was promptly reported to risk management and caused widespread consternation in JPMorgan, with discussions going all the way to the CFO to grant a temporary increase in the VaR limit. This increase was granted temporarily because traders were committed to a strategy of reducing risk and on the understanding that the VaR figure would be brought down below the previous limit. The VaR was indeed reduced, but as a result of a new model, now known to be erroneous, rather than the reduction of risks.

In retrospect, CIO management and traders were victims of exactly the same sort of management myopia that led to the problems at other institutions that suffered large trading losses. They saw what they wanted to see. It is a hypothetical discussion but given that the bank’s risk management processes worked well to catch and address the VaR spike in late January, it is highly likely that the same processes would have
caught the ballooning SCP risk much earlier, had not the new model underestimated and hidden the risks. Unlike the NAB case (PWC 2004) it was not the VaR limit monitoring process that failed but the process of understanding what the limits were actually limiting.

4.1.2 Disregard of complaints from outsiders

Perhaps one of the most surprising findings in the disasters reported by Turner (1976), Gleick (1992), Augustine (1995) and McConnell (2005, 2010) was that often there were clear warnings of potential danger before a disaster occurred. However, warnings from outsiders were routinely dismissed by management with the assumption that the firm knows better than outsiders as to how to run its business. The same “organizational exclusivity” (Turner 1976) or “groupthink” (Janis 1971) was apparent within CIO.

As noted above, the OCC was the bank’s primary banking regulator and as such carried out a series of regular formal “examinations” across the bank. As part of these examinations, regulatory staff would raise so-called matters requiring attention (MRA) in a formal “supervisory letter”, the contents of which would be discussed in detail as part of a formal “close out” meeting between the bank and the lead examiners (PSI 2013).

In late 2010, the OCC held an examination of the CIO divisions and noted that CIO management needed to “document investment policies and portfolio decisions” because the CIO portfolios (including SCP) “lacked ‘a documented methodology’, ‘clear records of decisions’, and other features to ensure that the CIO was making investments and controlling associated risks in line with the expectations of senior management and the appropriate Board of Directors committee” (PSI 2013). The OCC’s head capital markets examiner was “surprised” at the reaction of Ina Drew, whom he said “‘sternly’ discussed [the OCC’s] conclusions with him for 45 minutes” and “complained that the regulator was trying to ‘destroy’ JPMorgan Chase’s business, and that its requirements would take away necessary flexibility from the CIO” (PSI 2013). According to the examiner in chief, Drew informed the OCC “that investment decisions are made with the full understanding of executive management including Jamie Dimon [and] that everyone knows that is going on and there is little need for more limits, controls, or reports” (PSI 2013). The OCC examiner noted that the level of “pushback” by Drew was “extreme” for an MRA regarding “basic banking expectations” (PSI 2013). Nonetheless, the formal response to the supervisory letter by CIO “committed to documenting investment and risk decisions for the SAA [strategic asset allocation] portfolio, but never mentioned the TAA [tactical asset allocation] portfolio in which the SCP was then located” (PSI 2013). But such a pushback was not unique. In a section of its report entitled “Resisting OCC Examination Results” the PSI noted that it was “very common” for the bank to push back on examiners’
findings and recommendations and the report documents a number of occasions in which OCC examiners were “ambushed”, bullied or even verbally abused (PSI 2013).

Like other banks, JPMorgan has an independent Internal Auditing (IA) department that audits various operations on a regular schedule. Unfortunately, the last audit of CIO before the scandal was done during March 2012, i.e., as the losses were exploding. The auditors appear to have missed the importance of the losses but made “adverse ratings” of both the Valuation Control Group (VCG) and the CIO risk management processes (PSI 2013). While fairly prescient in its criticisms, the audit was probably “too little, too late”. With hindsight, if the criticisms made by the OCC in its regulatory visits and internal audit had been properly addressed, the losses may have at least been lessened, if not eliminated altogether.

4.1.3 Information difficulties and noise

Turner (1976) pays particular attention to the problems that arise within and between organizational groups, highlighting the fact that information about a potential disaster is often widely available but is not communicated to those who may need to know it. Turner (1976) warns that a large number of “messages”, many of which are just “noise”, are generated in large organizations, which offer the “opportunity for failures of communications to develop”.

The attachments to the PSI investigation (PSI 2013, Exhibits) show that there was no lack of communication by email and telephone calls between the relatively small number of key players involved, less than twenty or so traders and managers in CIO and JPMorgan in general. The attachments to the PSI report show numerous examples of long email “chain letters” constructed by and forwarded by managers to one another and other parties who might have an interest. As each party digested the contents of an email chain letter, they would typically add their own particular spin and their own jargon to it. Often, in the attempt to be transparent, the accumulation of input just proved confusing. While in retrospect some key phrases should have jumped out, the managers concerned would have been bombarded by hundreds of such messages each day and, with their Blackberrys, into the night as well, as trading continued around the world. At times, traders appeared to be working very late to come to grips with the rising losses and sending out quite cryptic emails summarizing the problems.

What was missing, however, was thoughtful analysis of the situation and a level of importance attached to key messages. Often what was, in retrospect, critical information was sent out with fairly innocuous subject headings, for example, a message titled “Core Credit Book Update” from Bruno Iksil on February 29 contained the explosive information that that day’s huge trading had broken a critical limit. The overall impression is of a group of people reacting to the latest nugget of news but not standing back and trying to see the “big picture”. Unfortunately, even if they had
taken time to stand back and consider the information being drip-fed to them, the data was, in fact, wrong because the new VaR model was wrong.

### 4.1.4 The involvement of strangers

Turner refers to “strangers” as members of the general public who may behave unpredictably in a disaster. In the AIB and NAB cases, McConnell (2003, 2005) identified examples of “strangers” in the banking industry, in particular brokers, who had an impact on those events. A similar phenomenon is also apparent in the whale case. In Turner’s framework, “strangers” may not necessarily contribute directly to the causes of disasters but become part of the “noise” that distracts the attention of the participants and hinders the detection of potential problems. In the whale case, there are several external parties that could fit Turner’s description, such as hedge funds, but one group in particular was not a “stranger” per se, but did contribute to some of the confusion surrounding the events: JPMorgan Investment Bank (JPMIB).

As part of their proprietary trading activities, JPMIB actively traded the same credit derivatives as the CIO. When permission was given to the CIO division to trade credit derivatives, the CIO was required to use the “same ‘prices and valuation inputs’ as the Investment Bank and to work closely with the Investment Bank’s valuation team drawing in part on independent pricing information from valuation services like Markit and Totem” (PSI 2013). But the PSI (2013) noted there was no evidence that the CIO actually coordinated their pricing data or sources with JPMIB but instead used their own methods because they believed their trading strategies were different to those held by JPMIB. As a CIO manager noted:

> CIO necessarily uses judgment to identify the point within the bid-offer spread that best represents the level at which CIO reasonably believes it could exit its positions, considering available broker quotes, market liquidity, recent price volatility and other factors. [Emphasis added.]

PSI 2013

As described above, the differences in pricing methodology emerged most starkly in late January 2012 when the CIO traders began to mark their positions to market away from the mid-point of the bid–ask spread, because they believed that “the market was irrational” (PSI 2013). This, of course, meant that CIO were valuing the same securities with different prices to their colleagues in JPMIB, which could not go unnoticed in the marketplace. In late March 2012, as events spiralled out of control, a senior CIO executive actually went so far as to accuse the JPMIB traders of “manipulating the market [and] disclosing information about the CIO’s positions to the marketplace at large” (PSI 2013). The response from JPMIB management was that because of the sheer size of the whale trades, the market was fully aware of the SCP positions and that the “mid-price” valuations used by JPMIB were correct.

*Journal of Operational Risk* 9(2)
The situation was exacerbated by the fact that CIO were experiencing numerous “collateral disputes” which arise when parties to a CDS trade have to post “collateral” usually in the form of cash or government securities, whenever market prices move against them. Collateral disputes arise when parties disagree about the current market price of a trade and hence the amount of collateral due. The head of CIO, Ina Drew, noted that, before 2012, the CIO did not experience any large disputes but by mid-April 2012 they were experiencing multiple disputes totalling over US$690 million. Counterparts in dispute with the CIO could point to the fact that the CIO used different “marks” to JPMIB and they had no disputes with those prices. A senior JPMIB executive noted that such collateral disputes were another “red flag” of positions being mismarked (PSI 2013).

An investigation by JPMIB executives into pricing differences not only turned up mismarking of positions but also other problems and these findings signalled the beginning of the end of the whale episode. Just a few weeks later, Drew resigned and the SCP positions were handed over to JPMIB traders to manage and to work out. There is no evidence that JPMIB employees actually worked to undermine their CIO colleagues: on the contrary, they maintained a very professional and disciplined approach to their trading, in particular their use of conservative VaR models and pricing methods. However, during the crisis needless finger-pointing distracted management from seeing the looming problems.

4.1.5 Failure to comply with discredited or out-of-date regulations

Turner (1976) points out that failures to do what is right do not usually happen in isolation but arise from a culture of failing “to comply with discredited or out-of-date regulations”. This, as with NAB and ANZ (McConnell 2003, 2005), was also true of JPMorgan. Turner (1976) suggests that ignoring “discredited or out-of-date policies” is especially problematic because there is an appearance of full compliance with policies giving management “false confidence” that all is well. Coupled with the lack of good information flowing to those managers who have the power to act, potentially serious problems can fester until there is a disaster.

Failing to comply with regulations or controls is one of the recurring features of disasters and is particularly dangerous not only because the regulations, even if imperfect, may nonetheless have some value, but, more importantly, because others may assume that the controls are still in place. In financial trading, some of the key regulations or controls relate to the breaching (called “excession” by JPMorgan) of risk limits. If risk limit monitoring processes are in place then it is not unreasonable for control functions, such as risk management, to assume that absence of limit breaks means that risk are being controlled within agreed limits. In other words, absence of
limit breaks implies absence of unauthorized risks. Unfortunately, that was not the case in JPMorgan.

JPMorgan prides itself on having a range of “statistical” risk measures such as VaR and “nonstatistical” measures such as stress testing and sensitivity analysis and a comprehensive range of limits to alert management when excessive risks are being taken (JPMorgan 2011).

In addition to a VaR limit, CIO utilized four other types of risk measures and limits: credit widening spread at 1% (CS01); credit widening spread at 10% (CSW10); stress loss limit; and stop advisories (which are designed to halt trading when a predetermined level of loss is encountered). Far from being in control, the PSI noted that in the first four months of 2012 “CIO risk limits and advisories were breached more than 330 times” (PSI 2013).

The PSI report describes in detail the measurement and use of these measures and limits, but CS01 is illustrative of the failure to react to recurring limit breaches. CS01, also known as CSPBV, measures the “expected profit or loss to a portfolio if the credit spread on a credit position widened by 1 basis point over the course of a day” or the sensitivity of the portfolio to a “widening” in credit spreads by 1 basis point (PSI 2013). In January 2012, the CS01 limit for CIO had been set at US$5 million. CS01 was not a “hard” limit requiring trading to stop or positions to be reduced but an advisory limit when a limit breach would “trigger a discussion as to whether the positions had to be unwound” (PSI 2013). In other words, CS01 was a “red flag” requiring attention, rather than a “red light”. But the PSI showed the CS01 limit was breached early in January 2012 and remained in breach (by more than 1000%) until it was deactivated in May 2012 (PSI 2013, see “CIO MTM CS01 Limit Breaches, Sept. 2011–May 2012”). By then, however, the horse had bolted.

The CIO traders were well aware that the CS01 limit was constantly being breached, as they made repeated requests for the CS01 limit to be “temporarily” increased, but the increases were refused by JPMorgan Risk Management (PSI 2013). When the continual breach was raised by the central market risk management group, the attitude to this particular control within CIO became apparent when Drew responded “I have no memory of this limit. In any case it need[s] to be recast with other limits. [It is] old and outdated” (PSI 2013). Rather than ask why the breach had occurred, which was precisely because the risk was growing out of hand, CIO management added the CS01 and other significant limits to a list of issues that had to be addressed in a future limit review (PSI 2013).

CIO also utilized another measure of risk, the comprehensive risk measure (CRM), which did not have a limit per se but measured potential losses over one year, somewhat similar to a “one-year” VaR. However, in February 2012, when the CRM warned of a yearly US$6 billion loss (which was in retrospect pretty accurate), the measure was derided by CIO staff as “garbage” (PSI 2013). CIO staff did not investigate the reasons
for the CRM estimate of large losses, but instead, as with other risk measures and limit breaches, criticized the methodology used and “when confronted with a metric signaling a huge increase in risk, the CIO manager responsible for the Synthetic Credit Portfolio not only disputed the metric, but also, as with the VaR results in January, questioned the model itself” (PSI 2013).

As Turner (1976) shows, managers react to what they perceive to be discredited regulations by ignoring rather than replacing them. When multiple controls are ignored and not replaced the situation arises where senior executives believe a division is prudent in its risk management but in fact may be out of control.

4.1.6 Minimizing emergent danger

A common feature of organizational disasters is that those who are closest to the problem “fail to call for help”, which has been attributed to fears of causing unnecessary alarm, psychological denial of the danger or the assertion of the individual’s invulnerability (Turner 1976). Turner points out that individuals consistently underestimate the scale of problems that they face because of ambiguity or disagreement about the evidence of danger. He also notes that when the danger becomes impossible to ignore, rather than address the causes of the problem, individuals often look to shift the blame to others (Turner 1976).

Aside from the CEO’s unfortunate comment that the whale losses were a “tempest in a teacup”, there are many instances of senior managers in CIO sticking their heads in the sand as losses began to mount up in the first quarter of 2012. Paradoxically, those closest to the problem were often the most realistic though they did continue to trade the SCP into further trouble. For example, the head trader Bruno Iksil, recommended taking “the pain fast” at the outset and several times over the next three months warned of additional losses and poor liquidity and suggesting at the end of January that “the ‘only’ course of action was ‘to stay as we are and let the book simply die’” (PSI 2013).

But CIO senior management, including CIO head Ina Drew, did not want to take the losses that would occur as a result of letting the “book simply die”; in fact, some senior management did not want to lose any money at all from unwinding the portfolio (PSI 2013). This was clearly unrealistic, which, as experienced professionals, they would have known. Furthermore, the strategy adopted by traders was “well-communicated” and accepted by CIO management. The overall strategy of “going long” was described by Drew as “not terrible” given that “the credit market was rallying and short positions had lost so much value”, a view that was shared by another senior executive, Javier Martin-Artajo, who “believed that the long position was necessary to stabilize the book, [but] being long did not serve the mission of the SCP” (PSI 2013). In other words, the senior executives were
downplaying the losses in the hope that the market would turn in their favor. More
seriously, they, and other JPMorgan executives, downplayed the significance of the
losses in the SCP to external parties, including the OCC and even neglecting to high-
light the issues in a meeting with the JPMorgan Board Risk Policy Committee (PSI
2013).

It is apparent from the many emails and recorded telephone conversations released
by the PSI (2013) that traders and senior executives in CIO were well aware of the
serious losses being incurred in the SCP portfolio but, like deer caught in head-
lights, were unable to do anything about them. The situation had spun out of their
control.

5 OPERATIONAL RISK MANAGEMENT

The breakdown of controls at the CIO division, and JPMorgan in general, illustrates
a failure in the management of operational risk. And it is worrying that, in spite of
the regulations, instituted after the failure of Barings and adopted as “best practice”
by major banks as part of Basel II regulations, similar failures of operational risk
management continue to occur.

5.1 The Basel proposals

In 2004, the Basel Committee of the Bank for International Settlements, the world’s
senior banking regulator, finalized proposals to bring the management of operational
risk in line with the standards already adopted for market and credit risks (Basel
Committee on Banking Supervision 2004). These so-called Basel II proposals are
designed to strengthen operational controls in international banks and to ensure that
they have set aside sufficient capital to cover large losses, such as those at JPMorgan.
The Basel Committee defines operational risk as “the risk of loss resulting from inade-
quate or failed internal processes, people and systems or from external events. This
definition includes legal risk but not strategic or reputational risk” (Basel Committee
on Banking Supervision 2004).

It is interesting that in the descriptions of the organizational failures that led up
to the losses (JPMorgan 2013; PSI 2013; CFTC 2013), there are many references to
“operational shortcomings” (JPMorgan 2013) but there are no references to oper-
tional risk as a contributing factor to the losses. Nor, except for a passing reference
at the firm-wide level, is there a reference to operational risk management (ORM) as
a discipline that was present in trying to avert the losses, According to the division’s
organization charts, CIO did not have its own ORM function (PSI 2013, exhibit 2). It
is obvious, however, that all of the following factors identified by the Basel Committee
as giving rise to operational risk were present in the whale case.
Processes: failure of basic processes designed to manage risks.

People: failure to follow policies in particular mismarking positions, failure to properly staff risk management and modeling groups, and evidence of bullying and aggressive behavior toward colleagues.

Systems: deficient VaR models.

External: adverse actions by competitors when the size of the whale trades became apparent.

In particular, the internal task force inquiry (JPMorgan 2013) highlighted the following significant deficiencies in processes at all of the following levels of CIO.

(a) Modeling: nonadherence to published Model Development and Approval policies and processes.

(b) Risk Management: the failure to properly manage market risk limit excesses.

(c) Financial: the failure to properly monitor CIO financial positions.

(d) Systems: the failure to build a robust VaR model.

(e) Audit: the failure to identify the losses even though an audit was being undertaken when the losses were occurring.

(f) Strategic: the failure of senior management to recognize that the SCP had morphed from a “macro-hedge” into a proprietary trading portfolio, which was never its intent.

Before discussing the lessons that can be learned for the risk management failures in the whale case, specific failures of model development are described.

### 5.2 Model Risk Management

In the 2004 Basel II regulations, “Model/System Misoperation” is identified as an Operational Risk Loss Event Type in the category of “Execution, Delivery & Process Management”, in the level 2 category “Transaction Capture, Execution & Maintenance” (Basel Committee on Banking Supervision 2004, Annex 7). In the more comprehensive classification used by the industry body, the Operational Risk data eXchange Association (ORX), “model error” is identified in several categories, including the same classification as Basel II, as EL0701, and also in the Basel II category of “Clients, Products & Business Practices” (EL0403). It is also categorized as a separate category of “Product Control” as PC 0609 – “Incorrect (but approved) model used to value position (asset or liability)” (ORX 2011). The whale case would seem to fit
into a number of these classes but while the exact classification is somewhat moot, the losses are clearly an Operational Risk Loss Event.

Despite being on the risk management agenda since the introduction of Basel II in 2004, the formal concept of Model Risk Management is relatively new, arising, in the case of JPMorgan, from a joint formal “Supervisory Guidance” from its two main banking regulators, the OCC and the Board of the Federal Reserve, in April 2011 (Federal Reserve 2011). The regulators define “model risk” as “the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports” and note that “model risk can lead to financial loss, poor business and strategic decision making, or damage to a bank’s reputation” and they conclude that “those consequences should be addressed by active management of model risk” (Federal Reserve 2011).

The regulatory guidance is too comprehensive to describe in detail in this paper but includes the creation of a “model risk management framework” that is comprehensive and rigorous and operates throughout the firm as a series of key processes:

Model risk management begins with robust model development, implementation, and use. Another essential element is a sound model validation process. A third element is governance, which sets an effective framework with defined roles and responsibilities for clear communication of model limitations and assumptions, as well as the authority to restrict model usage. [Emphasis added.]

Federal Reserve (2011)

It is obvious that JPMorgan attempted to embrace the concept of Model Risk Management by the creation of a central Model Risk and Development function and a Model Review Group (MRG) with responsibilities for validation and approval of new models. In the case of the CIO “Basel 2.5” model, this process was in fact followed, as the CIO model developer submitted the new model for validation and approval by the MRG. However, possibly because the MRG process was bedding in, the model review process was not as rigorous as it might have been.

In January 2012, the CIO model developer was being pressured to implement the new “Basel 2.5” model as quickly as possible because of the reduction in RW As that was expected from it (and because the CIO VaR limit was being exceeded!). The developer, an expert modeler, also believed that the RW As would be reduced by some 30%, bringing the VaR well below the current risk limits and, in turn, pressured the review group to expedite its approval (JPMorgan 2013). At the end of January 2012, approval was given to use the model but a number of issues were documented that required changes to be made to the model, not least its use of Excel as the calculation engine and the use of a nonapproved mathematical function library. While there is no evidence that the CIO modelers did not intend to make the changes, in fact what happened was that the key modeler was co-opted to input data to the model and

Journal of Operational Risk 9(2)
personally operate it on a daily basis; his request for additional staff to assist in changing the model were ignored (PSI 2013). As noted above, increasing problems in the CIO model gave the impetus for a review of the model which not only found technical errors but also problems with its theoretical methodology.

With hindsight it is not difficult to criticize what was still an evolving set of processes but it is hard to escape the conclusion that the model development and approval processes failed in this instance.

Despite the operational problems identified by the Model Review Group and the obvious questions raised by the new VaR model results, a lax approval process at the bank allowed the model to be put into effect immediately, prior to the specified corrective actions being completed.

PSI (2013)

While in the end, the losses were precipitated by failure to manage market risks, it is the failure of fundamental banking processes, inadequate models and, to a minor extent, staff misdemeanors that led to the losses, ie, the whale scandal was an Operational Risk Event as defined by Basel II.

6 LESSONS FOR OPERATIONAL RISK MANAGEMENT

If, as argued in this paper, Turner (1976) is correct in asserting that many spectacular operational risk loss events, such as the whale case, must be viewed as resulting from management failures that should be apparent over a long period of time, an obvious question is: what lessons can be learned from these failures?

6.1 Where was operational risk management?

That such an enormous trading loss should occur in a firm that had the highest reputation for risk management should give risk management professionals pause for thought. Risk management is an ever moving discipline but JPMorgan aspired to be a leader in this field (JPMorgan 2011). By 2012, JPMorgan had enthusiastically adopted all of the best practice risk management processes recommended by regulators and industry experts, such as independent risk functions, independent model approval, independent valuation and comprehensive, transparent reporting of risks.

And at the firm-wide level, JPMorgan’s risk management processes worked fairly well in the whale case, as it was the central groups that detected and brought to light the breaches of risk limits and the modeling errors. However, at the CIO divisional level, the processes were a “Potemkin village”, as the Parliamentary Commission on Banking Standards (PCBS) characterized risk management at several banks during the GFC (PCBS 2013). Such a village is in reality a facade designed to fool authorities that all is well. In the CIO, before the whale losses, there appeared to be a comprehensive
market risk management process, but the policies were in reality being circumvented or ignored.

This paper, and the reports on which it is based, detailed just some of the failures of processes that occurred in the CIO. The following three sets of interlinked processes, in particular, contributed to the magnitude of the losses.

(1) In the case of the new VaR model, failures to follow prudent model development and approval processes and to create a robust systems environment for operating the new model, reinforcing those failures.

(2) Failure to implement a meaningful set of risk limits appropriate to the CIO’s trading strategy for the SCP; failure to monitor all breaches of limits, and failure to take action to bring trading under limits after limit breaches.

(3) Failure to implement firm-wide policies on marking to market the trading positions and failure of the finance function to understand the sources of CIO’s income and risks.

To understand how these failures occurred it is necessary to consider the role of market risk management in the CIO and in general. As stated in Basel II (Basel Committee on Banking Supervision 2004), the basic requirements for approval to use a bank’s own model for calculating market RWAs and hence capital for the trading book include the following.

- Clearly documented trading strategy for the position/instrument or portfolios, approved by senior management (which would include expected holding horizon).

- Clearly defined policies and procedures for the active management of the position which must include:
  - positions are managed on a trading desk;
  - position limits are set and monitored for appropriateness;
  - dealers have the autonomy to enter into/manage the position within agreed limits and according to the agreed strategy;
  - positions are marked to market at least daily and when marking to model the parameters must be assessed on a daily basis;
  - positions are reported to senior management as an integral part of the institution’s risk management process; and
  - positions are actively monitored with reference to market information sources.

- Clearly defined policy and procedures to monitor the positions against the bank’s trading strategy including the monitoring of turnover and stale positions in the bank’s trading book. [Emphasis added.]

Basel Committee on Banking Supervision (2004, Paragraph 688)
The CIO division appear to have failed to follow even some of the most basic regulatory requirements for prudent market risk management and in addition, as noted above, failed to follow the processes for model development and approval as required by their regulators (Federal Reserve 2011).

Why did those failures occur? The response of the head of market risk management (MRM) in CIO gives an insight, in that the group acted as a “middleman” who coordinated between the risk modelers and the traders and managers to ensure that the risk metrics were properly calculated and disseminated to decision makers. [Furthermore …] when the SCP began causing the CIO to breach its risk limits in January 2012, he did not enforce those limits, or direct the traders to exit any positions. [Emphasis added.]

PSI (2013)

The market risk team at the time was interested in the intricacies of the market risks being taken by traders and in trying to model them as well as they could. They essentially had the role of being technical experts in modeling rather than experts in designing and implementing robust modeling processes. Given the complexities of market risk modeling, especially involving derivatives, it is unrealistic to presume that market risk managers can be both “rocket scientists” and process and management experts.

6.2 Suggested changes to risk management organization

Understanding the complex market risks being taken by a trading group and the processes needed to manage those market risks are two very different skill sets. Traditionally, the second, understanding processes, was a role that was, if not undertaken by, then at least reviewed by internal and external audit functions. However, audit functions cannot be everywhere all the time, and in fact they deliberately cycle their work through different departments according to a fairly prolonged schedule. So who should monitor the process?

It is suggested here that the role of the market risk management in large banks be split into two separate functions: market risk modeling and communication and market risk management processes. And it is suggested that this second role is taken by the firm’s operational risk management function using their expertise in evaluating “process risks”.

This is not a grab for power on the part of operational risk management so much as a recognition of the different skill sets required, or “horses for courses”, but it also adds a level of independence to the risk management process. To expand, while the choice of the models to use in measuring market risks in particular circumstances and the setting of risk limits for those measures would remain with existing MRM functions, monitoring of the processes for actually doing those tasks would become...
the responsibility of the independent ORM function. In practice that would mean, for example, that ORM would, for a new model, check that the model approval process had been followed and independently raise any issues and concerns to divisional and firm management. Likewise, ORM would receive notification of all risk limit breaches and proactively follow up to ensure that the breaches are resolved by approved processes. This is a sort of audit role, but a proactive, operational audit role. Unlike the situation where the reporting lines of the MRM function in the CIO were unclear and confused, the suggested ORM function would report directly to the firm-wide risk function.

In order to execute such a role effectively, however, the ORM staff involved would have to gain a degree of insight into the complexities of market risk, although obviously not as much as the designated MRM staff. It would also be incumbent on senior risk executives to ensure that the two functions worked well together and any turf issues were addressed and resolved.

### 6.3 Behavioral biases

As this paper concentrates on “process risks”, in particular model risk, it does not address in detail the many examples of “cognitive biases” that were apparent in the whale case, and as identified by Turner (1976), where managers ignore the mounting evidence of problems facing them. The paper does pick out two biases that were apparent and should be addressed as part of formal operational risk management frameworks (Blunden and Thirwell 2010).

First, there is some evidence of “groupthink” (Janis 1971) in the whale case in the manner in which CIO management and traders took a common and defensive approach to disquiet from outside parties, preferring to question their motives, rather than addressing their concerns (PSI 2013). Janis (1971) defines “groupthink” as the mode of thinking that persons engage in when concurrence seeking [original emphasis] becomes so dominant in a cohesive group that it tends to override realistic appraisals of alternative courses of action [and] refers to a deterioration in mental efficiency, reality testing and moral judgments as a result of group pressures.

Janis (1971)

The whale case illustrates just such a “deterioration” in “reality testing” and “collective rationalization” (Janis 1971) in seeing the huge losses that were occurring but being unable to stem the flow. Instead, CIO managers and traders turned on those raising concerns, for example, when large losses were predicted, rejecting the warnings as “garbage” (PSI 2013). This behavior is a typical symptom of “groupthink”, which is termed “direct pressure on dissenters” (Janis 1971), and is similar to Turner’s “disregard of complaints from outsiders” (Turner 1976).

Among other biases evident in the case, such as the “confirmation bias” displayed by traders and modelers in accepting without question the (flawed) estimates of the
new VaR model, there is evidence of “overconfidence” (Kahneman 2011), especially by the CIO traders:

Other people in the markets – like hedge funds and other traders – thought Iksil was being *ridiculously overconfident*.... They outsmarted Iksil. As he kept digging himself deeper into his position, he got backed into a corner and couldn’t cover his losses. [Emphasis added.]

PSI (2013)

Such overconfidence, not only from traders but also from the entire CIO management, led the group to overestimate their ability to trade out of the losing situation that they had got themselves into. As the case shows, the overconfidence was misplaced and extremely costly to JPMorgan. Further detailed studies of the whale case could lead researchers to make suggestions as to actions to reduce the impact of possible groupthink and overconfidence in such situations in future.

7 SUMMARY

The losses at JPMorgan due to the whale scandal were the result of an event that captured the attention of bankers, banking regulators and investors. Justice, in the form of an internal inquiry, was seen to be done and heads have rolled. But have the lessons of JPMorgan (and similar events at Barings, NAB, AIB, Société Générale and UBS) really been learned?

In summarizing their inquiry into the case, the US congress wrote:

The JPMorgan Chase whale trades provide *a startling and instructive case history* of how synthetic credit derivatives have become a multi-billion dollar source of risk within the US banking system. They also demonstrate how *inadequate derivative valuation practices* enabled traders to hide substantial losses for months at a time; lax hedging practices obscured whether derivatives were being used to offset risk or take risk; *risk limit breaches were routinely disregarded*; *risk evaluation models were manipulated to downplay risk*; inadequate regulatory oversight was too easily dodged or stonewalled; and derivative trading and financial results were *misrepresented to investors*, regulators, policymakers, and the taxpaying public who, when banks lose big, may be required to finance multi-billion-dollar bailouts. [Emphasis added.]

PSI (2013)

The paper examines the losses in the whale case using a framework for disasters developed by the late Barry Taylor, which identifies managerial deficiencies that can lead to significant losses. In particular, Turner identifies failures “to comply with discredited or out-of-date regulations” as being particularly crucial. In the whale case, experienced managers circumvented or ignored key control processes, opening the way for losses to occur. In particular, management circumvented the banks’ policies on model development, which led to the introduction of a new market risk model that
was later found to be flawed. However, the model’s errors were not detected until after the traders had vastly increased the risks in their portfolio of complex credit derivatives. Had the model not been introduced in haste, and warnings heeded as to the extent of the risky positions that the bank was holding, it is probable that the error would have been found before the catastrophic losses occurred. The paper describes how these deficiencies caused the losses and makes suggestions as to how similar events could be prevented in other banks.

As far back as 1976, Barry Turner argued that “organizational disasters” do not happen overnight but are the result of organizational failures over a long period of time. This paper analyzed the reports of official inquiries into the losses at JPMorgan, using Turner’s framework, and pointed out that most of the “common features of disasters” identified by Turner were present in the whale case. The paper argues that Turner’s work is not only useful as a forensic tool for analyzing disastrous events after they have occurred but also contains valuable lessons for practicing managers. There is also considerable scope for updating Turner’s framework to take account of new factors, such as the insidious effect of psychology biases in financial trading.

REFERENCES


*Journal of Operational Risk* 9(2)
CFTC (2013). Order instituting proceedings pursuant to Sections 6(c) and 6(d) of the commodity exchange act, making Findings and imposing remedial sanctions. October 16, US Commodity Futures Trading Commission, Washington, DC. URL: www.cftc.gov/ucm/groups/public/@lrenforcementactions/documents/legalpleading/enfjpmorganorder101613.pdf.


Forum Paper www.risk.net/journal


