REPRINTED FROM EnergyRisk

April 2012

MANAGING OPERATIONAL RISK

Proactive management of operational risk is critical to ensuring an organisation responds effectively to ever-changing market conditions and regulatory environments. Julie Shochat and Kenzel Fallen outline how to align strategy, processes and technologies to effectively mitigate operational risks and meet future regulatory demands

Brian A Jackson / Shutterstock.com

Commodity trading organisations have faced numerous types of risk throughout the evolution of the industry. In today's market, anticipating and responding to various operational risks has become particularly challenging and increasingly critical.

Several recent examples highlight the importance of effectively managing operational risk:

- In September 2011, UBS suffered a rogue trading incident resulting in a loss of $2.3 billion, after which the company's chief executive, Sergio Ermotti, announced an initiative to overhaul the bank's operational risk management framework.
- In January 2012, US FBI director Robert Mueller testified before the US Senate Select Committee on Intelligence that cyber threats, both espionage and disruption, by both rogue hackers and foreign governments, would surpass terrorism as the country's top concern.
- On February 13, 2012, Globex, the electronic platform used by the CME Group, experienced a technical issue that halted trade transmission for almost an hour.
- The Edison Electric Institute recently estimated that Dodd-Frank mandates, which may require electric utilities to post margin on over-the-counter transactions, would have a negative average annual cashflow impact of $250 million–400 million per utility.

Operational risk and potential loss

The Basel Committee on Banking Supervision defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". A failure in any of these areas can result in loss requiring a costly mitigation effort throughout the organisation. Losses resulting from improper operational risk management can be categorised into one of the Basel Committee's seven areas of potential loss that span across the four areas of operational risk.

The long-term costs incurred following such losses can substantially exceed the initial cost of the incident, and may put a significant dent in your organisation's working capital. These costs may include fees to legal counsel and consultants, impairment of company assets, regulatory fines and penalties, and/or expenses associated with returning to a normal state of operations. Additionally, your organisation may face forgone revenues or require investments to prevent or reduce future exposures and enhancements to controls, policies and systems.

Operational risk management

We find that the most effective preparation for and defence against operational risks is to evaluate your organisation's current capabilities, define your business strategy and develop a road map to establish a centralised operational risk capability across business units, commodities and functions.

Developing your operational risk capability will require a top-down vision from senior management coupled with a bottom-up plan to transform the organisations, processes and technologies involved. Implementing and maintaining such an operational risk capability will provide a competitive advantage by preparing you to efficiently address future operational failures, curtail loss events and minimise subsequent costs. Organisations that maintain fragmented risk groups and processes will lack the benefits of centralised strategic decision-making and cross-functional alignment and oversight.

Getting started: conduct a risk assessment

The first step in building an operational risk capability is to conduct a thorough risk assessment.

Julie Shochat and Kenzel Fallen

This provides insight into current and potential risks or regulatory demands to which your organisation is exposed. This process includes a current organisational snapshot, requirements inventory, gap analysis and a road map for development.

Current snapshot

When performing the current snapshot, assess all functions across regions and business units that currently conduct activities requiring operational risk management. Senior management and leadership across those functions should work together to identify and map activities within the global organisation, including:

- Organisational structure;
- Projects in-flight or planned;
- Internal processes and policies;
- External compliance requirements;
- Reporting tools and processes;
- Communication standards;
- IT infrastructure.

The current snapshot will provide a framework for your organisation's strategy and responsibilities for managing and controlling applications, current contingency plans and communication protocols.

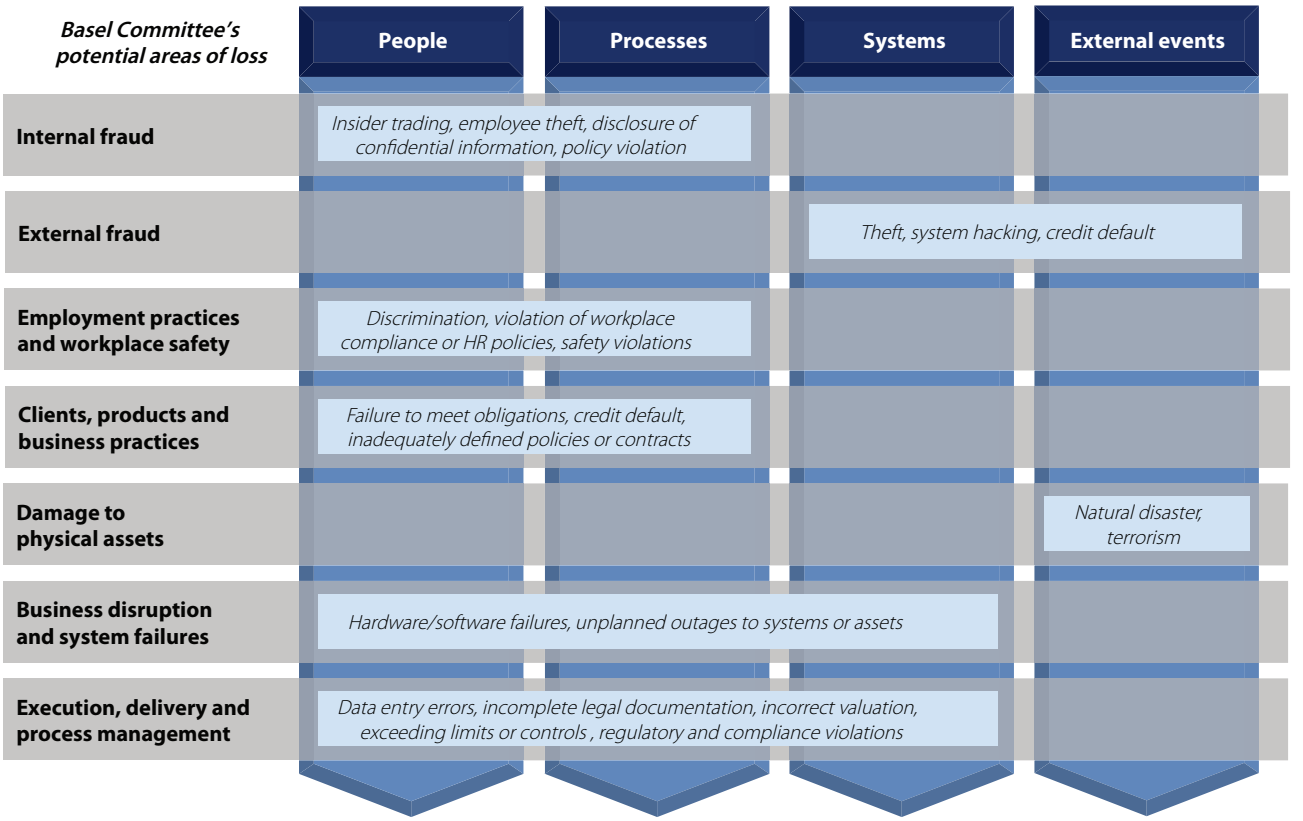
Operational risk requirements and impact

A global, cross-functional effort is required to create a comprehensive inventory of all internal and external operational risk requirements, including internal controls, processes and policies, regulatory agencies to which the business is responsible, and current and proposed regulations relevant to the business. This inventory is a foundation for identifying, quantifying and prioritising current and potential operational risks.

Gap analysis

The gap analysis is a detailed evaluation of current-state observations and future-state enhancement opportunities. This is

F1. Operational risk – potential areas of loss *Source: Enite*



a collaborative effort that considers a number of parameters, including each requirement's regulatory importance, potential penalties, headline risk and immediacy and urgency of impact. Each observation or requirement considered should be assessed and prioritised based on estimated benefit and cost (both current cost to organisation by not addressing, and cost to address).

Road map development

Developing the strategic road map for all organisational, process and technology enhancements is a collaborative effort between global senior leadership and functional leadership across business units. The road map should include strategic objectives, timeline, budget, organisational requirements and technology requirements.

> *In light of upcoming regulatory changes in the industry, there is an even greater sense of urgency to proactively address your operational risks*

Programme management

Concurrently with the execution of the risk assessment, it is important to develop a programme management office (PMO) to manage stakeholder alignment, internal communications, project planning, milestone monitoring, decision-making and budget tracking. Maintaining a clear line of communication with business representatives and key stakeholders is a critical but often overlooked component of a PMO. Keeping all parties informed and engaged will help ensure the success of building the operational risk capability. A programme management director should be responsible for maintaining the long-term sustainability of the resulting operational risk capability.

Next steps: enhance your organisation

The risk assessment will unveil several opportunities for your organisation to improve or build new processes,

technologies and/or capabilities. Each organisation will pursue a unique set of initiatives based on its specific needs and priorities. Below are a few common high-priority outcomes of the risk assessment.

Reporting capability enhancement

Integrate or enhance your reporting capabilities and/or create a sustainable reporting programme with clearly delineated points of accountability. Maintaining a reporting programme will help ensure that your operational risk capability is adequately identifying potential future risks or losses that your organisation can pre-emptively mitigate.

Architecture improvement

Build tools or enhance existing solutions to enable proactive risk identification and/or reduce potential future risks. For example, build a disaster recovery solution if one is not in place, ensure that technologies used for crucial communications are stable, improve performance and reliability on file storage drives, or establish viable back-ups for potential outages.

> *In light of upcoming regulatory changes in the industry, there is an even greater sense of urgency to proactively address your operational risks*

Organisational capability

If your organisation does not have resources with the skills required to manage operational risk capability, you may need to provide training, transfer qualified resources from another part of the company, or hire externally. Ideal candidates for managing the operational risk capability will have relevant experience in operations, risk management and regulatory compliance. They should also be well networked and respected across various functions of the organisation.

Each initiative your organisation decides to pursue will require an effort to design the future state, implement the solution and train your employees. As some of these efforts may place a significant strain on your resources, it is important to prioritise based on the cost and ability to implement as well as the expected benefit to your organisation.

Julie Shochat, manager, and Kenzel Fallen, consultant, Enite

Looking ahead

While it is unrealistic for your organisation to completely eradicate its exposure to operational risks, you can reduce or prevent losses by proactively building and maintaining a centralised operational risk capability. In light of upcoming regulatory changes, there is an even greater sense of urgency to proactively address your operational risks. Increasingly stringent regulatory conditions will require alignment of current capabilities with expected internal compliance and regulatory demands. By assessing your current operational risk capabilities, planning a strategic road map for enhancements, and implementing a formal operational risk capability, you can be more fully prepared to mitigate those inevitable operational risks. ■

F2. Risk assessment approach *Source: Enite*