SOCIETY OF ACTUARIES

2014 Enterprise Risk Management Symposium

Sept. 29 - Oct. 1, 2014, Chicago, IL

A Primer on Managing Operational Risk for Insurance Companies

By Kay K. Rahardjo, FCAS, MAAA

Actuaries

Risk is Opportunity.℠

A Primer on Managing Operational Risk for Insurance Companies

By Kay K. Rahardjo, FCAS, MAAA

Operational risk is likely one of the most significant risks faced by your organization. It is not only financial services firms that must manage operational risk. Each branch of the U.S. military has manuals that describe the appropriate management of operational risk[1]; the military's goal to ***protect and preserve resources*** is applicable to the military and also to corporations in every industry.

While all companies have operational risk, the examples herein will focus on how these concepts apply for insurance companies. This article will define operational risk and how a company or organization can effectively manage this risk, including types of management tools, metrics and measurement, and governance, risk and compliance (GRC) systems.

What Is Operational Risk?

Operational risk is *the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.* This includes legal and compliance risk and excludes strategic and reputational risk. This widely accepted definition is from the Basel Committee on Banking Supervision, a group that promulgates international standards used by many banking regulators.

[1] See, for example, Operational Risk Management, Marine Corps Institute, ORM 1-0, Headquarters Marine Corps, Washington, D.C., February 2002.

Operational risk can occur due to:

- An error by the person doing an activity.
- The system necessary to perform an activity is broken or not functioning.
- The process supporting an activity is flawed or inappropriately controlled.
- An external event occurs that disrupts activity.

All companies, whether or not they actively manage and recognize operational risk, have operational risk. Companies do not willingly take operational risk and they are not rewarded for it, yet it is inherent throughout the firm. Companies willingly take other types of risk because they believe they will be rewarded for taking this risk. For example, insurance companies write insurance policies that cover property exposures on the coast where hurricanes are inevitable. Successful companies manage catastrophe risk by prudently managing the exposures and by pricing the policies appropriately. Managing operational risk is not as straightforward as managing financial or insurance risk.

The comptroller of the currency, Thomas Curry, has cited the increased prominence of operational risk saying that it has eclipsed credit risk as the regulator's chief concern.[2] His examples of operational risk include:

[2] Remarks by Thomas J. Curry, comptroller of the currency, before the Exchequer Club, May 16, 2012.

- **Model risk**: The need to validate critical models and to ensure appropriate assumptions and input data. Simply put: When you add 2 + 3, do you get 5?
- **Information technology security**: Companies must continue to invest in security to ward off increasingly sophisticated criminals who steal consumer data or disrupt customer service.
- **Third-party reliance**: Companies continue to own the risk even though they may have outsourced portions of their business process—that is, a company can outsource the *process* but it does not outsource the *risk*.
- **Compliance deficiencies:** Curry specifically cited the Banking Secrecy Act and Anti-Money Laundering as complex but necessary regulations with which companies must comply. A recent insurance company example is the National Association of Insurance Commissioners (NAIC) Own Risk and Solvency Assessment (ORSA) requirement due in 2015.

Recent examples of losses from operational risks include various incidents from JPMorgan, as well as from Knight Trading and UBS. JPMorgan's various woes—including the London Whale incident and alleged electricity market manipulation—have cost the company $31 billion in fines and legal costs as of January 2014.[3] This does not include the reported $6.2 billion of financial loss from the London Whale incident nor damage to JPMorgan's reputation as a very well-managed financial services firm. Knight Capital had a trading error in 2012 that erased 75 percent of

[3] Gangloff, Mark, "JPMorgan Would Prefer You Not See This Shameful Rectangle," *The Huffington Post*, updated Jan. 25, 2014.

its equity value; GETCO LLC subsequently acquired the company. UBS is one of several high-profile examples of a rogue trader who was able to amass huge losses.

How Do Companies Manage Operational Risk?

A prudent, widely accepted, and effective model for managing risk is known as the *three lines of defense*[4] (3LOD). While the 3LOD is useful for managing all risk types, it is especially useful for managing operational risk, which is inherently broad and diverse. At a high level:

- The **first line of defense** is typically operational management who manages and takes risk on a day-to-day basis.
- The **second line of defense** sets the guardrails within which the first LOD operates, aggregates risk exposures across the firm, and provides a framework to determine which risks shall be mitigated and which risks will be accepted.
- The **third line of defense** is the internal audit function, which provides independent assurance to the board audit committee on the effectiveness of governance, risk controls and risk management (for all types of risk).

While every company is different, a typical universe of the various operational risk types—the second LOD—for an insurance company will include:

[4] *The Three lines of Defense in Effective Risk Management and Control*, Institute of Internal Auditors Position Paper, January 2013.

- Business resiliency
- Claims processing
- Critical programs
- Data security
- Financial reporting
- Fraud
- Legal/compliance
- Model risk management
- Operational processing
- Vendor risk.

Each of these second LOD areas should be working with the first LOD to establish guardrails, to aggregate exposures at the enterprise level across the various business units, to evaluate and establish controls, to gather metrics, and to analyze trends.

Ideally, each second LOD area has a senior leader responsible for that risk type—for example, a chief resiliency officer for business resiliency. This second LOD risk leader is well-established within the firm as the person who governs the risk and who partners with the business leaders to ensure the risk is effectively managed across the enterprise. While the business leader should have a thorough understanding of that risk within her business area, the second LOD leader should have a thorough understanding of that risk at the enterprise level. To ensure the company is effectively managing each risk, it is vitally important to have an enterprise-level view.

Here is an example to demonstrate the 3LOD, using **model risk** to illustrate each of the LODs:

- **First LOD**: The first LOD builds a complex, predictive pricing model; designs the modeling approach; and determines the modeling assumptions.

- **Second LOD**[5]: The second LOD ensures the data used to build the model is complete and accurate; they validate that the model calculations and approach are sound and that the model, assumptions and data are documented.
- **Third LOD**: Internal audit will periodically (every three to five years) review the model risk management framework developed by the second LOD and test a sample of models to ensure the first LOD has deployed the framework as intended. For example, internal audit will ensure the pricing model was updated according to the schedule, the critical model inputs (e.g., interest rate) were refreshed timely, and change management procedures were followed.

While the 3LOD helps a company to manage operational risk, the 3LOD does not eliminate the risk. It is not possible to eliminate all operational risk. A company who is prudently managing risk will determine when to *mitigate* risk and when to *accept* the risk.

- **Example of risk mitigation**: Companies who rely heavily on technology must have electrical power to run the technology. The need for electrical power may lead to a major investment in a generator—even redundant

[5] In the example above, it should be noted that the second LOD (the model risk governor) will also ensure the firm has an inventory of all of the firm's critical models, including the critical model owners, schedule for updates, etc.

generators—to keep its data centers up and running in the event of widespread and long-term power outages. In this example, the company spends millions of dollars to invest in installing and maintaining industrial generators to mitigate the risk of losing its technology.

- **Example of risk acceptance:** Employees who work in large corporate offices have access to office supplies, e.g., pencils, notepads, batteries, etc. It is likely that some employees—intentionally or not—take home these office supplies for personal use. Thus, corporations are losing thousands of dollars annually on office supplies. Most companies will accept this loss in lieu of setting up a central, controlled environment where employees must register to remove supplies from a centralized location. The cost of the control would exceed the losses so the company accepts this risk.

How Can Companies Identify and Assess Operational Risk?

Insurance companies typically have many tools to quantify insurance and financial risk, e.g., catastrophe models, risk capital models, value-at-risk (VaR) models, etc. There are no models to quantify operational risk, and few insurance companies have gathered loss data that would allow the building of a quantitative model. So how can a company size up and assess the risk? Some tools are:

- Risk control and self-assessments
- Identification of the top operational risks
- Identification of the top emerging operational risks
- Operational risk scenarios.

Risk control and self-assessments. One commonly used tool is the risk control and self-assessment (RCSA) process[6]. Each business area and functional group will perform an RCSA periodically (every two to four years), and may also report the RCSA results to the board of directors. The business area/functional group will identify its top risks (generally four to seven top risks) along with the controls and any action plans that are in place to mitigate and further control each of the top risks. The RCSA generally involves surveying and interviewing the senior-most leaders in each business area/functional group, so it is important that the focus be on the significant risks and not a laundry list of anything that can possibly go wrong. The RCSA serves many purposes:

- The business leader has a periodic process to identify and assess the top risks and the corresponding controls.
- The board gains further insights into each business and functional area as well as the state of risk and controls.
- A firm with a robust RCSA process reinforces risk governance and a strong risk culture.
- The full suite of RCSAs across business groups and functions can inform the top risks for the enterprise.

[6] See, for example, Accenture Risk Management; Deriving Value from a Risk and Control Self-Assessment Program, Oct. 8, 2012.

Identification of top operational risks: It is important for a firm to assess and have a view of the top risks across the enterprise. As this is an inexact science, there is no precise way for determining the top risks. For example, should you prioritize the risks based on severity or based on expected losses? There are some useful sources for collecting the top risks: (1) gather the results from each RCSA; (2) survey the second LOD risk governors about their top risks; (3) interview subject matter experts within the firm. Once you have derived a list of top risks, it will be helpful to interview the executive leaders of the firm to get their input.

Once you have identified the top operational risks across the enterprise, you should then identify the state of the current controls and determine the need for further risk mitigation. Any large investments to control risk will have to be weighed with other desired corporate investments. A formal process for evaluating risk mitigation investments will ensure that executive leaders have the opportunity to accept the risk as it currently is or to invest the dollars to mitigate the risk.

Identification of emerging operational risks: In addition to a prioritized list of your firm's top operational risks, it is important to have a view into what operational risks are lurking around the corner. What new issues are out there that could cause considerable financial loss or reputational damage to your firm? Insurance companies should have a process for identifying emerging risks in each major risk area (insurance, financial, operational) and for aggregating these across the enterprise to determine emerging risks that could damage the firm.

Analyze scenarios: One way to quantify operational risk events is through scenario analysis. Ideally, for each of the firm's top operational risks, one will develop a set of assumptions and quantify the financial loss. For example, if a cyber-breach is one of the firm's top operational risks, a set of assumptions might include: (1) number of records stolen; (2) number of days the systems will be inaccessible while the environment is cleaned; (3) any impact to vendors/agents/business partners; (4) revenue lost; (5) fines paid; (6) forensic costs to clean the systems and prevent further break-ins, etc.

Quantifying the scenarios around each of the top risks will reinforce or change the priority order of the top risks. Walking through a "real" scenario will also provide insights into the current controls, and it will inform further action plans, investments and resource needs to prevent the scenario from happening or to minimize the losses if the scenario does happen.

How Do Companies Monitor, Measure and Report on Operational Risk Exposures?

It is an important tenet of risk management that a firm should have a framework for identifying, assessing, monitoring, measuring, and reporting on risk. Some common tools include:

- Monthly (or quarterly) dashboards
- A loss collection process based on an operational risk library

- An operational risk management (ORM) system.

Dashboard: Operational risk is disparate and distributed throughout the firm (as shown earlier on page 5). A dashboard that provides a few key metrics from each operational risk area can provide insights into trends at the enterprise level. Key metrics will ensure that executive management periodically reviews exposures in each area. The dashboard could include metrics such as the number of processing errors, hours of system downtime, number of compliance failures, number of firewall breaches, percentage of business resiliency plans that are out of date, etc.

Loss collection and data libraries: A company should develop a loss collection process to collect and analyze data on both internal and external operational risk events. This allows the firm to understand risk exposures and the effectiveness of internal controls by comparing loss results over time. It can also lead to a comparison of the cost of losses from operational loss events vs. the cost of controlling the losses. Comparing (1) the cost of losses vs. (2) the cost of controlling the losses can provide insights into overspending or under-spending.

In order to effectively collect losses, the company should develop an operational risk library to segment the losses. Basel has seven risk types[7]:

1. Internal fraud
2. External fraud
3. Employment practices and workplace safety

[7] Operational Risk Data Collection Exercise—2002, Basel Committee on Banking Supervision.

4. Clients, products and business practices
5. Damage to physical assets
6. Business disruption and system failures
7. Execution, delivery and process management.

Ideally, the company's operational risk library will map into these seven Basel risk types because this will facilitate industry benchmarking. These are firms who collect and aggregate industry data, which may be used for benchmarking a firm's operational losses.

While banks are required to record operational risk events and losses, it is not yet a regulatory requirement for insurance companies. However, it is a best practice to collect loss data as this will allow for the understanding of the cost of operational risk—both the cost of the actual loss events as well as the cost of controlling and mitigating future losses. The cost of controlling and mitigating future losses will include the expenses of the departments overseeing the risk, i.e., the second LOD areas, as well as investments made in mitigating future losses, e.g., investments in firewalls to prevent cyber-attacks or investments in generators to provide uninterrupted power supplies.

ORM systems: ORM systems—also known as governance, risk, and compliance (GRC) systems—have grown in popularity as companies look for solutions to manage risks, automate operational risk processes, and demonstrate compliance. These systems provide an efficient way of managing data by eliminating inefficient spreadsheet tracking.

While spreadsheets are useful for math calculations and graphing purposes, they are frequently misused for database tracking. For example, assume your company wants to understand the number of security incidents by month in each department, i.e., lost/stolen laptops, confidential info sent to the wrong address, etc. A typical response would be to require each department to set up a spreadsheet with basic information to track this data. Even if each department starts with a common spreadsheet format, this format will change over time as managers in each department ask specific questions that require new fields to be captured. One year later when it is time to aggregate the data across all departments, it will be very difficult to add the incidents due to differing spreadsheet formats, different definitions of an incident, staff who have left and the spreadsheet was abandoned in that department, etc. A GRC would be consistent across all departments and would force standardization of processes.

Common uses of GRCs include loss data tracking, risk policy management, business continuity tracking, internal audit applications, data security, compliance and regulatory change monitoring, etc. These tools are generally inexpensive and easily configurable with many out-of-the-box applications. Ideally, a company will have one GRC to facilitate the sharing and aggregation of data across all operational risk types.

While operational risk is likely one of the most significant risks faced by your organization, it is not well-understood nor is there a standard definition accepted within insurance companies. New insurance regulations such as ORSA and Solvency II will bring operational risk into the mainstream, so insurance companies will be required to provide the framework they use for managing operational risk. Companies who have or wish to build a strong risk culture will take this on even in the absence of regulatory requirements because it is necessary for a well-managed firm.