Operational Risk – An Enterprise Risk Management Presentation

Margaret Tiller Sherwood
FCAS, ASA, MAAA, FCA, CPCU, ARM, ERMP, CERA
President
Tiller Consulting Group, Inc.

Session Number: TBR4

Joint IACA, IAAHS and PBSS Colloquium in Hong Kong
www.actuaries.org/HongKong2012/
Operational Risk – An ERM Presentation

Definition
Types of Operational Risk
Operational Risk Management Framework
Quantification
Mitigation
Monitoring
Risk Identification and Mitigation Examples
Words of Wisdom
Definition

Basel II – Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk, but excludes strategic and reputation risk.
Definition

Who are these people?
What does this have to do with us?
Definition

Basel Committee on Banking Supervision – Committee of banking supervisory authorities that provides a forum for cooperation on bank supervisory matters and encourages convergence towards common approaches and standards. It also frames guidelines and standards for banks and bank supervisors.

Basel Accords – Recommendations on banking laws and regulation
Definition

Basel II was intended to create an international standard for banking regulators to control how much capital banks need to put aside to guard against the types of financial and operational risks banks face.

Basel II lists three types of risk:
  Credit risk
  Market risk
  Operational risk

What about liquidity risk?
Definition

Market liquidity is the risk that a security can not be sold at all or quickly enough to prevent a loss.

Market liquidity risk is a type of market risk. It is addressed in Basel III.

Funding liquidity risk is the risk that liabilities can not be met when due.

Funding liquidity risk is an operational risk.
Definition

Solvency II codifies and harmonizes EU insurance regulation.

Solvency II definition - *Operational risk means the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events. [It] shall include legal risks, and exclude risks arising from strategic decisions, as well as reputation.*
Definition

Legal risk - risk of loss due to legal actions or uncertainty in the applicability or interpretation of contracts, laws, or regulations. Included.

Strategic risk – risk arising from decisions concerning a company’s direction. Excluded.

Reputational risk - risk related to the trustworthiness of the company. Excluded.
Definition

Better definition - *Operational risk is the risk arising from execution of a company’s business function.*

This focuses on the risks arising from people, processes, and systems.

Note that it includes external events that affect a company’s operations.
Definition

Operational risk does not include strategic risk – the risk that arises from decisions concerning a company’s objectives.

Reputational risk may arise from operational risk but is not, in and of itself, an operational risk. It also can arise from credit risk, market risk, and strategic risk.

Operational risk is not used to generate profit, whereas market risk, credit risk, and strategic risk can do so.
Types of Operational Risk

**Basel II List**

**Internal fraud** – misappropriation of assets, tax evasion, intentional mismarking of positions, bribery

**External fraud** – theft of information, hacking damage, third party theft and forgery

**Employment practices and workplace safety** – discrimination, workers’ compensation, employee health and safety

**Clients, products, and business practice** – market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning

**Damage to physical assets** – natural disasters, terrorism, vandalism

**Business disruption and system failures** – utility disruptions, software failures, hardware failures

**Executive, delivery, and process management** – data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets

Legal risk is in several of these categories.
Types of Operational Risk

Operational risk losses usually are idiosyncratic to a particular institution.

Operational risk losses most commonly are from a failure of internal controls.

Internal operational risk losses arise from errors and ineffective operations.
Operational Risk Management Framework

Basel II

Risk organizational and governance structure

Policies, procedures and processes

Systems used by a bank in identifying, measuring, monitoring, controlling and mitigating operational risk

Operational risk measurement system (ORMS) – systems and data used to measure operational risk to estimate the operational risk charge
Operational Risk Management Framework

Enterprise Risk Management Steps

1. Identify risks
2. Describe and/or quantify risks
3. Decide how to mitigate risks
4. Implement decisions
5. Monitor results of decisions and make changes as needed

Communication is key.
Operational Risk Management Framework

Basel II differentiates between verification and validation.

Verification tests the effectiveness of the overall ORMF and tests ORMS validation processes to ensure they are independent and implemented consistent with bank policies.

Validation ensures that the ORMS is sufficiently robust and provides assurance of the integrity of inputs, assumptions, processes, and outputs.
Operational Risk Management Framework

Essential elements for verification and validation:

Independence

Capacity – adequately staffed with adequate resources

Professional competence and due diligence
Quantification

Basel Committee on Banking Supervision “Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches” June 2011

Operational risk data categories for Advanced Measurement Approaches:

- Internal loss data (ILD)
- External data (ED)
- Scenario analysis (SA)
- Business environment and internal controls factors (BEICF)
Quantification

It all starts with scenarios.

Ask “What if…?”

Don’t know what internal and external data to collect unless you have some idea of what scenarios you need to look at.

Data includes qualitative as well as quantitative.

Qualitative data sometimes is more important than quantitative, particularly when there are recent changes.
Quantification

Internal Loss Data (ILD)

Internal to the organization

Used to estimate loss frequencies

Used to inform the severity distribution(s)

Serves as input into the scenario analysis
Quantification

External Data (ED)

External to the organization

Used to estimate loss severity, particularly for the tail

May be from a consortium of like members

(Association of British Insurers’ Operational Risk Consortium – www.abioric.com)
Quantification

Scenario Analysis (SA)

Scenario outputs form part of the input into the Advanced Measurement Approach model

Qualitative

Produce range of results

Quantify uncertainty arising from scenario biases – This is a significant challenge.
Quantification

Business Environment and Internal Controls Factors (BEICF)

Highly subjective

Often used as indirect input into the quantification framework

Often used as an ex post adjustment to model output
Mitigation

Goals

Have business continuity

Mitigate financial loss

Reduce reputational risk
Mitigation

The size of loss a company is willing to accept compared to the cost of correcting errors or improving operations determines its operational risk appetite.

Most effective means of reducing operational risk are sound policies, practices, and procedures for internal events and insurance for external and some internal events.
Mitigation

Low frequency, low severity – may do nothing.

Low frequency, high severity – analyze by scenario testing. Handled by planning for these in advance and/or by financing risk such as by purchasing insurance.

High frequency, low severity – may do nothing. However these can accumulate to the point where the severity becomes larger, such as if it triggers a loss of reputation.

High frequency, high severity – take risk control measures. May finance risk such as by purchasing insurance.
Mitigation

Insurance companies sell products that mitigate others’ operational risks.
Mitigation

Basel Committee on Banking Supervision - “Principles for the Sound Management of Operational Risk” June 2011

Internal controls embedded in day-to-day operations are designed to ensure to the extent possible that:

Activities are efficient and effective

Information is reliable, timely and complete

The entity is compliant with applicable laws and regulation.
Mitigation

Three lines of defense:

- Business line management
- An independent corporate operational risk management function
- An independent review
Monitoring

Key Performance Indicator (KPI) – Are we achieving our desired level of performance?

Key Risk Indicators (KRI) – How is our risk profile changing and is it within our desired tolerance levels?

Key Control Indicators (KCI) – Are our organization’s internal controls effective?
Risk Identification and Mitigation Examples

Fine Dining Restaurant

Family owned
Open only for dinner Monday through Saturday
Seats 80 at a time for two seatings a night
Private party room upstairs
Owner is one of the managers on duty but is also a chef
Has a general manager and one other manager on duty
Has two part-time office staff and one cleaner
Has an Executive Chef, two Line Chefs, one Dessert Chef
Has two expediters and two dishwashers
Has three captains, six waiters, six bussers, and one bartender
Has one hostess and one coat checker
Subcontracts car parking
Risk Identification and Mitigation Examples

Fine Dining Restaurant

Internal policies, practices, and procedures
- What can go wrong in the front of the house?
- What can go wrong in the kitchen?
- What can go wrong in the office?
- What can go wrong elsewhere?
- What communication problems can there be?

External events
- What could negatively affect the restaurant?
Risk Identification and Mitigation Examples

Large Taxi Company

In major city
Owned by one private investor
No Board of Directors
One garage location
Owns 500 cabs
Has 1,000 drivers
Has 20 mechanics in own repair shop
Has own gas station and car wash
Has 5 dispatchers
Has 10 office staff including CEO, COO, and CFO positions
Risk Identification and Mitigation Examples

Large Taxi Company

Internal policies, practices, and procedures
- What can go wrong on the streets?
- What can go wrong in the repair shop?
- What can go wrong with the gas station and car wash?
- What can go wrong with dispatching?
- What can go wrong in the office?
- What can go wrong elsewhere?
- What communication problems can there be?

External events
- What could negatively affect the company?
Risk Identification and Mitigation Examples

Insurance Company

Privately held
Much of board is family members
Writes automobile liability and physical damage for taxis in large city
Recently had large business expansion
Is moving from low-tech to high-tech back office
Uses independent agents to write business
Risk Identification and Mitigation Examples

Insurance Company

Internal policies, practices, and procedures
   What can go wrong with the agents?
   What can go wrong with customer service?
   What can go wrong with underwriting?
   What can go wrong with claim handling?
   What can go wrong with data processing?
      Increased inefficiency due to data overload
      Compliance risk if data not protected
      Privacy risk
      Security risk
Risk Identification and Mitigation Examples

Insurance Company

Internal policies, practices, and procedures (continued)

What can go wrong with accounting?
What can go wrong with investing?
What can go wrong with reinsurance?
What can go wrong with the Board of Directors?
What can go wrong with the owners?
What can go wrong elsewhere?
What communication problems can there be?

External events

What could negatively affect the company?
Risk Identification and Mitigation Examples

Insurance Company

Operational risk losses usually are idiosyncratic to a particular institution.

Very highly automated back-office systems – exposure to IT operational risks

Low tech back office – exposure to people and process operational risks
Words of Wisdom

Strategic decisions affect operations.

Have an “open door” policy.

Manage by walking around.

“Good reason” versus “real reasons.”

When someone presents a problem, they must also present a possible solution or be willing to participate in finding a solution.
Words of Wisdom

Some processes need to be “hard-wired” in: no exceptions.

Manage by exception. Use those to improve processes and systems.

Allow people to make exceptions that are in the company’s long-term best interest.

Cross train.
Words of Wisdom

Be aware of what is going on outside the company:
- Clients/customers
- Service providers
- Competitors
- Related industries
- General population – demographics, work environments, socially
- Technology innovation
- Accounting standards
- Politically
- Judicially
- Legislatively
- With the country in general
- With the world in general
Words of Wisdom

Be more proactive than reactive.

Keep an open mind.

See what is really there.

Be prepared.

Be flexible.

Communicate, communicate, communicate.
Definition - *Operational risk is the risk arising from execution of a company’s business function.*

Types of Operational Risk

Operational Risk Management Framework

Quantification

Mitigation

Monitoring

Risk Identification and Mitigation Examples

Words of Wisdom
Operational Risk – An ERM Presentation

Margaret Tiller Sherwood
FCAS, ASA, MAAA, FCA, CPCU, ARM, ERMP, CERA
President

Tiller Consulting Group, Inc.
10401 Litzsinger Road
St. Louis, Missouri 63131
USA
www.tillerconsultinggroup.com

Phone: 1 314 567 7480
Fax: 1 314 567 4199
msherwood@tillerconsultinggroup.com