12. Operational Risk: Identification, Measurement, Management, and Control

Asia Pacific Economic Cooperation Forum –
Financial Regulators Training Initiative –
Bank Analysis and Supervision Seminar

Manila, Philippines May 2014

Operational Risk
Definition

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

The definition includes legal risk. *(Note that some kinds of legal risk like fines and penalties may be categorized as compliance risk.)*

Losses can be direct (monetary) or indirect (effects of negative media coverage, loss of customers).

Operational Risk
Sources

- People… make mistakes, act unethically or carelessly
- Processes… sometimes not adequate
  …sometimes not followed
- Systems… have limitations
  …can have programming errors
  …can have security issues
  …can be "down" or unavailable
- External events… aren't preventable, but sometimes the consequences are

Operational Risk *Sources* (1 of 4)

People

ChoicePoint, a data aggregation company, had to acknowledge selling personal data on over 140,000 customers to an identity theft ring

Resulted in over $30m in fines and costs – company is no longer independent

Operational Risk *Sources* (2 of 4)

Processes

Citi (one of the largest US banking groups) confirmed that UPS (a logistics and delivery service) had lost computer tapes containing information on nearly 4 million customers while they were in transit to the bank's credit bureau

Bank of America admitted to losing tapes with customer identifiers and account information on 1.2 million. It also announced a USD 4 billion accounting error in 2Q 2014.

Operational Risk *Sources* (3 of 4)

Systems

- **Target Corporation,** a large American retailer, was hacked in November 2013, ultimately resulting in the accessing by a criminal network of 40 million credit-card numbers, along with 70 million addresses, phone numbers, and other pieces of information.
- The retailer has been criticized for ignoring warnings from its hacker-detection tools. The CEO resigned in early May 2014.

Operational Risk *Sources* (4 of 4)

External events

- Natural disasters
- Terrorism

Cantor Fitzgerald, a U.S. Government securities dealer, lost 658 out of its 960 New York employees in 9/11 attacks

It survived as a business because it had an electronic trading subsidiary, and also was able to reconfigure its system so trades went through London instead of New York

Some other consequences of operational risk events

Investor punishment: **One study showed that the negative impact on market value over a 120-day period following the announcement of an operational risk loss is roughly 12 times the amount of the actual loss**

Regulatory sanctions: **Regulators required one bank in Singapore to increase its capital by an additional SGD 200 million following a data-center failure that lasted only seven hours, even though customers were compensated.**

Operational Risk: *Spectacular News* (some trading examples)

- **Bruno Iksel, aka "London Whale,"** JP Morgan Chase, lost more than $2b in 15 days

Total Losses: $6.2 billion

- **Jerome Kerviel**, Soc Gen, bet 200% of the bank's capital, or €50 b

Losses: €4.9 billion

- **John Rusnak**, AIB, bet 3,000 times his $2.5 m trading limit

$700 million

- **Yasuo Hamanaka**, Sumitomo, held 5% of the global copper market

$2.6 billion

Another way of categorizing Operational Risk – by Event Types

- Event type A: Internal Fraud
- Event type B: External Fraud
- Event type C: Employment Practices and Workplace Safety
- Event type D: Clients, Products, and Business Practices
- Event type E: Damage to Physical Assets
- Event type F: Business Disruption and System Failure
- Event type G: Execution, Delivery, and Process Management

What are the most common Event Types? Which cause the biggest losses?

- Event type A: Internal Fraud
- Event type B: External Fraud
- Event type C: Employment Practices and Workplace Safety
- Event type D: Clients, Products, and Business Practices
- Event type E: Damage to Physical Assets
- Event type F: Business Disruption and System Failure
- Event type G: Execution, Delivery, and Process Management

Note: The data were compiled from a sample of 66 leading banks in all regions of the world, from 2006-2010

- ***Number*** of instances
  - **G:** 37% of all instances (158,000 total instances of loss amounting to €20,000 or more)
  - **B:** 35% of all instances
- ***Monetary volume*** of losses
  - **D:** 38% of losses (total losses €53.8 billion)
  - **G:** 32% of losses

Taking a look at the important Event Types in detail

- **Event type B: External Fraud**
  - Client misrepresentation of information
  - Theft
  - Loan fraud
  - Cybercrime
  - Forgery
  - Check fraud
  - Theft of information
  - Fraudulent transfer of funds
  - Payment fraud

Taking a look at the important Event Types in detail

- **Event type D: Clients, Products, and Business Practices**
  - Regulatory violation
  - Compromised customer information
  - Fiduciary breach
  - Mis-selling products, ignoring customer suitability
  - Noncompliance with anti-money laundering regulations

Taking a look at the important Event Types in detail

- **Event type G: Execution, Delivery, and Process Management**
  - Inaccurate/incomplete contract
  - Transaction, processing, data entry error
  - Staff error in lending process
  - Mismanagement of account assets
  - Model risk
  - Pricing error
  - Failure of external supplier/vendor
  - Failure to follow procedures
  - Lost or incomplete loan documentation
  - Tax noncompliance

In which business lines do we find the most operational risk?

- Corporate Finance
- Trading and Sales
- Retail Banking
- Commercial Banking
- Clearing
- Agency services
- Asset management
- Retail brokerage
- Private banking
- Corporate items
- Across multiple lines

In which business lines do we find the most operational risk?

- Corporate Finance
- Trading and Sales
- Retail Banking
- Commercial Banking
- Clearing
- Agency services
- Asset management
- Retail brokerage
- Private banking
- Corporate items
- Across multiple lines

- ***Number of losses:***
  - 1. Retail banking 59%
  - 2. Trading and sales 11%

- ***Monetary volume of losses:***
  - Retail banking 37%
  - Trading and sales 26%

Operational Risk

Risk Management Environment

Four steps in Ops Risk management

Identification and Assessment

Monitoring and Reporting

Control and Mitigation

Business Resiliency and Continuity

Four Steps in Ops Risk Management

Identification and Assessment

- **Conditions that increase exposure to operational risk**
  - Bank engages in new activities or develops new products
  - Bank enters unfamiliar markets
  - Bank implements new business processes or ICT systems
  - Bank has far-flung operations geographically distant from HQ
  - New activities transition from low level to key revenue drivers
  - High staff turnover
- ***Under these circumstances, banks have to be especially alert!***

Four Steps in Ops Risk Management
Identification and Assessment (1/5)

- **Tools to use in identifying and assessing Ops Risk:**
  - Audit findings (can uncover inherent risk or vulnerabilities)
  - Internal loss data collection and analysis
    - Categorize actual losses according to Event Type and Business Line
    - Quantify losses
  - External loss data collection and analysis
    - Use industry studies to determine most common/most costly events
    - Stay up to date on actual bank OR events as reported in media
  - Risk assessments
    - Bank reviews its processes against a ***library of potential threats and vulnerabilities*** and considers potential impact

Four Steps in Ops Risk Management
Identification and Assessment (2/5)

- **Tools to use in identifying and assessing Ops Risk:**
  - Business process mapping (can show exact points of possible vulnerability)
  - Scenario analysis:
    - Purpose is to identify high-impact, low-frequency events in business units
    - Business unit heads may not like this!
    - Requires putting estimated value and probability of occurrence on possible events
    - May lead to higher capital requirements for business unit

Four Steps in Ops Risk Management
Identification and Assessment (3/5)

- **Tools to use in identifying and assessing Ops Risk:**
  - Scenario analysis (continued)

"Are you saying that you want us to figure out how to lose $10 million?" – business line head

Goal of scenario analysis is to identify potential scenarios that could create losses above some threshold (say, $10 million)

Four Steps in Ops Risk Management
Identification and Assessment (4/5)

- **Tools to use in identifying and assessing Ops Risk:**
  - Scenario analysis (continued)

The risk of catastrophic loss is difficult to measure by other means.

Has some drawbacks:

Humans are poor at estimating probabilities of catastrophic events (also known as "tail Events)

Managers may be shy about discussing potential vulnerabilities in their business units

Four Steps in Ops Risk Management
Identification and Assessment (5/5)

- **Tools to use in identifying and assessing Ops Risk:**
  - Scenario analysis (continued)

Example of successful scenario analysis:

Participants identified a large loss due to a duplicate wire sent overseas that was not recoverable.

Expected loss was $10 million and probability estimated as one event every five years.

Four Steps in Ops Risk Management
Monitoring and Reporting

- **Senior management MUST regularly monitor operational risk profiles and material exposures to losses**

- **Reports on OR to senior management should include:**
  - **Actual losses**
  - **Inventory of possible events and expected losses**
  - **Narrative of internal and external vulnerabilities**
  - **Progress on correcting gaps**

Four Steps in Ops Risk Management
Control and Mitigation (1/2)

- **Internal controls are key to avoiding operational risk events**
  - **Code of conduct**
  - **Segregation of duties and dual control (to avoid concealment of losses, errors, or other inappropriate actions)**
  - **Clear authorities, approval processes**
  - **Monitoring for adherence to limits**
  - **Safeguards for access to and use of bank assets, records**
  - **Appropriate staffing level and training**
  - **Identification of business units where activity seems excessive**
  - **Vacation policy (absence for two consecutive weeks)**

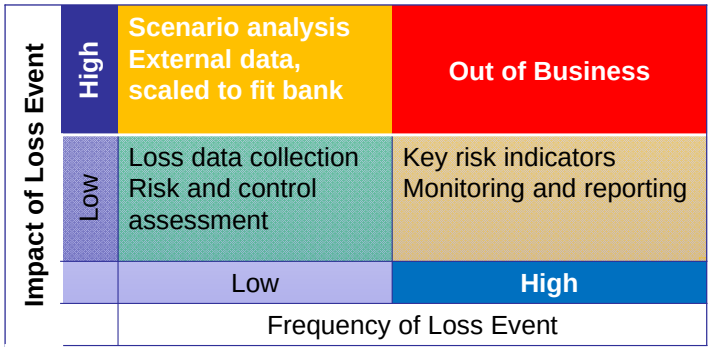
Four Steps in Ops Risk Management
Control and Mitigation (2/2)

- **Control over ICT risks and outsourcing risks**
  - **Business continuity, disaster recovery**
  - **Careful selection of service providers**
  - **Contingency plans in case of non-performance by service provider**

- ***Transferring risk*** is sometimes an option
  - Insurance
  - ***Insurance is a complement, not a substitute, for internal controls!***

Operational Risk
Some Summary Remarks

- Categorize potential event losses by ***impact*** and ***frequency***



Operational Risk
Some Summary Remarks

- Have a ***governing structure*** for Ops Risk

Business units, subsidiaries, support functions	Risk identification		
CFO's office (Operational Risk Section)	Determination of risk owner and creation of Top Risk List		
Business units, subsidiaries, support functions	Key Risk Indicator identification	Creation of mitigation plans	
Operational Risk Committee	Mitigation of risk	Acceptance of risk	Transfer of risk
Business units, subsidiaries, support functions	Implementation of mitigation		Outsourcing or Insurance

Every risk must have an owner!