

# PRMIA 3C and 3D

July 1, 2013

## 1 PRMIA 3C1

Operational Risk Management Framework

3.C.1.1. Introduction to Operational Risk Management 3.C.1.2. Evidence of Operational Failures 3.C.1.3. Defining Operational Risk 3.C.1.4. Types of Operational Risk 3.C.1.5. Aims and Scope of Operational Risk Management 3.C.1.6. Key Components of Operational Risk 3.C.1.7. Supervisory Guidance on Operational Risk 3.C.1.8. Identify Operational Risk - The Risk Catalogue 3.C.1.9. Operational Risk Assessment Process 3.C.1.10. Operational Risk Control Process 3.C.1.11. Conclusion.

### Learning Outcome Statement

The candidate should be able to:

- Explain the relevance of Operational Risk Management (ORM)
- Describe how to develop and apply operational risk models
- Describe the various ORM tools
- Describe the Top-down models
- Describe the Bottom-up models
- Describe the Key Attributes of the ORM Framework
- Describe the Integrated Economic Capital Model
- State the objectives of an ORM programme
- Demonstrate Risk Transfer
- Discuss the IT Outsourcing case study

### **3.C.1.1. Introduction to Operational Risk Management**

### **3.C.1.2. Evidence of Operational Failures**

### **3.C.1.3. Defining Operational Risk**

The Basel Definition is mainly for capital adequacy purposes.

### **3.C.1.4. Types of Operational Risk**

### **3.C.1.5. Aims and Scope of Operational Risk Management**

### **3.C.1.6. Key Components of Operational Risk**

(i) Core Operational Capability (ii) People (iii) Client Relationships (iv) Transactional and booking systems (v) Reconciliation and accounting (vi) Change and new activities (vii) Expense and Revenue Volatility

### **3.C.1.7. Supervisory Guidance on Operational Risk**

Four main themes 1) Developing an appropriate risk management environment 2) Risk management identification, assessment, monitoring, mitigation and control 3) Role of supervisors 4) Role of disclosure

### **3.C.1.8. Identify Operational Risk - The Risk Catalogue**

### **3.C.1.9. Operational Risk Assessment Process**

Step 1 Input to Risk C Step 2 Risk Assessment Scorecard Step 3 Review and Validation Step 4 Outputs of Risk Assessment Process

### **3.C.1.10. Operational Risk Control Process**

Failures in risk control due to

- 1) lax management processes
- 2) Inadequate assessment of risk ( on and off balance sheet activities)
- 3) Lack of transparency

- 4) Inadequate communication of information between levels of management
- 5) Inadequate or ineffective audit and compliance programmes

### **3.C.1.11. Conclusion**

This section discusses operational risk process models. By better understanding business processes we can find the sources of risk and often take steps to re-engineer these processes for greater efficiency and lower risk.

Top-down approaches tend to be those an external analyst could use with public information. Armed with an income statement and market data, most of them (e.g., multi-factor model) can be performed by a third-party. Consequently, they are limited but easier to conduct. Bottom-up approaches require an "inside job:" internal data, management interviews. Consequently, they are generally superior but more difficult (data intensive): they are diagnostic, predictive, and often revealing of causality. A key difference is that "top down" approaches do not differentiate between HFSL/LFHS losses but bottom-up approaches can indeed distinguish between HFSL/LFHS losses.

## **2 PRMIA 3C2**

### **3.C.2 Operational Risk Process Models**

1. Introduction
2. The Overall Process
3. Specific Tools
4. Advanced Models
5. Key attributes of the ORM framework
6. Integrated Economic Capital Model
7. Management Actions
8. Risk Transfer
9. IT outsourcing.

#### **3.C.2.1. Introduction**

The focus on operational risk has been driven by a number of important factors. 1) Corporate disasters 2) Regulatory actions 3) Industry Initiatives 4) Corporate programs 5) Technology developments.

#### **3.C.2.2. The overall process**

**Step 1:** Established the objectives and requirements of key stakeholders

**Step 2:** Identify the core processes that support these objectives.

**Step 3:** Define performance and risk metrics, including goals and MAPS.

**Step 4:** Implement organizational and risk mitigation strategies.

### **3.C.2.3. Specific Tools**

Loss Incidence Database Control Self Assessment: Internal Subjective Assessment Risk Mapping Key Risk Indicators (KRIs) Key Risk Drivers are ex post indicators of operational risk performance. Training hours, number of versus manual processes, time to fill open positions, and time to resolve outstanding audit findings. As such, KRDs can be thought of as controllable factors that will influence future KRIs.

### **3.C.2.4. Advanced Models**

When ORM was in its infancy. There was two schools of thought. The first was that you can not manage what you can not measure. The other school believed that operational Risk cannot be Quantified effectively, and they focussed on more humanistic qualitative approaches such as self assessment, riskmaps , and audit findings. **3.C.2.4.1 Top Down models**

Implied Capital model Income volatility model. Economic pricing. model Analogue model. **3.C.2.4.2 Bottom Down models**

(Page 382) Revenue multiplier. This is a top down estimate of the amount of operational Risk capital Required by a business or operating unit.

### **3.C.2.5 Key Attributes of the ORM Framework**

### **3.C.2.6 Integrated Economic Capital Models**

### **3.C.2.7 Management Actions**

### **3.C.2.8 Risk Transfer**

### **3.C.2.9 IT Outsourcing**

1. Stakeholder Objectives
2. Key Processes
3. Performance Monitoring
4. Risk Mitigation

### 3 PRMIA 3C3

#### 3.C.3 Operational VaR

3.C.3 Operational VaR 3.C.3.1. The "Loss Model" approach The Severity distribution 3.C.3.2. The Frequency Distribution

ama: advanced measurement approach 3.C.3.1. The "Loss Model" approach Operational Risk Matrix

ORC is held to cover all losses. The ORC is thus defined using the VaR matrix, for some risk horizon and at some percentile. The Basel Committee recommend 99.9

The Frequency distribution

: expected loss frequency N: expected total number of events during the risk horizon p: expected loss probability

Poisson distribution negative binomial distribution Estimating the poisson frequency from historical data The Severity distribution

Example Assume the following operational process:

A Bernoulli distribution characterizes the frequency of losses. The probability

The loss severity is characterized by a PMF:  $P(-\$50,000 \text{ loss}) = 2\%$ ,  $P(-\$30,000$

(Note this is a discrete distribution where the outcomes are mutually exclusive

99% Operational VaR = Unexpected loss = Loss @ 99% - Expected Loss (EL).

Start with the worst loss and works backwards:

$P(\$50,000 \text{ loss}) = (5\%)(2\%) = 0.1\%$

$P(\$30,000 \text{ loss}) = (5\%)(18\%) = 0.9\%$

Cumulatively, that is 1% ( $0.1\% + 0.9\% = 1.0\%$ ). So, the loss @ 99% is \$30,000

The expected loss =  $5\% * [(2\%)(50,000) + (18\%)(30,000) + (24\%)(10,000) + (56\%)(5,000)]$

So, the 99% Operational VaR = \$30,000 (loss @ 99%) - \$580 = \$29,420

Similarly, the 95% Operational VaR = \$4,420

99% Operational VaR = Unexpected loss = Loss @ 99% - Expected Loss (EL).

Start with the worst loss and works backwards:

$$P(\$50,000 \text{ loss}) = (5\%)(2\%) = 0.1\%$$

$$P(\$30,000 \text{ loss}) = (5\%)(18\%) = 0.9\%$$

Cumulatively, that is 1% ( $0.1\% + 0.9\% = 1.0\%$ ). So, the loss @ 99% is \$30,000

$$\text{The expected loss} = 5\% * [(2\%)(50,000) + (18\%)(30,000) + (24\%)(10,000) + (56\%)(5,000)]$$

$$\text{So, the 99\% Operational VaR} = \$30,000 \text{ (loss @ 99\%)} - \$580 = \$29,420$$

$$\text{Similarly, the 95\% Operational VaR} = \$4,420$$

VaR is not the worst loss

This is the operational LDA approach: a loss frequency distribution is compounded

I called the discrete severity a PMF versus a PDF per Gujarati definitions. Known as the expected loss (EL). The VaR is the worst loss

If you look at the EditGrid below, the two distributions compound into a single PMF. Next to it, the running total is the CDF. Each discrete outcome in the PDF is simply the product of [Frequency][Severity]. Notice the analogy to credits where  $EL = PD * LGD$ . In operational terms,  $EL = PE$  (probability of event, frequency) \* LGE (loss given event, severity). Finally, back to Gujarati, that's a joint probability.

#### 3.C.3.2. The Frequency Distribution Defined risk horizon

The Probability of a loss event can be translated into the loss frequency denoted  $\lambda$ . the product of the total number of events during the risk horizon Loss frequency is a discrete random variable

Binomial frequency can only be used when a value for N is specified

Poisson Distribution

negative binomial distribution

$$b(n) = \frac{n!}{(n-1)!1!} + 1 +$$

Choosing the best functional form is not a main source of model risk

#### 3.C.3.3. The Severity Distribution

Lognormal distribution for loss severity L has the density function.

High frequency risks can have severity distributions that are relatively lognormal, but low frequency risks can have severity distributions that are

too skewed and leptokurtic to be well captured by the lognormal density function.

$\Gamma(\cdot)$  denoted the gamma function  $B(\cdot)$  denotes the Bessel function of the first kind.

#### Extreme Value Theory

It is debatable that fitting a generalized Pareto distribution to a sparse and fragmented data set yields anything useful Peaks over Thresholds model applies when losses over a high and predefined threshold are record.

The internal measurements approach (IMA) Gamma. expected annual loss  $N$  is a volume indicator  $p$  is the expected number of losses gamma is a multiplier that depends on the operational risk type. The loss distribution is binomially distributed and loss severity is not regarded as a random variable standard deviation of annual loss.

Loss Distribution Approach ( LDA ) will always increase the ORC. ORC is measured by a VaR metric and is either unexpected loss at percentile or the percentile itself depending on whether or not the expected losses were provisioned.

### **3.1 3.C.3.1**

### **3.2 3.C.3.2**



## 4 PRMIA 3D1

This paper introduces the candidate to the dangers of not having up-to-date, clean, and available data in order to make risk management decisions, and a remedial path to achieving the best possible assurance of accurate data. Enterprise Information Risk Learning Outcome Statement

### 4.1 Learning Outcomes

The candidate should be able to:

- 1 Describe the dangers and risks inherent in risk models, transparency, and risk
- 2 Explain some of the causes of poor data
- 3 Construct a clear plan for solving the problem of data quality
- 4 Demonstrate an understanding of the 8 criteria, and priorities for analyzing
- 5 Explain, and demonstrate, the need for holistic Risk Information Management E
- 6 Describe the 7 components of a Data Management Framework, and a Logical Data
- 7 Discuss the 5 Critical Success Factors of implementing a Risk Information Man
- 8 Identify the 4 components of AS-IS to TO-BE environments

## 5 PRMIA 3D2

This section consists of 2 papers, which provide details of factors inherent in the financial crisis of 2007-9 and identify some of the causes, and suggestions for remedial actions.

### Learning Outcome Statement

The candidate should be able to: Discuss the concept of zero-sum relative to financial instruments, and risk engineering. Discuss the function of the intermediaries of the financial system Explain the importance of the balance of the component parts of the financial services industry Describe how uncertainty can unbalance the financial system Discuss the role played by government in financial crises Discuss how infusions of cash into the monetary system stopped the system from seizing up Demonstrate how limited memory, and disaster myopia, were prevalent in the Golden Decade Explain networked risk externalities can, and did, build up in a short period of time

Discuss the apparent role conflicts between risk managers and risk takers, and their management, and the regulators

**5.1 3.D.2.1**

**5.2 3.D.2.2**

**5.3 3.D.2.3**