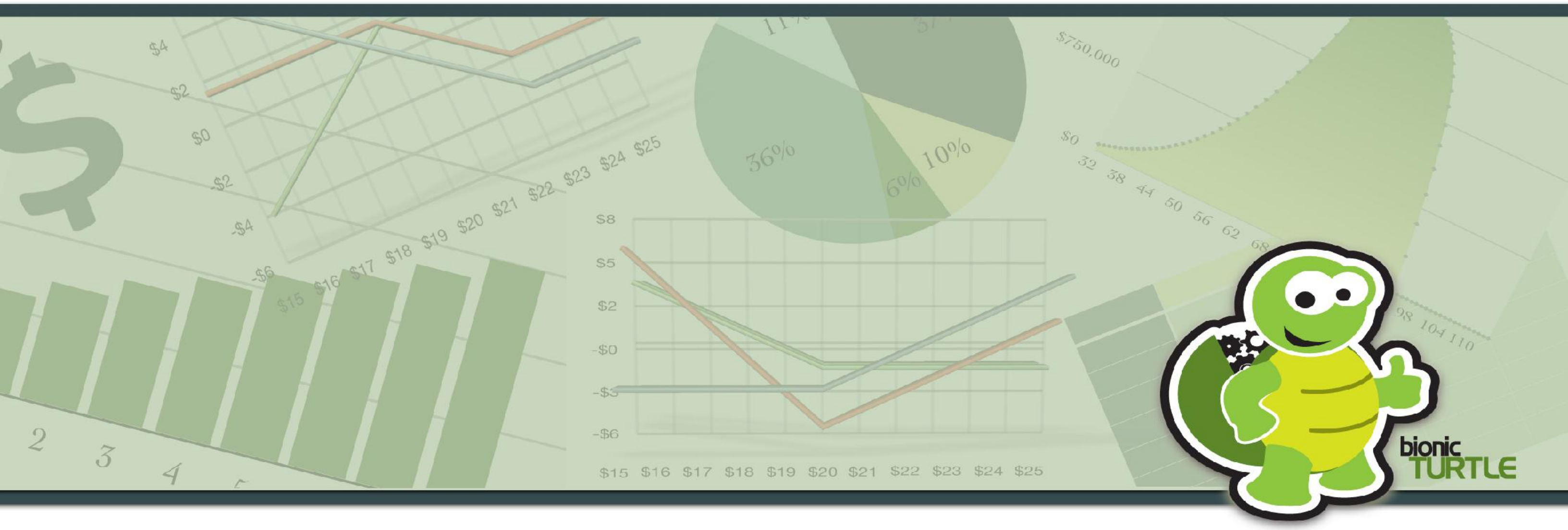

P1.T4. Valuation & Risk Models

Chapter 7. Operational Risk

Bionic Turtle FRM Study Notes

Chapter 7. Operational Risk

Chapter 7. Operational Risk

Describe the different categories of operational risk and explain how each type of risk can arise.

Compare three approaches for calculating regulatory capital.

Describe the Basel Committee's seven categories of operational risk.

Derive a loss distribution from the loss frequency distribution and loss severity distribution using Monte Carlo simulations.

Describe the common data issues that can introduce inaccuracies and biases in the estimation of loss frequency and severity distributions.

Describe how to use scenario analysis in instances when data is scarce.

Describe how to identify causal relationships and how to use risk and control self-assessment (RCSA) and key risk indicators (KRIs) to measure and manage operational risks.

Describe the allocation of operational risk capital to business units.

Explain how to use the power law to measure operational risk.

Explain the risks of moral hazard and adverse selection when using insurance to mitigate operational risks.

Describe the different categories of operational risk and explain how each type of risk can arise.

Realizing that the potential for losses due to operational risks could be even higher than that of either market risks or credit risks in the recent past, the Basel committee in 1999 started including minimum capital requirements for operational risk under its Basel II regulations.

The Basel definition of 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 reputational risk".[1]

In brief, operational risks can be mainly linked to the losses derived from the various operations conducted as a part of the business activities of a bank. These include cyber risks, regulatory fines, lawsuit proceedings, rogue trading activities, operational failures, etc.

[1] Bank for International Settlements, Basel Committee on Banking Supervision, Principles for the Sound Management of Operational Risk (June 2011). Historically, the FRM follows BIS with this traditional definition of operational risk that excludes reputational risk (as a non-financial, non-business risk) and strategic risk (as one of many business risks) but this definition is neither universal nor static. This typology follows from defining OpRisk as a *financial* OpRisk, but in practice, modern risk managers often include non-financial and/or business risks.

The seven categories of operational risk events as defined in the Basel II framework[2] are:

1. **Internal Fraud:** Operational risk losses occur due to fraudulent activities carried out within a firm by its employees. They include losses caused by intentionally fraudulent or deceitful activities, misuse of property, or bypassing laws and regulations where at least one internal person is involved. **These exclude diversity/discrimination events**. Examples include:
    - *Unauthorized activities:* deliberately not reporting transactions, unauthorized transactions, intentional mismarking of positions
    - *Fraud and theft:* credit fraud, robbery, forgery, asset misuse, willful tax evasion, smuggling, giving bribes/getting kickbacks, insider trading
2. **External Fraud:** Operational risk losses are due to damages caused by an external or third party. They include acts intended to cheat, steal property, or damage systems security. Examples include:
    - *Theft and fraud:* robbing, forgery, check kiting
    - *Systems security*: hacking, stealing information
3. **Employment Practices and Workplace Safety (EPWS):** Operational risk losses arise from non-compliance with employment laws, health/safety regulations, and from the disbursement of personal injury claims or diversity/discrimination events. Examples include:
    - *Employee relations*: compensation, benefits, termination disputes, structured labor activity
    - *Safe environment*: general accountability (falling, slipping), employee wellbeing and safety guideline events, compensation
    - *Diversity and discrimination*: charges of discrimination among different employees.
4. **Clients, Products, and Business Practices (CPBP):** Operational risk losses are caused by those who do not uphold their professional responsibilities, such as fiduciary duty, to clients, or from the nature or design of a product. Such losses could be classified as accidental/involuntary or those occurring as a result of careless behavior. Examples include:
    - *Suitability, disclosure, and fiduciary:* fiduciary violations, suitability/disclosure concerns, retail client release breaches, privacy violations, hostile sales, account churning, mishandling of private data, lender responsibility
    - *Improper business or market procedures*: antitrust, illicit trade/market habits, market maneuvering, insider trading (on the company's account), unlicensed actions, money laundering
    - *Product flaws:* product deficiencies (unapproved), model errors
    - *Selection, sponsorship, and exposure:* failure to investigate client per regulations, surpassing client exposure restrictions
    - *Advisory activities:* disagreements over the performance of advisory class action lawsuits, disputes over performance of advisory actions, lawsuits/penalties for guideline violations, fiduciary breaches, antitrust issues, money laundering, exceeding client exposure limits

[2] BCBS, "OPE, Calculation of RWA for operational risk; OPE30 Advanced Measurement Approaches", Version effective as of 15 Dec 2019. Dynamic (BIS) source at https://www.bis.org/basel_framework/chapter/OPE/30.htm

Operational risk event categories continued:[3]

5. **Damage to Physical Assets (DPA):** Operational risk losses may be caused by damage to physical assets due to natural events or human interruption. Examples include:
   - *Catastrophes and other incidents:* asset damage due to natural disasters, losses due to humans in the form of terrorism, vandalism
6. **Business Disruption and System Failures (BDSF):** Operational risk losses that occur because of the disturbance of corporate or system failures. This is self-explanatory! Examples include:
   - *Systems*: Hardware/software failures, interruption of telecommunications systems, utility outages.
7. **Execution, Delivery, and Process Management (EDPM):** Operational risk losses from unsuccessful transaction handling or inappropriate process management, due to unhealthy relations with trade counterparties and suppliers.
   - *Transaction, Capture, Execution, and Maintenance:* failure to communicate information, incorrect data entry, maintenance or loading errors, missed deadlines, incorrect operation of model or system, accounting errors, failure to perform specific tasks, delivery failures, failure of collateral management, not maintaining reference data
   - *Monitoring and Reporting:* failure to report, incorrect external reports
   - *Customer Intake and Documentation:* not obtaining client permissions or missing disclaimers, incomplete legal documents
   - *Customer/Client Account Management*: unauthorized account access, loss from inaccurate client data, negligent loss to client assets
   - *Trade Counterparties:* improper performance and disagreements by non-client counterparties
   - *Vendors and Suppliers:* disputes due to outsourcing and vendors.

[3] BCBS, "OPE, Calculation of RWA for operational risk; OPE30 Advanced Measurement Approaches", Version effective as of 15 Dec 2019. Dynamic (BIS) source at https://www.bis.org/basel_framework/chapter/OPE/30.htm