操作风险与弹性

FRM二级培训讲义-基础班

讲师：Mikey Chow

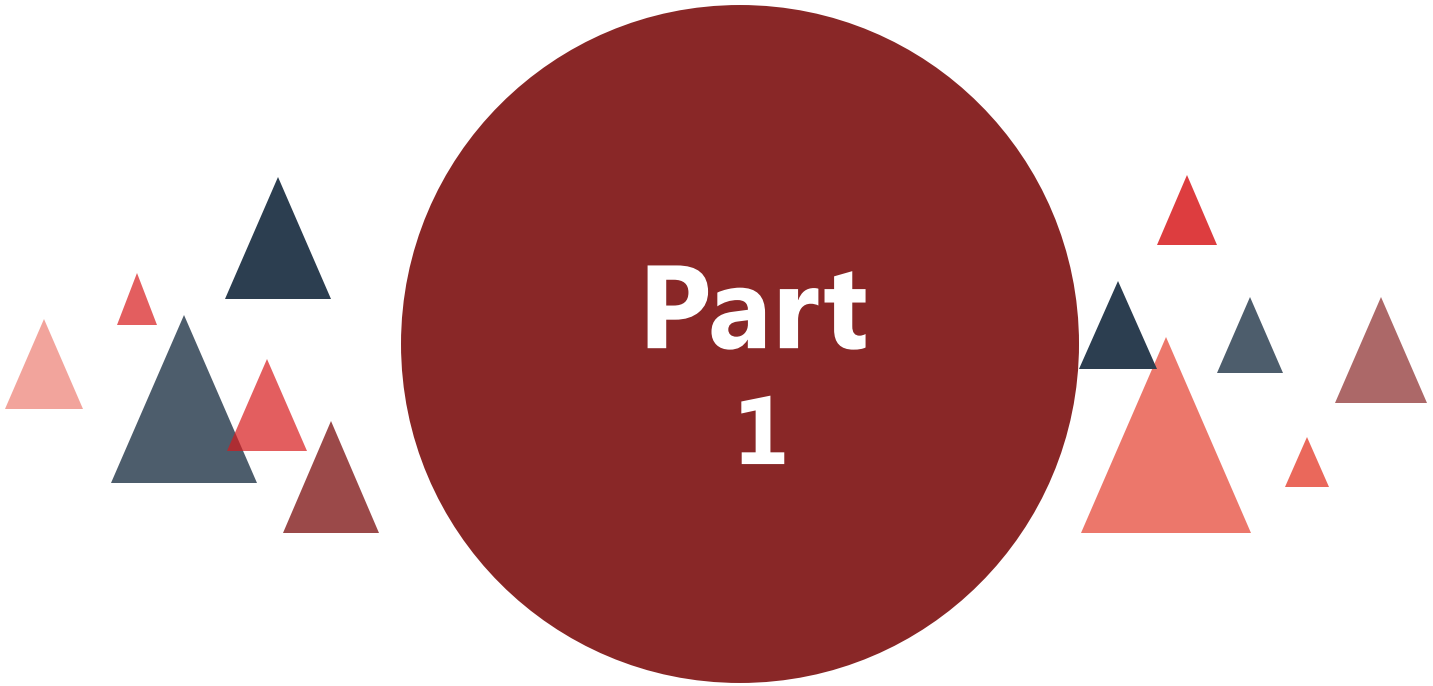
Topic Weightings in FRM Part II

Session NO.	Content	%
Study Session 1	Market Risk Measurement and Management	20
Study Session 2	Credit Risk Measurement and Management	20
Study Session 3	Operational Risk and Resiliency	20
Study Session 4	Liquidity and Treasury Risk Measurement and Management	15
Study Session 5	Risk Management and Investment Management	15
Study Session 6	Current Issues in Financial Market	10

Framework

Operational Risk and Resiliency

- Part 1: Operational Risk Management(CH1~CH6)
- Part 2: Model Risk and Data Quality(CH7~CH11)
- Part 3: Economic Capital Management and other related issues(CH12~CH18)
- Part 4: The Basel Accord(CH19~CH22)
- Part 5: Cyber-Resilient and Operational Resilience(CH23~CH26)



Operational Risk Management

Principles for the Sound Management of Operational Risk

Chapter 1

Framework

1. Three Lines of Defense
2. 11 Principles of Operational Risk Management

1. Three Lines of Defense

① **Business line management**

- Business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

② **Functionally independent corporate operational risk function (CORF)**

- Include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting.
- Challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems.

③ **Independent review and challenge of the bank's operational risk management controls, processes and systems.**

- This review may be done by audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties.

2. 11 Principles of Operational Risk Management

- **11 Principles**
  - **Fundamental Principles of Operational Risk Management**
    - ✓ Principle 1, 2
  - **Governance**
    - ✓ Principle 3, 4, 5
  - **Risk management environment**
    - ✓ Principle 6, 7, 8, 9
  - **Business resiliency and continuity**
    - ✓ Principle 10
  - **Role of disclosure**
    - ✓ Principle 11

2. 11 Principles of Operational Risk Management

➢ Fundamental Principles of Operational Risk Management

- **Principle 1**: The **board of directors** should take the lead in establishing a strong risk management culture.
  - ✓ The board should establish a code of conduct or an ethics policy
- **Principle 2**: **Banks** should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes.
  - ✓ The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

2. 11 Principles of Operational Risk Management

Governance(Cont'd)

- **Principle 3**: **The board of directors** should establish, approve and periodically review the Framework.
  - ✓ Establish a **mgt. culture**, and related supporting processes
  - ✓ develop comprehensive, dynamic **oversight** and control environments
  - ✓ Provide senior mgt. with **clear guidance**
  - ✓ Ensure the Framework is subject to **effective independent review** by audit or other appropriately trained parties
  - ✓ Ensure that as **best practice** is availing themselves of these advances
  - ✓ Establish clear lines of mgt. **responsibility and accountability**
- **Principle 4**: **The board of directors** should approve and review a risk appetite and tolerance statement for operational risk.

2. 11 Principles of Operational Risk Management

- **Governance**
  - **Principle 5**: **Senior management** should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility.
    - ✓ **Establish and maintain** robust challenges mechanisms and effective issue-resolution processes.
    - ✓ **Translate the operational risk mgt. Framework** into specific policies and procedures.
    - ✓ **Clearly assign authority, responsibility and reporting relationships** to encourage and maintain accountability.
    - ✓ **Ensure the mgt. oversight** process is appropriate.
    - ✓ **Ensure staff** for managing different risks coordinate and communicate effectively.
    - ✓ **Ensure that the bank activities** are conducted by staff with the necessary experience, technical capabilities and access to resources.
    - ✓ The managers of CORF should be of sufficient stature to **perform their duties effectively.**

2. 11 Principles of Operational Risk Management

- **Risk management environment(Cont'd)**
  - **Principle 6**: **Senior mgt.** should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood. **Examples of** Tools used to Identify and Assess Operational Risk
    - ✓ Audit Findings
    - ✓ Internal/External Loss Data Collection and Analysis
    - ✓ Risk Self Assessment (RSA) or Risk Control Self Assessments (RCSA)
    - ✓ Business Process Mapping: Identify the key steps in business processes, activities and organizational functions.
    - ✓ Risk and Performance Indicators: Key Risk Indicators (KRIs)
    - ✓ Scenario Analysis

2. 11 Principles of Operational Risk Management

➢ Risk management environment(Cont'd)

- **Principle 7**: **Senior mgt.** should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk. The review and approval process should consider:
  - ✓ inherent risks in the new product, service, or activity;
  - ✓ changes to the bank's operational risk profile and appetite and tolerance, including the risk of existing products or activities;
  - ✓ the necessary controls, risk management processes, and risk mitigation strategies;
  - ✓ the residual risk;
  - ✓ changes to relevant risk thresholds or limits; and
  - ✓ the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

2. 11 Principles of Operational Risk Management

- **Risk management environment**
  - **Principle 8**: **Senior mgt.** should implement a process to regularly monitor operational risk profiles and material exposures to losses including an appropriate reporting mechanisms.
  - **Principle 9**: **Banks** should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.
    - ① **Effective Control Environment**
    - ② Managing Technology Risk(same as other operational risk)
    - ③ **Managing Outsourcing Risk**

2. 11 Principles of Operational Risk Management

① Features of an Effective Control Environment

- An effective control environment requires appropriate segregation of duties and dual control.
- In addition, banks should ensure that **other traditional internal controls**:
  - ✓ clearly established authorities and/or processes for approval;
  - ✓ close monitoring of adherence to assigned risk thresholds or limits;
  - ✓ safeguards for access to, and use of, bank assets and records;
  - ✓ appropriate staffing level and training to maintain expertise;
  - ✓ ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;
  - ✓ regular verification and reconciliation of transactions and accounts; and
  - ✓ a vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.

2. 11 Principles of Operational Risk Management

③ **To manage Outsourcing Risk,** bank should have

- procedures for determining whether and how activities can be outsourced;
- processes for conducting due diligence to select potential service providers;
- sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;
- programs for managing and monitoring the risks within the outsourcing arrangement, including the financial condition of the service provider;
- establishment of an effective control environment at the bank and the service provider;
- development of viable contingency plans;
- execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

2. 11 Principles of Operational Risk Management

- **Business Resiliency and Continuity**
  - **Principle 10**: Banks should have business resiliency and continuity plans.
- **Role of disclosure**
  - **Principle 11**: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

Enterprise Risk Management

Chapter 2&3

Framework

1. ERM Definitions
2. Why ERM works?
3. Implementation of ERM
4. The Chief Risk Officer

1. ERM Definitions

- **Two major definitions of ERM**
  - Committee of Sponsoring Organizations of the Treadway Commission (COSO) :
    - ✓ "ERM is a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the **entity**, and manage risk to be within its appetite, to provide reasonable assurance regarding the achievement of **entity objectives**."
  - International Organization of Standardization (ISO 31000):
    - ✓ Risk is the "effect of uncertainty on objectives" and risk management refers to "**coordinated activities** to direct and control an organization with regard to risk."

1. ERM Definitions

- **[Author's opinion]While the COSO and ISO definitions provide useful concepts, it is important that ERM is defined as a value added function:**
  - Risk is a variable that can cause deviation from an expected outcome. ERM is a comprehensive and **integrated** framework for managing key risks in order to achieve business objectives, minimize unexpected earnings volatility, and maximize firm value.
- **A corporation can manage risks either:**
  - One risk at a time: largely compartmentalized, decentralized, or
  - **Enterprise risk management (ERM)**: All risks viewed together within a coordinated and strategic framework.

2.Why ERM works?

- **Create Shareholder Value both at the Macro and the Micro Level**
  - **At the Macro level**
    - ✓ ERM enables senior management to quantify and manage the risk-return tradeoff that faces the entire firm. This helps
      - ◆ maintain access to capital markets,
      - ◆ implement strategy and business plan.
    - ✓ By reducing non-core exposures, ERM effectively enables companies to take more strategic business risk and to take greater advantage of the opportunities in their core business.
  - **At the Micro level**
    - ✓ Well-designed ERM system ensures that all material risks are owned ("becomes a way of life for managers and employees").
    - ✓ Operating managers and employees can evaluate risk-return tradeoff.

2.Why ERM works?

- **ERM is all about integration, in three ways:**
  - ① enterprise risk management requires an integrated risk organization
  - ② enterprise risk management requires the integration of risk transfer strategies
  - ③ enterprise risk management requires the integration of risk management into the business processes of a company

2.Why ERM works?

- **Three Benefits To ERM**

① Organizational Effectiveness

✓ Various functions work cohesively and efficiently.

② Risk Reporting

✓ Timely and relevant risk reporting

③ Business Performance

✓ Market value improvement.

✓ Lower earnings volatility.

✓ Increased earnings.

✓ Improved shareholder value…

3.Implementation of ERM

- **Conceptual Framework of an ERM System (Cont'd)**

① **Determine firm's risk appetite (level of acceptable risk)**: When credit ratings are used as the primary indicator of financial risk, the firm determines an optimal or target rating based on its risk appetite and the cost of reducing its probability of financial distress.

② **Estimate capital requirement:** Given the firm's target rating, management estimates the amount of capital required to support the risk of its operations.

③ **Determine mix of capital and risk:** Management determines the optimal combination of capital and risk that is expected to yield its target rating. For a given amount of capital, management can alter its risk through hedging and project selection.

④ **Decentralize:** Top management decentralizes the risk-capital tradeoff with the help of a capital allocation and performance evaluation system that motivates managers throughout the organization to make optimal investment and operating decisions.

3.Implementation of ERM

① **Determine the Optimal Amount of Risk within ERM by targeting Credit Rating**

- **Articulate Risk Appetite:** The firm defines its rating-equivalent level of financial distress (e.g., we define financial distress as occurring when our bond rating falls to Baa or below) and sets a target probability of distress (e.g., we want to maintain a 1% chance of distress).
- **Specify Transition Matrix to Located Current Target Credit Rating:** Then the firm can use a transition matrix to determine its optimal, current bond rating (e.g., if our current rating is A, we will have a 1% change of falling to Baa, which is what we determined to be the level of financial distress)
- **Based on Target Credit Rating, Solve for Optimal Equity Cushion:** Finally, after determining the appropriate current bond rating, the firm can use the Merton model to determine the equity cushion consistent with the implied probability of default.

3.Implementation of ERM

- 7 components of ERM

3.Implementation of ERM

- **Challenges when implementing ERM (Cont'd)**
  - Inventory of Risks
    - ✓ Pay attention to liquidity, reputational, strategic risks and so on
  - Economic Value versus Accounting Performance
    - ✓ Stable cashflow v.s. volatile accounting earnings
  - **Aggregating Risks**
  - Measuring Risks
    - ✓ Tail risk beyond VaR measure
  - Regulatory versus Economic Capital(discussed later)
    - ✓ Problematic when RC exceeds EC, the difference is called stranded capital

3.Implementation of ERM—Aggregating Risks

- **Different distributions of three risks**
  - Market risk: have a normal (or at least symmetrical) distribution
  - Credit risk: have an asymmetric distribution.
  - Operational risk: have an asymmetric distribution
    - ✓ large numbers of small losses and some chance of large losses, so that the distribution of operational losses has a long [fat] tail."
- **Issues with Correlation in Risk Aggregation**
  - Across the firm, there is diversification across risk categories: firm-wide VaR is less than the sum of the market risk, credit risk, and operational risk VaRs.
  - the tendency for correlations to increase in highly stressed environments

4.The Chief Risk Officer

A CRO Is Responsible For

- Providing the overall leadership for enterprise risk management.
- Establishing an integrated risk management framework for all aspects of risks.
- Developing risk management policies, including the quantification of the fi rm's risk appetite through specific risk limits.
- Implementing a set of risk indicators and reports, including losses and incidents, key risk exposures, and early warning indicators.
- Allocating economic capital to business activities.
- Communicating the company's risk profile to key stakeholders.
- Developing the analytical, systems, and data management capabilities to support the risk management program.

4.The Chief Risk Officer

- **Reporting**
  - The heads of individual risk department report to the CRO.
  - The CRO reports to the CFO or CEO.
  - A dotted-line reporting relationship between the CRO and the board.

4.The Chief Risk Officer

- **An Ideal CRO's Superb Skills**
  - The leadership skills.
  - To convert skeptics into believers.
  - The stewardship to safeguard the company's assets.
  - Having the technical skills.
  - Having consulting skills.

Exercise

- The severity distribution of operational losses usually has the following shape:
  - A. Symmetrical with short tails
  - B. Long - tailed to the right
  - C. Uniform
  - D. Symmetrical with long tails

- Correct Answer: B

Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions

Chapter 4

Framework

1. Best Practices in RAF
2. Key Challenges in Implementing RAF
3. Key Lessons Learned From Cases

1.Best Practices in RAF

- **Convergence experience in risk appetite framework(Cont'd)**

① Successful implementation is highly dependent on effective interactions among all key stakeholders, including Board members, senior management, the risk management function, and the operating businesses.

② Putting in place an effective risk appetite framework is inextricably linked to the risk culture of a firm.

③ Limits and controls have a central role in any well-run organization, but an excessively narrow emphasis on granular limits (or too many of them) can provide false comfort to management and supervisors.

1.Best Practices in RAF

- **Convergence experience in risk appetite framework**

④ A large majority of firms (70%) are taking a comprehensive view of all risks across the firm, not merely focusing on those risks that can be easily measured, and are using a combination of quantitative and qualitative metrics in expressing risk appetite.

⑤ Stress testing and stress metrics play a role in the risk appet ite framework of almost all respondents (only one firm stated that they are not used).

⑥ A large majority of those responding indicated that risk appetite is monitored on an ongoing basis at the group level and that a contingency plan or escalation procedure is triggered when a risk appetite metric is exceeded.

2.Key Challenges in Implementing RAF

- **The largest challenges that are proving most difficult to overcome(Cont'd)**
  - ① **The link with risk culture is of central importance but is also problematic.**
  - ② Effectively cascading the risk appetite framework throughout the firm and embedding and integrating it into the operational decision-making process
  - ③ Express risk appetite in a way that covers all relevant risks.
  - ④ It is difficult to shift the perception that risk appetite is primarily about setting limits.
  - ⑤ **Forge the necessary links between risk appetite and the strategic and business planning processes.**
  - ⑥ **How stress testing should be effectively incorporated into the RAF?**
  - ⑦ How to achieve an appropriate aggregation at the group level of the levels of risks for the different individual businesses and how to establish relationships between these?

2.Key Challenges in Implementing RAF

① Risk Appetite and Risk Culture

- A crucial challenge is building a strong link and an effective interaction between culture and the RAF.
- Firms that had made the most progress in establishing a risk appetite framework report that there is a close and indissoluble link between risk appetite and culture.
- The link with culture is therefore potentially **self-reinforcing**
  - ✓ firms with a strong risk culture find it relatively more straightforward than others to implement a risk appetite framework.
  - ✓ At the same time, an effective risk appetite framework can consolidate and reinforce an effective risk culture with individuals and business heads feeling reinforced a bout doing the right thing.

2.Key Challenges in Implementing RAF

⑤ **Establishment of an effective link between the risk appetite framework and the strategy and business planning processes.**

- There needs to be an **iterative** relationship between setting risk appetite and planning at both the group and the business unit levels.
  - ✓ Iteration starts with a concept of risk appetite→business planning → aggregation → checking back with the risk appetite framework → adjusting as necessary
- The final stage in the iterative process may involve changing either aspects of the business plans or of the overall risk appetite
  - ✓ Too conservative: unable to effectively and prudently accommodate business and strategy evolution
  - ✓ Too flexible: fail to create the necessary discipline on the business

2.Key Challenges in Implementing RAF

⑥ **A comprehensive, enterprise-wide stress testing mechanism is a key part of a fully effective risk appetite framework.(Cont'd)**

I. Management needs to develop clear and consistent criteria for deciding on the severity/plausibility of the stress and scenario tests chosen.

II. Scenarios are needed to assess the array of secondary implications for the firm as a whole.

III. Management and Boards need to feel confident in assessing the results of the chosen stress and scenario tests.

2.Key Challenges in Implementing RAF

⑥ **A comprehensive, enterprise-wide stress testing mechanism is a key part of a fully effective risk appetite framework.**

IV. Results of stress tests need to be linked to key objective variables such as P&L, RWAs, and Tier 1 capital and illustrate explicitly how outcomes for these would comply with risk appetite boundaries through time.

- ✓ If the decision is to take no action in response to a stressed scenario, the Board and management should be able to explain fully why this decision is defensible.
- ✓ The compliance of stressed outcomes with the boundaries contained with in the RAF should be monitored frequently, and the risk appetite and stress testing frameworks themselves should be reviewed at least annually with the Board.

3.Lessons Learned From Cases

- **As the risk appetite has been developed a number of lessons have been learned:**
  - ① Without sponsorship from the top it is difficult to get traction in developing a risk appetite framework.
  - ② Without a clear conceptual definition of risk appetite there are many confusing and ineffective discussions about risk management and we fail to get business buy-in to the framework.
  - ③ The conversations around risk appetite are equally as important and beneficial as the actual Risk Appetite Statement document produced from them.
  - ④ Culture is a fundamental part of risk appetite and to the success of embedding risk appetite in the organization. Taking the time to craft descriptions of what risk appetite the Group and business units have for variance in risk culture breathes life into risk culture.

Banking Conduct and Culture

Chapter 5

Framework

1. Mindset of Culture and Conduct
2. Improving Conduct and Culture
3. Regulators Expectations
4. Lessons Learned

1.Mindset of Culture and Conduct

What is Culture？

- Culture is defined as the mechanism that delivers the values and behaviors that shape conduct and contributes to creating trust in banks and a positive reputation for banks among key stakeholders, both internal and external.
  - ✓ Culture comprises not only conduct and behaviors, but also the bank's values and ethics.
- Culture, on the other hand, is intangible and ubiquitous; as such, it requires deep understanding of the strategy, operating model, and values of the organization.

1.Mindset of Culture and Conduct

- **What is conduct?**
  - While cultural norms and beliefs cannot easily be measured, the conduct and behaviors that the cultural norms encourage or discourage can be.
  - While conduct can be evaluated as good or bad, culture itself cannot be.
    - ✓ The culture of each firm is unique to that organization and it is not empirically right or wrong; rather, it has to be right for that organization.
    - ✓ In that same vein, firms that have had conduct issues or scandals do not necessarily have an overall bad culture but have elements of their culture that are **misaligned** with the outcomes the firm is seeking and that are driving undesirable or inappropriate behaviors.

1.Mindset of Culture and Conduct

- Over the last decade, bank culture and conduct have received increased attention from bank management and their supervisors, clients/ customers, and investors. As a result, banks have invested significant effort in improving their culture and conduct. (Cont'd)
  - ① Refinement and/or re-articulation of bank purpose and values, with subsequent establishment of extensive communication and training programs.
  - ② Heightened engagement at the board level on conduct and culture issues.
  - ③ Modification of compensation and performance management schemes to incorporate not just financial results but also **behavioral considerations**.

1.Mindset of Culture and Conduct

- Over the last decade, bank culture and conduct have received increased attention from bank management and their supervisors, clients/ customers, and investors. As a result, banks have invested significant effort in improving their culture and conduct.

  ④ Systematization of the roles of second and third lines of defense in culture and conduct, and a push toward greater ownership of these concerns by the first line.

  ⑤ Changes to business processes, including

  - ✓ new product approval and product governance, revised pricing approaches, improved whistleblowing mechanisms, and review of questionable market practices in trading hedging, all of which are signs that the conduct agenda is beginning to cascade down to the way business is done.

1.Mindset of Culture and Conduct

- **Despite these efforts to improve conduct and culture, the banking industry still suffers from a negative reputation, and trust still needs repairing.**
  - the banking industry historically ranked among the most highly trusted industries since the end of the World War II; however, trust declined precipitously during the financial crisis, and today remains low compared to other industries and far from recovering to precrisis levels.
    - ✓ The ongoing stream of conduct scandals, ranging from lapses in customer protection to anti-money-laundering deficiencies to manipulation of market benchmark rates to rogue traders.
  - **conduct** is not just an investment banking issue but an "all banks, all geographies, all businesses potential issue".
  - the **reputational** overhang can live on long after the misconduct occurs, sometimes even after the specific issue has been addressed.

1.Mindset of Culture and Conduct

- **Banks cannot afford to be complacent about their trust and reputational problems, especially in light of emerging competition from alternative providers.**
  - "banking is necessary; banks are not."——Bill Gates
  - Without earning trust every day, the continued survival of banks is at risk from displacement by new industry entrants
  - trust and reputational issues may over time also lead to problems in acquiring and retaining talent.

1.Mindset of Culture and Conduct

- **Bank culture and conduct are more important than ever, to repair trust and reputational issues and fulfill the role of banks in society.**
  - And yet, many banks spend insufficient time thinking about their purpose and the role they play in society.
  - Banks are held to a higher standard than many other service providers given that the services banks provide are viewed to benefit society
    - ✓ intermediating between sources and needs of funds and facilitating transactions throughout the economy and the effects of failure extend beyond just shareholders, with repercussions for the broader economy.
    - ✓ Further, because banking products and services can be complex and difficult to understand, the public expects banks to provide good advice based on expertise and in the clients' best interest.

2.Improving Conduct and Culture

- Two key recommendations for improving conduct and culture:
  - **THE WHAT.** Banks should specify
    - ① their cultural aspirations through a robust set of principles, and
    - ② fashion mechanisms that deliver high standards of values and
    - ③ associated conduct consistent with the firm's purpose and broader role in society.
  - **THE HOW.** Banks should work to fully embed the desired culture through ongoing monitoring and perseverance, drawn from four key areas: (Cont'd)
    - ① senior accountability and governance
    - ② **performance management and incentives**
    - ③ **staff development and promotion**
    - ④ an effective three lines of defense

2.Improving Conduct and Culture

② **performance management and incentives**

- Recent years have seen cases of conflicted remuneration models that incentivize overly aggressive sales behaviors that resulted in harmful outcomes for customers.
  - ✓ A number of individual firms have removed sales-focused incentives for frontline staff, opting instead for alternative measures such as those based on team goals and customer satisfaction outcomes.
  - ✓ The challenge of this transition consists of:
    - ◆ initial sales decline,
    - ◆ Need to experiment with alternative performance measures to achieve the right balance between incenting good conduct and achievement of strategic goals.
    - ◆ it requires insight into how employees perform their role.

2.Improving Conduct and Culture

② **performance management and incentives**

- limited impact on culture this change will have if done in isolation.
- It also requires willingness and courage on the part of leadership to deal with high performers (from a purely results perspective) who display toxic behaviors.
  - ✓ Banks have much lower tolerance for bad behavior and are even willing to forego revenue opportunities(terminate) where necessary in favor of maintaining a strong culture.
  - ✓ Banks are also beginning to weigh the potential benefits of using breach of conduct incidents and terminations as teaching moments, against the potential risks of running afoul of privacy, confidentiality, and employment law.

2.Improving Conduct and Culture

③ Staff Development and Promotions

- Training programs often focusing on defining specific expectations around behavior and helping employees understand how abstract values and principles specifically translate into day-to-day responsibilities and expectations.
- It is important to have the right training for the right people at the right time and to target the training and not push everyone through everything.
- **Conduct screens** are also increasingly being applied to promotion and external hiring decisions.
  - ✓ Some banks have stepped up their hiring practices to better assess new recruits' alignment with the organization's purpose, values, and expectations on behavior.

2.Improving Conduct and Culture

③ Staff Development and Promotions

- Recent years have also seen active investment in **surveillance technology** at banks, typically beginning with capital markets businesses but increasingly broadening in scope to other areas.
  - ✓ with advanced analytics, **surveillance technology** aims to detect or predict potential conduct events.
  - ✓ While the technology is rapidly evolving to support such capabilities, the ethical questions around the acceptable degree and level of employee monitoring remain.

3.Regulators Expectations

- **In our interviews we heard significant differences of opinion in terms of the role regulatory agencies can play.**
  - On the one hand, culture is so intimate and unique to the strategy and values of a specific institution, it is hard to imagine any external party being able to engage productively in an assessment of the culture.
  - On the other hand, numerous scandals and conduct issues have shown that insiders can miss signals of cultural deterioration, and management could benefit from external, unbiased inquiry. Some regulators have taken an optimistic view on this and are experimenting with alternative approaches.

4.Lessons Learned

- **8 key lessons learned(cont'd)**

① Managing culture is not a one-off event, but a continuous and ongoing effort that needs to be constantly reinforced and that must become a permanent way of doing business.

② Leadership always matters; conduct and culture must be embedded from the top down throughout the firm, starting with the board and senior management but also importantly including middle management.

③ The scope of conduct management is shifting from misconduct to conduct risk management more broadly.

④ Managing culture requires a multipronged approach and the simultaneous alignment of multiple cultural levers(policies, procedures).

4.Lessons Learned

- **8 key lessons learned**

⑤ Ten years out from the financial crisis, there is strong recognition that a more diverse set of views and voices in senior management will lead to better (and more sustainable) outcomes for all stakeholders.

⑥ While cultural norms and beliefs cannot be explicitly measured, the behaviors and outcomes that culture drives can and should be measured.

⑦ Regulation has a limited role in rule setting and mandating culture.

⑧ Restoring trust will benefit the industry as a whole; as such, industry-wide dialogue and best practices sharing are important elements in the journey toward a stronger and healthier banking sector.

Risk Culture

Chapter 6

Framework

1. Risk Culture and Corporate Culture
2. Drivers and Measurement
3. Characteristics of a strong risk culture
4. Challenges to Deploy an Effective Risk Culture

1.Risk Culture and Corporate Culture

- **What is corporate culture?**
  - Literature often refers to corporate culture as the missing link to fully understand how organizations act.
    - ✓ Culture is much more than a management style: it is a set of experiences, beliefs and behavioral patterns. It is created, discovered or developed when a group of individuals learn to deal with problems of adaptation to the outside world and internal integration.
    - ✓ Culture is more complex than other organizational variables

1.Risk Culture and Corporate Culture

➢ Why Corporate Culture Matters?

- In principle, a culture suitable for being applied to a business formula makes a significant contribution to business performance.
  - ✓ A suitable culture implies that people "make use" of the same assumptions and adopt behavior inspired by the company's values; this increases the market value of the company identity.
- According to economic literature, culture is a mechanism in such a way that makes the corporation more efficient through simplified communication and decision-taking process.
  - ✓ From this perspective, a strong culture has high fixed costs but reduces its marginal costs.

1.Risk Culture and Corporate Culture

- Risk Culture Definitions
  - **Risk culture** can be defined as the norms and traditions of the behavior of individuals and of groups within an organization that determine the way in which they identify, understand, discuss, and act on the risks the organization confronts and the risks it takes (Institute of International Finance 2009).
  - A bank's norms, attitudes, and behavior related to risk awareness, risk-taking and risk management and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day to-day activities and has an impact on the risks they assume (Financial Stability Board 2014; Base/ Committee 2015).
  - Risk Culture is a term describing the values, beliefs, knowledge, and understanding about risk shared by a group of people with a common purpose, in particular, the employees of an organization or of teams or groups within an organization (Institute of Risk Management 2012).

1.Risk Culture and Corporate Culture

- How Corporate Culture interact with Risk Culture
  - **Risk Culture** could be seen as a **subculture** with a central role in financial institutions.
    - ✓ The growing complexity of operations, roles, and activities performed by firms produces different subcultures at all levels of the organization;
  - Risk Culture **interacts with** dominant corporate culture.

2.Drivers and Measurement

- Factors that influence a firm's corporate culture and its risk culture
  - First of all, risk culture depends on national culture and environment.
    - ✓ As far as culture is concerned, some countries are more homogeneous than others, even though sometimes, areas having a similar culture are part of different nations.
  - Similarly, culture is very much a product of the environment.
    - ✓ Firms operating in countries characterized by lower aversion to uncertainty, greater individualism and sectors with a strong opacity of information such as the financial world have a more aggressive risk culture, and "even in a highly-globalized world with sophisticated managers, culture matters".

2.Drivers and Measurement

- In academic literature, there are some relatively well-established approaches to measuring culture.

① **Qualitative methods (cont'd)**

- ✓ Qualitative methods are the ethnographic analysis and the case study, which allow an in-depth investigation, but at the same time limit the comparability of results.
- ✓ direct observation is the only way to understand culture, since many of its aspects are silent.
  - ◆ people within an organization are not aware of how many assumptions affect their behavior and take for granted that it applies to everyone in the sector.
  - ◆ cognitive beliefs of researchers may influence evaluation capacity.
- ✓ As a consequence, a problem of objectivity prevents the possibility for other researchers to replicate the analysis and confirm its results.

2.Drivers and Measurement

- In academic literature, there are some relatively well-established approaches to measuring culture.

② **Quantitative methods**

✓ quantitative methods use standardized approaches of analysis through **statistical tools**.

◆ These methods do not provide in-depth observations but are more objective and allow the comparison of different situations.

✓ Quantitative methods have been primarily used to evaluate culture indirectly,

◆ E.g. By observing developments in risk governance and the link between risk governance and the company's risk-return combinations.

3.Characteristics of a strong risk culture

- Characteristics of a strong risk culture(cont'd)

① Risk culture is not a static thing but a formal and informal process continuously repeating and renewing itself.

② Building a sound risk culture is a collective process, not simply a matter of improving technical skills. Risk culture shall be a part of a business and not simply of the supervision, which is not necessarily a good proxy.

③ A suitable culture, with particular regard to risk, is not a critical success factor but is displayed only to meet the expectations of a public, customers or norms at particular times.

3.Characteristics of a strong risk culture

- Characteristics of a strong risk culture

④ The main changes since 2008 in the risk culture scenario are

- ✓ enforcement in legislation
- ✓ growth of the risk function
- ✓ balanced scorecards replacing sales staff performance indicators
- ✓ shift in focus from compliance to conduct
- ✓ culture becoming a board issue

⑤ In fact, there is no doubt that risk culture is widely inadequate today and that there is a need to move from "form to substance".

4.Challenge to Deploy an Effective Risk Culture

- **Critical Challenges to implement conduct risk management**

① Integration in business decision-making

✓ The integration of behavior and ethical considerations in business decisions (which could involve limiting or withdrawing from certain transactions or businesses) challenges the "prevailing consensus" on success;

② Consistency of messages and action

✓ The "tone at the top" is not always supported by consistent actions that demonstrate that conduct and ethical considerations visibly determine hiring, promotions, professional standing, and success.

③ Role of directors

✓ While board oversight of conduct risk is critical to the strengthening of conduct risk management, an appropriate balance should be established between the accountability of individual executives and the board.

4.Challenge to Deploy an Effective Risk Culture

- **Critical Challenges to implement conduct risk management**

④ Cross-border and cross-cultural issues

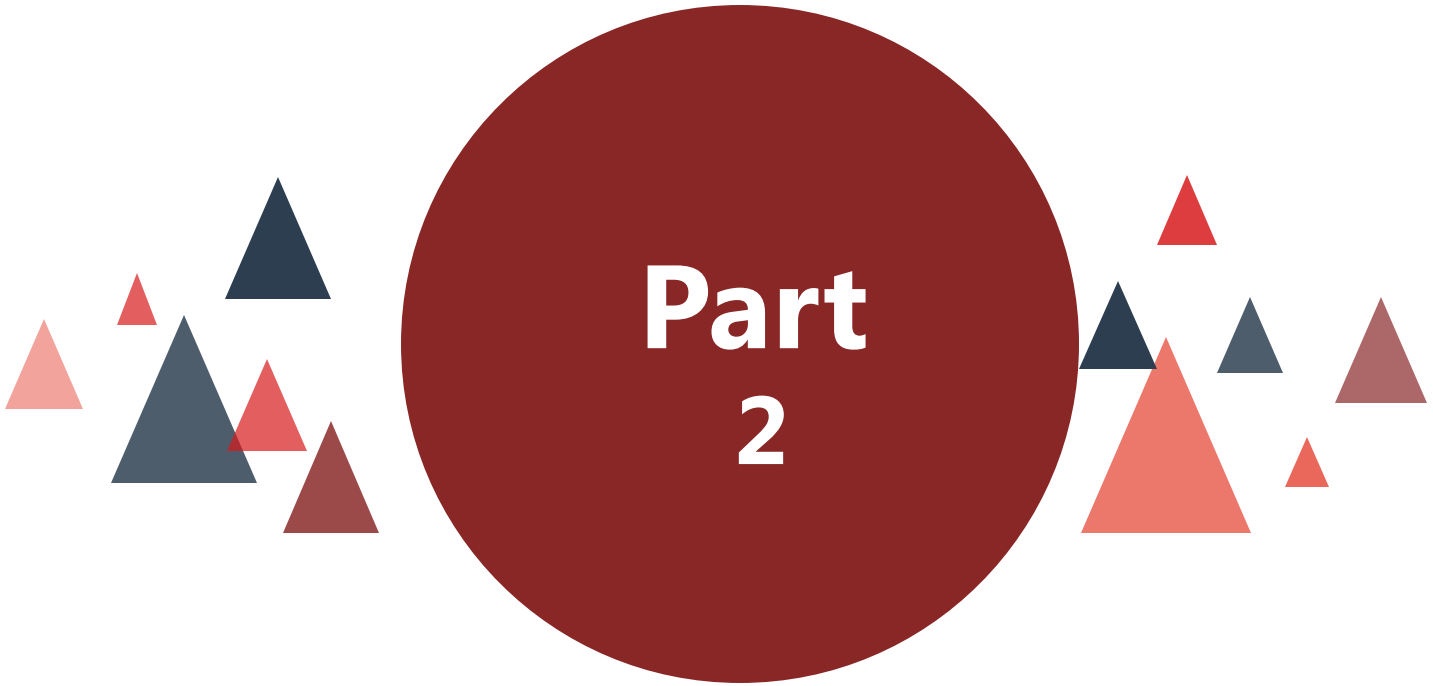
✓ Supervisors, clients, and stakeholders have different expectations and perspectives of the role of financial services providers.

⑤ Common taxonomy for conduct risk

✓ The integration of conduct risk in all aspects of a firm's business, in a manner that is consistent across the industry, requires the development of a consistent set of definitions, methods of assessment, and measurement of conduct risk.

⑥ Grey areas

✓ Actions that are not "illegal" but which, under particular circumstances, could be inconsistent with a firm's values are sometimes difficult to address because they are often dependent on facts and circumstances.



Model Risk and Data Quality

Operational Risk Data and Governance

Chapter 7

Framework

1. Seven categories of OpRisk
2. Four elements of the OpRisk Framework
3. OpRisk Profile in Different Financial Sectors
4. Risk Organization and Governance

1.Seven categories of OpRisk

- **Seven categories of operational risk**

① **Clients, products, and business practices**: Examples include mishandling of confidential information, breaches in fiduciary duty, and money laundering.

② **Internal fraud:** Examples include misreporting data or insider trading. These are usually low-frequency/high-severity events.

③ **External fraud:** Actions by a third party that disobey the law or misuse property. Examples include robbery or computer hacking. External fraud is very common in retail businesses with millions of clients.

④ **Damage to physical assets (DPA):** natural disasters. Examples include a terrorist attack, earthquakes, or fires.

1.Seven categories of OpRisk

- **Seven categories of operational risk (cont'd)**

⑤ Execution, delivery, and process management. Failure to correctly process transactions and the inability to uphold relations with counterparties. Examples include data entry errors or unfinished legal documents. Loss events are small but occur very frequently

⑥ Business disruption and system failures (BDSF). Examples include computer failures, both hardware- and software-related, or utility outages. Aside damage to physical assets, this risk type has least number of events.

⑦ Employment practices and workplace safety (EPWS). Actions that do not follow laws related to employment or health and safety. Examples include worker compensation, discrimination disputes, or disobeying health and safety rules.

2.Four elements of the OpRisk Framework

- The major **four sources** that can be used in any OpRisk framework are as follows **(cont'd)**:
  - ① Internal loss data
  - ② Business environment and internal control factors(BEICFs)
  - ③ External loss data
  - ④ Scenario analysis

2.Four elements of the OpRisk Framework

① Internal loss data **(cont'd)**

- may not be long enough
- When a bank acquires another banking operation, the assimilation of the two pre-acquisition internal datasets can pose challenging issues.
- Setting a threshold for loss can have significant impact
- Recoveries and Near Misses
  - ✓ The Basel II rules (BCBS, 2006) in **general do not allow** for the use of recoveries to be considered for capital calculation purposes.
  - ✓ The only exception is on **rapidly recovered loss events**, but even this exception is not accepted everywhere. When the rapid recovery is full, the event is considered to be a "**near miss".**

2.Four elements of the OpRisk Framework

① Internal loss data

- Provisioning Treatment of Expected Operational Losses
  - ✓ a provision should not be recognized for future operating losses;
  - ✓ a provision should be recognized for an **onerous contract**—a contract in which the unavoidable costs of meeting its obligations exceeds the expected economic benefits;
  - ✓ a provision for restructuring costs should be recognized **only when** an enterprise has a detailed formal plan for restructuring and has raised a valid expectation in those affected.

2.Four elements of the OpRisk Framework

② Business environment and internal control factors(BEICFs)

- If the control environment is fair and under control, large operational losses are not likely to take place and OpRisk is considered to be under control.
- **Risk Control Self-Assessment (RCSA)**
  - ✓ These are also known as Control Self-Assessment (CSA) in some firms, According to this procedure, firms regularly ask experts about their views on the status of each business process and subprocess.
- **Key Risk Indicators(KRIs)**
  - ✓ These indicators/factors are mostly quantitative and are used as a proxy for the quality of the control environment of a business.

2.Four elements of the OpRisk Framework

③ External loss data

- may not be representative of the bank's operational risk profile.
- Publicly available external data has a strong bias in favor of large and well-publicized losses.
- The exercise of relevance-based filtering can only make this problem worse: Relevance-based filtering may reduce bias by eliminating irrelevant data points, but increase variance due to potential filtering error and clearly fewer data points.
- Unproperly accounted for size differential.

2.Four elements of the OpRisk Framework

④ Scenario analysis

- These scenario estimates are usually gathered, through expert opinions. The Challenges exist when there are behavior biases among experts.
  - ✓ Presentation Bias
  - ✓ Availability bias.
  - ✓ Anchoring bias.
  - ✓ "Huddle" bias or anxiety bias
  - ✓ Gaming
  - ✓ Over/under confidence bias
  - ✓ Inexpert opinion
  - ✓ Context bias

3.OpRisk Profile in Different Financial Sectors

- OpRisk profile is generally very **diverse across different businesses** within a financial institution.
- A typical list of business units includes**(Cont'd)**
  - Corporate Finance
  - **Trading and Sales**
  - **Retail Banking**
  - Commercial Banking
  - Payment and Settlement
  - Agency Services
  - **Asset Management**
  - **Retail Brokerage.**

3.OpRisk Profile in Different Financial Sectors

- **Trading and Sales**
  - quite simple
  - However, as the products are diverse and complex and settlement deadlines and procedures vary significantly it is not surprising that executing these transactions is the major OpRisk of this business
- **Retail Banking**
  - most losses are due to external frauds that are daily events for these firms.

3.OpRisk Profile in Different Financial Sectors

- **Asset Management**
  - Due to the characteristics of their business, OpRisk is typically the largest risk exposure an asset manager has.
  - **OpRisk can be manifested** in many different ways for an asset manager as, for example, in errors in processing transactions or a system failure that can cause severe damage and impact the balance sheet of the asset manager.
- **Retail Brokerage**
  - Brokers usually do not hold large proprietary positions and lending
  - therefore, most exposure comes from potentially explosive system issues, execution errors, litigation with retail customers, fraud committed by clients, etc.

3.OpRisk Profile in Different Financial Sectors

- **Corporate Finance**
  - This business is where financial firms many times behave similar to consulting firms by providing advice to corporations in possible mergers and acquisitions, doing an IPO or even assessing strategic alternatives.
  - most of the losses fall under the umbrella of "litigation" or disputes with clients for arguably poor advice when, for example, IPOs go wrong.

4.Risk Organization and Governance

➢ Role of Operation Risk Governance

- Developing a **solid risk organization** is a key part of the framework.
- Having proper organizational involvement in OpRisk issues where key stakeholders are regularly informed and oversee risk is fundamental for success.
- The OpRisk manager needs to be integrated to the rest of the organization.
- **Sound internal governance** forms the foundation of an effective OpRisk management framework.

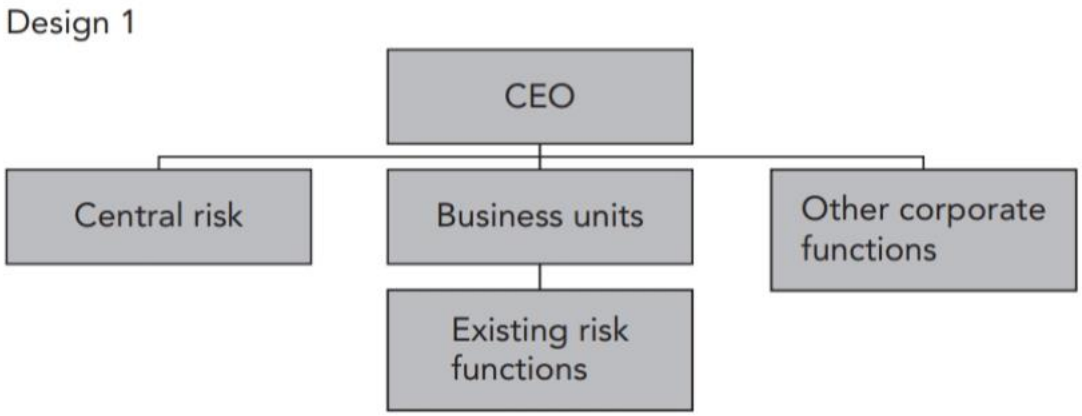
4.Organization of Risk Departments

- The organizational design would usually hint at the strength and degree of development of an OpRisk framework at a firm. **(cont'd)**
  - ① Design 1-Central Risk Function as Coordinator
  - ② Design 2-Matrix reporting-the "dotted lines"
  - ③ Design 3-Solid reporting lines to Central Risk Management
  - ④ Design 4-Strong Central Risk Management

4.Organization of Risk Departments

① Design 1-Central Risk Function as Coordinator

- Usually in this structure, risk management gathers information and reports to the CEO or the Board
- Business Units will be responsive to the Central Risk demands

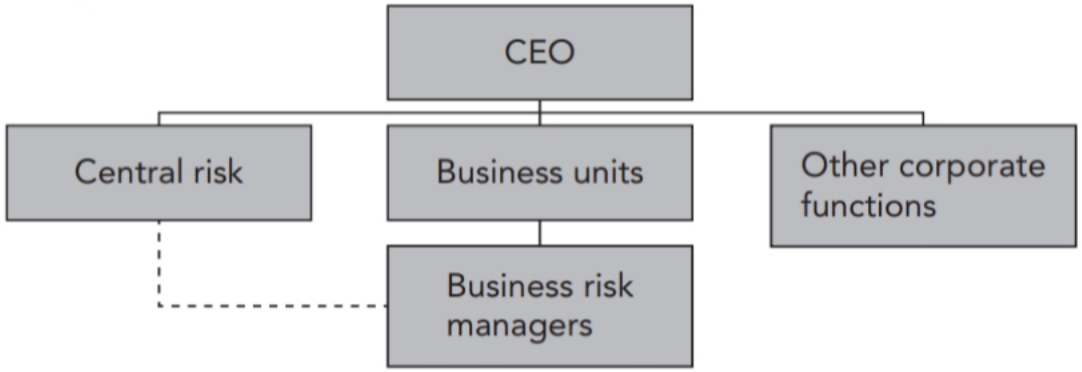


4.Organization of Risk Departments

② Design 2-Matrix reporting-the "dotted lines"

- risk managers have a dotted line to the Central Risk function; however, they are appointed by the Business Units and compensation decisions are still taken by these.
- the Business Units should have a strong risk culture and collaborate very closely with the Central Risk function.

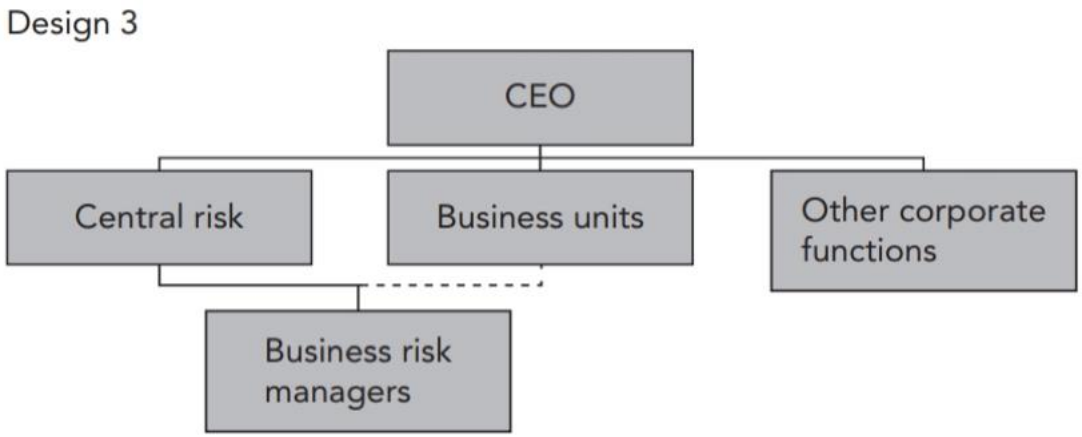
Design 2



4.Organization of Risk Departments

③ Design 3-Solid reporting lines to Central Risk Management

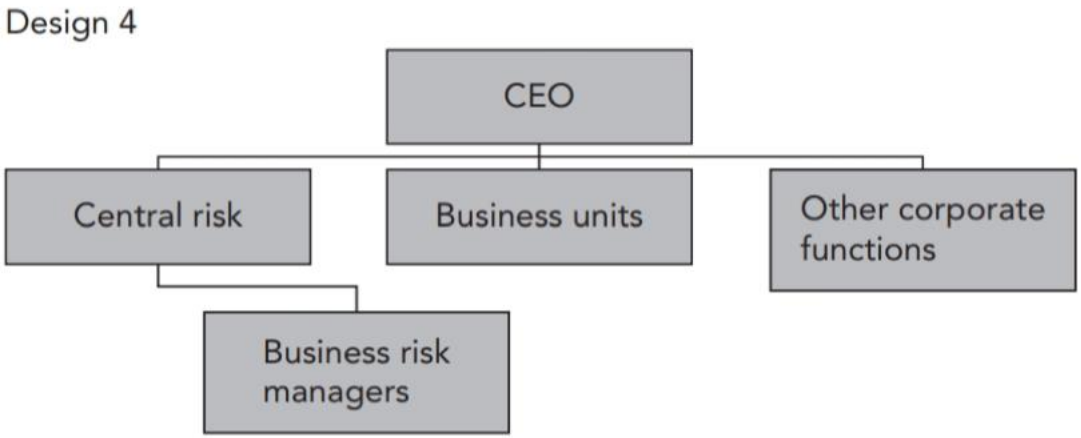
- Risk Managers still physically work in the Business Units but report to the Central Risk function usually based in the headquarters.
- This solid line reporting will also assist in the creation of a more homogenous risk culture and consistent approach across the enterprise;



4.Organization of Risk Departments

④ Design 4-Strong Central Risk Management

- the Corporate Chief Risk Officer is the key decision maker in risk management and fully responsible for risk across the firm



Exercise

- Which one of the following cases or events can be considered as resulting from operational risk?

  A. A bank reports losses on a diversified portfolio of stocks during the stock market decline.

  B. The bank becomes embroiled in a high-profile lawsuit with a customer that accuses it of improper selling practices.

  C. The bank reports the loss of $1.5 billion due to rises in interest rates.

  D. A U.S. investor makes a loss as the yen depreciates relative to the dollar.

- Correct Answer: B

Supervisory Guidance on Model Risk Management

Chapter 8

Framework

1. Overview of Model Risk Management
2. Effective Process to Manage Model Risk

1.Overview of Model Risk Management

What is Model Risk

- The use of models invariably presents **model risk**, which is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports.
- Model risk can lead to financial loss, poor business and strategic decision making, or damage to a bank's reputation.

1.Overview of Model Risk Management

- **Model risk occurs primarily for two reasons:**

① The model may have **fundamental errors**.

- ✓ shortcuts, simplifications, or approximations used to manage complicated problems
- ✓ errors in inputs or incorrect assumptions will lead to inaccurate outputs

② The model may be **used incorrectly or inappropriately**.

- ✓ Models by their nature are simplifications of reality, and real-world events may prove those simplifications inappropriate
- ✓ Model risk arises when existing models are applied to new products or markets, or inadvertently as market conditions or customer behavior changes.

Model Risk

- Model risk should be managed like other types of risk. Banks should identify the sources of risk, assess the magnitude and form effective process to manage model risk.
- **Three elements of effective process to manage model risk (cont'd)**
  - ① A robust model development, implementation, and use.
  - ② A sound model validation process.
  - ③ A good governance
    - ✓ sets an effective framework with defined roles and responsibilities for clear communication of model limitations and assumptions, as well as the authority to restrict model usage.

Model Risk

① The **best practices** for the **development and implementation** of a model

- Form a clear statement of purpose to ensure that model development is aligned with the intended use.
- The data and other information used to develop a model are of critical importance; there should be rigorous assessment of data quality and relevance, and appropriate documentation.
- An integral part of model development is **model testing**
  - ✓ Model testing includes checking the model's accuracy, demonstrating that the model is robust and stable , assessing potential limitations, and evaluating the model's behavior over a range of input values.
- Banks should ensure that the development of the more judgmental and qualitative aspects of their models is also sound.

2.Elements of Effective Process to Manage Model

② **A sound model validation process**.

- to verify that models are performing as expected, in line with their design objectives and business uses.

➢ An effective validation framework should include **three core elements (cont'd)**

I. Evaluation of conceptual soundness

II. Ongoing monitoring

III. Outcomes analysis

➢ If model validation reveals significant errors or inaccuracies that consistently fall outside the bank's acceptability. In such cases, model adjustment, recalibration, or redevelopment is warranted.

2.Elements of Effective Process to Manage Model

I. Evaluation of conceptual soundness

- the overall theoretical construction, key assumptions, data, and specific mathematical calculations.
- If testing indicates that the model may be inaccurate or unstable in some circumstances, management should consider modifying certain model properties, putting less reliance on its outputs, placing limits on model use, or developing a new approach.

2.Elements of Effective Process to Manage Model

II. Ongoing Monitoring

- **Benchmarking** is the comparison of a given model's inputs and outputs to estimates from alternative internal or external data or models. It can be incorporated in model development as well as in ongoing monitoring.
- Ongoing monitoring should include the analysis of overrides with appropriate documentation. In the use of virtually any model, there will be cases where model output is ignored, altered, or reversed based on the expert judgment of model users.

2.Elements of Effective Process to Manage Model

III. Outcome Analysis

- a comparison of model outputs to corresponding actual outcomes.
- Back-testing is one form of outcomes analysis
- **Parallel outcomes analysis**, under which both the original and adjusted models' forecasts are tested against realized outcomes, provides an important test of such model adjustments.

Information Risk and Data Quality Management

Chapter 9

Framework

1. Types of erred data
2. Key Dimensions of Data Quality
3. Data Quality Management

1.Types of erred data

- **Many types of erred data**
  - Data entry errors
  - Missing records
  - Duplicate records
  - Inconsistent data
  - Nonstandard formats
  - Complex data transformations
  - Failed identity management process
  - Undocumented, incorrect, or misleading metadata

2.Key Dimensions of Data Quality

- **Six Key Dimensions of Data Quality(cont'd)**

① Accuracy

- ✓ Description: accuracy is measured in terms of agreement with an identified reference source of correct information.
- ✓ Example: the temperature recorded in a weatherglass compared to the real temperature.

② Completeness

- ✓ Description: specifies the expectations regarding the population of data attributes.

2.Key Dimensions of Data Quality

- **Six Key Dimensions of Data Quality(cont'd)**

③ Consistency

- ✓ Two data values drawn from separate data sets must not conflict with each other.
- ✓ Three types of consistency:
  - ◆Record level: between one set of data values and another set within the same record.
  - ◆Cross-record level: between one set of data values and another set in different records.
  - ◆Temporal level: between one set of data values and the same set within the same record at different points in time.

2.Key Dimensions of Data Quality

- **Six Key Dimensions of Data Quality(cont'd)**

④ Reasonableness

- ✓ Description: measure conformance to consistency expectations relevant within specific operational contexts.
- ✓ Example: one might expect that the total sales value of all the transactions each day is not expected to exceed 105 percent of the running average total sales for the previous 30 days.

⑤ Currency

- ✓ Description: measures whether the data is considered to be "fresh", and its correctness in the face of possible time-related changes.

⑥ Uniqueness

- ✓ Description: uniqueness suggests that there can only be one data item within the data set.

3.Data Quality Management

Operational Data Governance Process

- **Operational data governance** is the manifestation of the processes and protocols necessary to ensure that an acceptable level of confidence in the data effectively satisfies the organization's business needs.
- A **data governance program** defines the roles, responsibilities, and accountabilities associated with managing data quality. Rewarding those individuals who are successful at their roles and responsibilities can ensure the success of the data governance program.
- To measure this, a "**data quality scorecard**" provides an effective management tool for monitoring organizational performance with respect to data quality control.

3.Data Quality Management

- **Data Quality Scorecard: two types of data quality metrics (cont'd).**

① **Simple metrics, also called** "base-level" metrics, and they quantify specific observance of acceptable levels of defined data quality rules.

113-310

3.Data Quality Management

- **Data Quality Scorecard: data quality scores introduces two types of metrics.**

② **Complex metric** representing a rolled-up score computed as a function (such as a sum) of applying specific weights to a collection of existing metrics, both base-level and complex. There are three different view for reporting purpose:

- ✓ **Data Quality Issues View**: Evaluating the impacts of a specific data quality issue across multiple business processes
- ✓ **Business Process View**: representing the impacts associated with each issue for a specific business process
- ✓ **Business Impact View**: representing the impacts of a number of different data quality issues originating in a number of different business processes.

Validating Rating Models

Chapter 10

Framework

1. Model Validation Process
2. Validating Rating Models

1.Model Validation Process

- **Process of Model Validation lies on**
  - statistical comparisons of actual risk measures against the ex ante estimates
  - checking of parameter calibrations
  - Benchmarking
  - stress tests
  - analyses of all the components of the internal rating system, including operational processes, controls, documentation, IT infrastructure, as well as an assessment of their overall consistency.
  - Reviewing model building steps and application choices, detecting weaknesses and limitations, verifying the proper use of the system
  - analyzing contingent solutions planned in case the robustness of the model falls or is lacking.

1.Model Validation Process

- **The validation process is performed by a specific organizational unit.**
  - In smaller banks, the least that is needed is the appointment of a manager devoted to coordinate and oversee these activities.
- **Best practise**
  - the validation unit has to be independent of other functions devoted to develop and to maintain model tools and to handle credit risk processes and procedures.
    - ✓ Where compliance with this requirement would prove to be excessively **burdensome**, the internal audit function should verify that these activities are performed in an independent manner, fully achieving the intended objectives.
  - Specific attention has to be paid to ensure the appropriate skills of human resources employed.
  - The scope, transparency, and completeness of documentation are essential.

2.Validating Rating Models

- **Qualitative and Quantitative Processes(cont'd)**

  ① **Qualitative validation** ensures proper application of quantitative methods and proper usage of ratings.

  ② **Quantitative validation** comprises validation procedures of ratings in which statistical indicators are calculated and interpreted on the basis of an empirical dataset.

2.Validating Rating Models

① Qualitative Validation – Rating Systems Design

- **Obtaining probabilities of default.**
- **Rating system completeness.** In order to ensure the completeness of credit rating procedures, banks need to take all available information into account when assigning ratings to borrowers or transactions.
- **Rating system objectivity.** A good rating system needs procedures that capture creditworthiness factors clearly and also minimize room for interpretation.
- **Rating system acceptance.** Rating systems have also to be accepted by internal users such as credit analysts, credit officers, and loan officers.
- **Rating system consistency.** Models have to be coherent and suitable for the borrowers to which they are applied and with the theoretical frameworks of users.

2.Validating Rating Models

① Qualitative Validation – Data Quality

- Completeness of data
- Volume of available data
- Representativeness of samples
- Consistency and integrity of data sources
- Adequacy of procedures used to ensure data quality

2.Validating Rating Models

② Quantitative Validation

I. **Sample representativeness** of the reference population at the time of the estimates and in subsequent periods.

II. **Discriminatory power** is the relative ability of a rating model to accurately differentiate between defaulting and non-defaulting entities for a given forecast period.

III. **Dynamic properties**: the stability of rating systems and properties of migration matrices.

IV. **Calibration**: the predictive power concerning probabilities of default.

- ✓ **benchmarking** could be used as a supplement to validation, which compares a financial institution's ratings and estimates to those of other comparable sources.

2.Validating Rating Models

- **Three fundamental activities for validating rating systems**
  - Back testing
    - ✓ accuracy of risk parameter estimates when compared with ex post empirical evidence
  - Benchmarking
    - ✓ relative performance of systems and risk parameter estimates against benchmarks
  - Stress testing
    - ✓ adequacy of models when stress tests are applied

Assessing the Quality of Risk Measures

Chapter 11

Framework

1. Model Errors
2. Model Risk in VaR Models and Mapping
3. Two Case Studies

1.Model Errors

- **Model risk and variability can arise through the implementation of VaR models(cont'd)**

  ① **Data preparation**

  - ✓ Market data: time series asset price data
    - ◆**Challenge**: Missing data
  - ✓ Security master data: descriptive data on securities, such as maturity dates, currency, and units
    - ◆**Challenge**: Such databases are difficult to build and maintain
  - ✓ Position data: must be verified to match the firm's books and records.
    - ◆**Challenge**: Such data may have to be collected from many trading systems and across a number of geographical locations within a firm.

2.Model Risk in VaR Models and Mapping

- **Model risk and variability can arise through the implementation of VaR models**

② The risk manager has a great deal of **discretion** in actually computing a VaR.

✓ There is not much uniformity of practice as to confidence interval and time horizon.

③ Different ways of measuring VaR would lead to different results.

- Length of time series used for historical simulation or to estimate moments.
- Technique for estimating moments.
- Mapping techniques and the choice of risk factors.
- Decay factor if applying EWMA.
- In Monte Carlo simulation, randomization technique and the number of simulations.

2.Model Risk in VaR Models and Mapping

- **Problems with Mapping**

① Some decisions about mapping are pragmatic trade-offs with pros and cons.

✓ Choice between cash flow versus duration-convexity mapping for fixed-income.

② It may be difficult to find data that address certain risk factors.

✓ Mapping residential mortgage-backed securities (RMBS) and other securitized credit products

✓ convertible bond mapping using replicating method will ignore **liquidity risk**

③ A position and its hedge might be mapped to the same risk factor or set of risk factors. The result, however, will be a measured VaR of zero, even though there is a significant **basis risk**.

3.Two Case Studies

➢ Case Study 1: The 2005 Credit Correlation Episode

- A popular trade especially among hedge funds and proprietary trading desks was:
  - ✓ Sell protection on the equity tranche of the CDX.NA.IG
  - ✓ Buy protection on the junior mezzanine tranche of the CDX.NA.IG
- The trade was thus long credit and credit-spread risk through the equity tranche and short credit and credit-spread risk through the mezzanine.
- The portfolio had positive carry; that is, it earned a positive net spread.

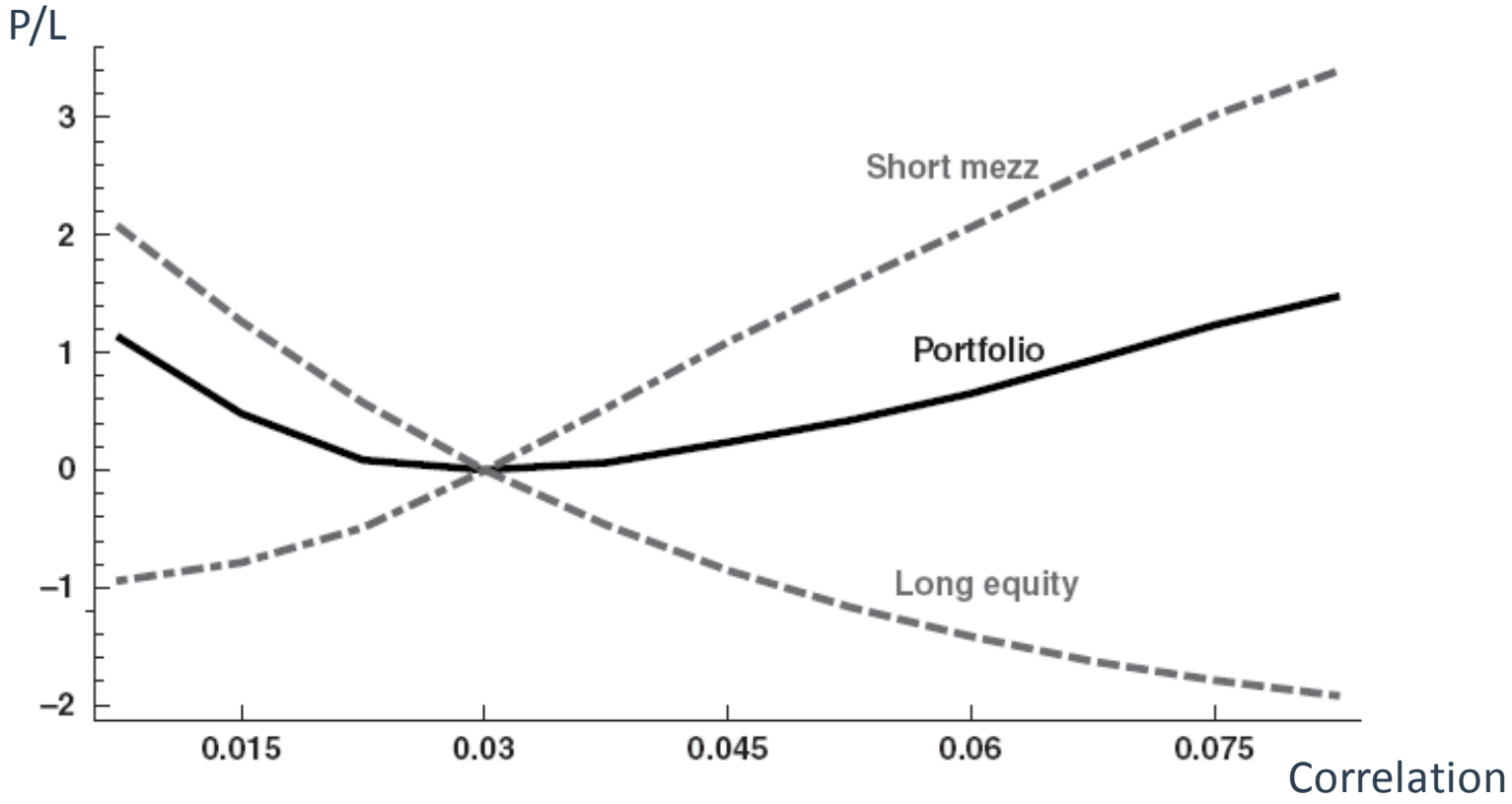
3.Two Case Studies

➢ Case Study 1: The 2005 Credit Correlation Episode

- The trade was designed to be default-risk-neutral at initiation.
  - ✓ How to determine the hedge ratio with default01s, for example,
    - ◆the default01 of a 1M notional position in the equity is -6,880.
    - ◆the default01 of a 1M notional position in the mezzanine is -721,
    - ◆hedge ratio= -6880/-721=9.54.
  - ✓ The trade has zero sensitivity to a small rise or decline in defaults.
- However, the trade has positive convexity. The trade benefits from **small changes** in the default rate in either direction.
- The model assumes the default correlation stays stable!

3.Two Case Studies

- **Case Study 1: The 2005 Credit Correlation Episode**



3.Two Case Studies

➢ Case Study 1: The 2005 Credit Correlation Episode

- The critical flaw was that the correlation assumption was static. Changing correlation drastically altered the hedge ratio between the equity and mezzanine tranches.
  - ✓ Stress testing correlation would have revealed the risk.
  - ✓ The trade could also have been hedged against correlation risk by employing an overlay hedge: that is, by going long single-name protection in high default-probability names.
- An additional risk was that the recovery amount was at risk. In the event of a default on one or more of the names in the index, the recovery amount was not fixed but a random variable.

3.Two Case Studies

Case Study 2: Subprime Default Models

- Credit-rating agencies assigned ratings to bonds utilizing subprime residential mortgage-based security (RMBS) valuation and risk models that utterly failed. Two key widespread defects:
  - ✓ House price appreciation assumption: The models assumed positive future house price appreciation rates.
  - ✓ Low (geographical) correlation assumption: Bonds based on pools of loans from different geographical regions were assumed to be well-diversified. However, house prices fell in nearly all regions and systemic correlations were much higher than anticipated.

Economic Capital Management and Other Related Issues

Risk Capital Attribution and Risk-Adjusted Performance Measurement

Chapter 12

Framework

1. Risk Capital
2. Risk-Adjusted Return on Capital
3. Adjusted RAROC
4. RAROC in Practice
5. Modeling Diversification Effect

1.Risk Capital

- **What is risk capital?**
  - **Risk capital** is the cushion that provides protection against the various risks inherent in the business of a corporation so that the firm can maintain its financial integrity and remain a going concern even in the event of a near-catastrophic worst-case scenario.
- **Economic Capital versus Regulatory Capital**
  - Economic Capital
    - ✓ Economic capital equals to risk capital. (Generally accepted convention)
    - ✓ Economic capital = Risk capital + Strategic capital
  - Regulatory Capital

1.Risk Capital

- **Economic Capital versus Regulatory Capital**
  - **Economic Capital**
    - ✓ Economic capital (EC) is intended to capture the economic realities of the risks a firm runs.
    - ✓ Economic capital (EC) is an internal policy decision by senior management and the board.
    - ✓ The determination of economic capital, and its allocation to the various business units, is a strategic decision process that affects the risk/return performance of the business units and the bank as a whole.

1.Risk Capital

- **Economic Capital versus Regulatory Capital**
  - **Regulatory Capital**
    - ✓ Regulatory capital only applies to a few regulated industries, such as banking and insurance companies.
    - ✓ It is calculated according to a set of industry-wide rules and formulas and sets only a minimum required level of capital adequacy.
    - ✓ Rule-based with the intention to ensure enough capital in the banking system. Regulatory capital has a macro-prudential motive.
    - ✓ In fact, most financial institutions hold more capital than the regulators require.

1.Risk Capital

➢ Risk capital measurement methods

- Risk capital measurement is based on the same concepts as the value-at-risk (VaR) calculation methodology.
  - ✓ The choice of the confidence level and the time horizon are key policy parameters that should be set by the senior management of the bank and endorsed by the board.
- Risk capital should be calculated in such a way that the institution can absorb unexpected losses up to a level of confidence in line with the requirements of the firm's various stakeholders.

1.Risk Capital

- **Allocating risk capital using economic capital approaches is important.**

① Capital is primarily used in a financial institution not only to provide funding for investments (as for a manufacturing corporation) but also to absorb risk.

② A bank's target solvency is a vital part of the product the bank is selling.

③ Maintaining enough risk capital allows the bank to reduce "agency costs" by convincing external stakeholders, including rating agencies, of the bank's financial integrity.

④ Banks operate in highly competitive financial markets. Risk capital will affect banks' profitability.

2.Risk-Adjusted Return on Capital

- **Risk-Adjusted Return on Capital (RAROC)**

$$\text{RAROC} = \frac{\text{After Tax Risk-Adjusted Return(RAR)}}{\text{Economic Capital(EC)}}$$

- **After tax risk-adjusted return**

$$\text{RAR} = \text{Revenues} - \text{Costs} - \text{Losses} - \text{Taxes} + \text{Return on EC} \pm \text{Transfer}$$

  - ✓ **Transfers** correspond to transfer pricing mechanisms, primarily between the business unit and the treasury group

- **Economic capital=** Risk capital + Strategic capital

Example

- A loan portfolio:
  - Revenues: 85 million USD
  - Expected Loss: 10 million USD
  - Operating Cost (business unit to make the loan): 13 million USD
  - Interest expense:50 million USD
  - Return on EC: 5 million USD
  - EC: 75million USD
- **Answer:**

$$\text{RAROC} = \frac{85 + 5 - 13 - 50 - 10}{75} = 22.7\%$$

2.Risk-Adjusted Return on Capital

- **The use of RAROC**

  ① capital budgeting

  - ✓ ex ante basis
  - ✓ expected revenues and losses should be used
  - ✓ RAROC can be interpreted as the annual after-tax expected rate of return on equity needed to support this project.

  ② performance evaluation

  - ✓ ex post
  - ✓ realized revenues and realized losses in calculation

2.Risk-Adjusted Return on Capital

- **The challenge when apply RAROC framework(cont'd)**

  ① Choose time horizon

  - ✓ how to harmonize the different time horizons used to measure credit, market, and operational risk.
  - ✓ usually adopt a one-year time horizon as a business planning cycle

  ② Choose confidence level

  - ✓ The confidence level in the economic capital calculation should be **consistent** with the firm's target credit rating.
  - ✓ It is the quantitative expression of the risk appetite of the firm.
  - ✓ Setting a lower confidence level may significantly reduce the amount of risk capital.

2.Risk-Adjusted Return on Capital

- **The challenge when apply RAROC framework**

  ③ **measuring of default probability.**

  - ✓ A **point-in-time (PIT) PD**
    - ◆ reasonable for calculating near-term expected losses (EL) and for pricing financial instruments that are subject to credit risk.
  - ✓ A **through-the-cycle (TTC) PD**
    - ◆ reasonable for calculating economic capital, current profitability, and strategic decisions regarding products, geographies, and new business ventures.
    - ◆ TTC reduces the volatility of economic capital, compared to PIT.

2.Risk-Adjusted Return on Capital

➢ Hurdle Rate

- Most firms use a single hurdle rate for all business activities: the **after-tax weighted-average cost of equity capital**.

$$h_{AT} = \frac{CE \times r_{CE} + PE \times r_{PE}}{\text{Common Equity} + \text{Preperred Equity}}$$

✓ The **cost of preferred equity,** r_{PE}, is simply the yield on the firm's preferred shares.

✓ The **cost of common equity,** r_{CE}, is determined via a model such as the CAPM.

$$r_{CE} = r_f + \beta_{CE}(\bar{R}_M - r_f)$$

2.Risk-Adjusted Return on Capital

- **Decision Rule with Hurdle Rate**
  - If the RAROC ratio is greater than the hurdle rate, the activity is deemed to add value to the firm.
  - In the opposite case, the activity is deemed to destroy value for the firm and the activity should be closed down or the project rejected.

3.Adjusted RAROC

- **Adjusting the traditional RAROC**
  - calculation to obtain a RAROC measure that takes into account the systemic riskiness of returns, and for which the hurdle rate is the same across all business lines.

$$\text{Adjusted RAROC} = \text{RAROC} - \beta_E(R_M - r_f)$$

  - The new decision rule
    - ✓ Accept (reject) projects whose adjusted RAROC is greater (smaller) than risk free rate.

Exercise

- The bank wants to adjust the traditional RAROC calculation to obtain a RAROC measures that take into account the systemic riskiness of the expected returns. If the risk-free rate is 1%, and the expected rate of return on the market portfolio is 8% such that the equity risk premium is 7%, and the beta of the firm's equity is 1.6, which of the following project is advisable if RAROC is 13%?

Exercise

A. ARAROC is -7.5% but no, the project is bad because ARAROC is below the risk-free rate.

B. ARAROC is -1.8% but no, the project is bad because ARAROC is below the risk-free rate.

C. ARAROC is 7.5% and yes, the project is good because ARAROC is above the risk-free rate.

D. ARAROC is 1.8% and yes, the project is good because ARAROC is above the risk-free rate.

➢ Correct Answer: D

4.RAROC in Practice

- **Best Practices in Implementing RAROC Approach(cont'd)**

① **Senior management commitment.**

- ✓ sponsor the implementation of a RAROC system
- ✓ promoting a new culture in which performance is measured in terms of contribution to share holder value.

② **Communication and education.**

- ✓ The RAROC group should be transparent and should explain the RAROC methodology to all the management layers of the firm.

③ **Ongoing Consultation.**

- ✓ Firm should institute a forum that periodically reviews the key parameters that drive risk and economic capital.

4.RAROC in Practice

- **Best Practices in Implementing RAROC Approach**

  ④ Maintaining the integrity of the process.

  ✓ a rigorous process of data collection and centralization of financial information.

  ⑤ Combine RAROC with qualitative factors.

  ✓ Maintain a two-dimensional strategy with RAROC return and qualitative assessment of the quality of the earnings.

  ⑥ Put an active capital management process in place.

5.Modeling Diversification Effect

- Risk capital for the firm should be significantly less than the sum of the stand-alone risk capital of the individual business units, which is called **diversification benefits**
- **Challenges in modeling diversification benefits**

① aggregating a firm 's risk capital

- ✓ There is no fully integrated VaR model for a firm.
- ✓ Banks tend to adopt a bottom-up decentralized approach and neglects diversification effects, which will produces an unnecessarily large amount of overall risk capital.

② allocating economic capital to different business lines

- ✓ how do we allocate any diversification benefit that we calculate for the business as a whole back to the business lines?

Range of Practices and Issues in Economic Capital Frameworks

Chapter 13

Framework

1. Challenges within Economic Capital Implementation
2. Benefits of Economic Capital Framework
3. Governance of Economic Capital Framework

Implementation

- **Challenges within Economic Capital Implementation(cont'd)**

① Risk Measures

✓ A bank should understand the limitations of the risk measures it uses, and the implications associated with its choice of risk measures.

② Risk Aggregation

✓ Modeling Diversification benefit is complecated

✓ Harmonisation of the measurement horizon is a difficult issue

③ Validation of Models

✓ The validation of economic capital models is at a very preliminary stage.

Challenges within Economic Capital Implementation(cont'd)

④ Dependency Modeling in Credit Risk

- ✓ The main continues to center on the accuracy and stability of correlation estimates, particularly during times of stress.

⑤ Evaluating Counterparty Credit Risk

- ✓ gathering data from multiple systems
- ✓ measuring exposures from potentially millions of transactions
- ✓ spanning variable time horizons ranging from overnight to thirty or more years
- ✓ tracking collateral and netting arrangements
- ✓ and categorising exposures across thousands of counterparties

Implementation

- **Challenges within Economic Capital Implementation**

  ⑥ **Assessing Interest Rate Risk in the Banking Book**

  - ✓ long holding period for balance sheet assets and liabilities
  - ✓ additional needs to model indeterminate cash flows on both the asset and liability side due to embedded optionality in many banking book items.

2.Benefits of Economic Capital Framework

- **Benefit and impacts of using economic capital framework(cont'd)**

① **Credit Portfolio Management**

✓ A loan with a higher stand-alone risk does not necessarily contribute more risk to the portfolio. A loan's marginal contribution to the portfolio, as a result, is critical to assessing the concentration of the portfolio. Economic capital is a measurement of the level of concentration.

② **Risk Based Pricing**

✓ Risk-based pricing typically incorporates the variables of a value-based management approach.

✓ For example, the application of RAROC.

2.Benefits of Economic Capital Framework

- **Benefit and impacts of using economic capital framework**

  ③ Customer Profitability Analysis

  - ✓ It aims at providing a broad and comprehensive view of all the costs, revenues and risks (and consequently, economic capital absorption) generated by each single customer relationship.
  - ✓ The analysis is complicated in that many risks need to be aggregated at the customer level.

  ④ Management Incentives

  - ✓ the use of economic capital needs to be extended in a way that directly affects the objective functions of decision-makers at the business unit level.
  - ✓ This is achieved by influencing the incentive structure for business-unit management.

3.Governance of Economic Capital Framework

- **Concerns with regard to governance of economic capital framework(cont'd)**
  - ① senior management involvement and experience in the economic capital process
  - ② the unit involved in the economic capital process and its level of knowledge;
    - ✓ For less centralized firms, allocate capital to the business unit.
    - ✓ For more centralized firms, management is likely to be more involved in the allocation of capital.

3.Governance of Economic Capital Framework

- **Concerns with regard to governance of economic capital framework**

③ the frequency of economic capital measurements

- ✓ data quality is a prominent concern.
- ✓ most banks calculate economic capital on a monthly or quarterly basis.

④ policies, procedures, and approvals relating to economic capital model development, validation, on-going maintenance and ownership.

- ✓ Diagnostics procedures are typically run after an economic capital model change
- ✓ Some banks specifically name an owner of the economic capital model. However, few formal responsibilities are assigned the owner.

Capital Planning at Large Bank Holding Companies

Chapter 14

Framework

1. Federal Reserve's Capital Plan Rule
2. Capital Adequacy Process

1.Federal Reserve's Capital Plan Rule

- **Capital in Bank Holding Company**
  - Capital is central to a Bank Holding Companies' ability to absorb unexpected losses and continue to lend to creditworthy businesses and consumers.
- **Federal Reserve's Capital Plan Rule**
  - The Federal Reserve's Capital Plan Rule requires all U.S.-domiciled, top-tier BHCs with total consolidated assets of $50 billion or more to develop and maintain a capital plan supported by a robust process for assessing their capital adequacy.
  - Comprehensive Capital Analysis and Review (CCAR) is the Federal Reserve's supervisory program for assessing the capital plans.

2.Capital Adequacy Process

- **Seven Principles of Capital Adequacy Process**

① Sound **Foundational Risk Management**

✓ a sound risk-measurement and risk-management infrastructure

② Effective **Loss-Estimation Methodologies**

✓ estimates of potential losses over a range of stressful scenarios

③ **Solid Resource-Estimation** Methodologies:

✓ a clear definition and estimation of available capital resources.

④ Sufficient Capital Adequacy **Impact** Assessment

⑤ Comprehensive **Capital Policy** and Capital Planning

⑥ Robust **Internal Controls**

⑦ Effective **Governance**

2.Capital Adequacy Process

- **Practices for effective capital adequacy process in BHCs(cont'd)**

① Risk identification

✓ all risks are appropriately accounted for

✓ regularly update risk assessments and review risk exposures

② Internal controls

✓ **Independent** model review and validation

③ Corporate governance

④ Capital policy

✓ setting of capital goals and targets

✓ setting of capital contingency plan

2.Capital Adequacy Process

- **Practices for effective capital adequacy process in BHCs**

⑤ Stress testing and stress scenario design

✓ reflect an individual company's unique vulnerabilities

⑥ Estimating losses, revenues, and expenses

✓ quantitative and qualitative methodologies(expert judgment)

⑦ Assessing the impact of capital adequacy

✓ risk-weighted asset (RWA) and balance sheet **projections**

Stress testing in Banks

Chapter 15

Framework

1. The Historical Evolution of Stress Testing
2. Stress Testing Design
3. Executing the Stress Scenario

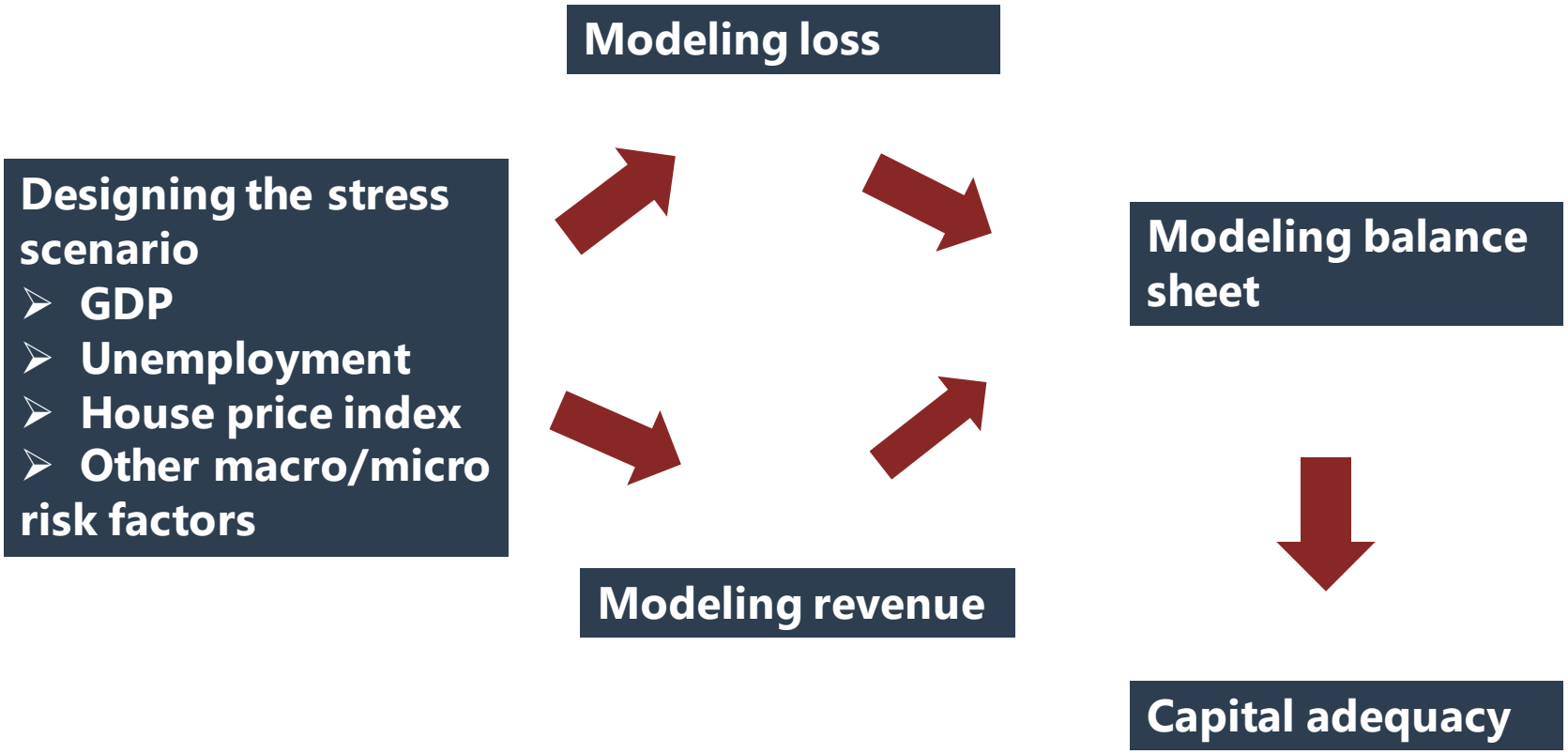
1. The Historical Evolution of Stress Testing

- **The time line of three stress testing process**
  - SCAP(US, March 2009)
    - ✓ all banks with assets greater than 100bn conducted stress test
    - ✓ the first of the macro-prudential stress tests using a broad macro scenario with market-wide stresses(Unemployment, GDP growth, HPI)
    - ✓ focusing firm-wide losses
    - ✓ All tied to a post-stress capital ratio to ensure a going concern.
  - EBA(EU, July 2011)
    - ✓ Retail and corporate only
  - CCAR(US, March 2012)
    - ✓ asking banks to develop their own stress scenario(s)

2.Stress Testing Design

- **Coherence in designing stress scenarios**
  - The scenarios are inherently multi-factor.
    - ✓ when one risk factor moves significantly, the others don't stay fixed.
    - ✓ The real difficulty is in specifying a coherent joint outcome of all the relevant risk factors.
  - Compounding the problem is the challenge of finding a scenario where the real and financial factors are jointly coherent.

3.Executing the Stress Scenario



3.Executing the Stress Scenario

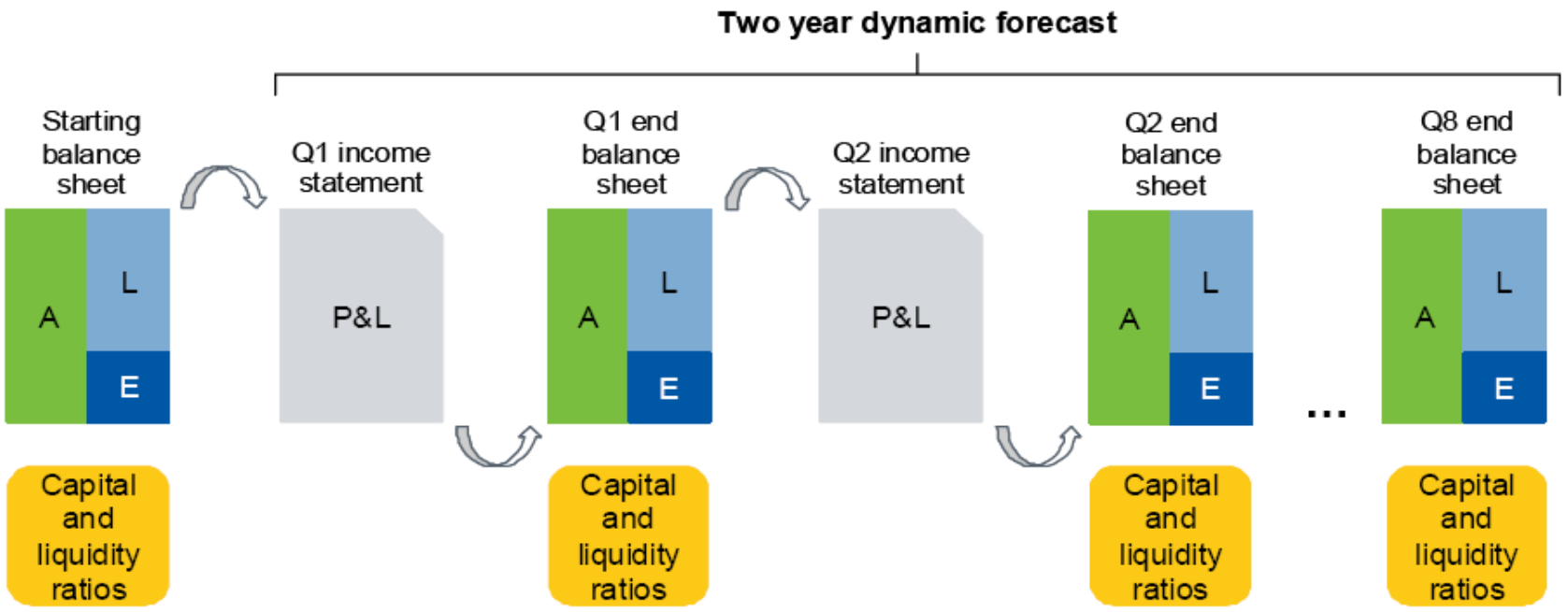


Figure 2: Stress testing balance sheet and income statement dynamics.

Guidance on Managing Outsourcing Risk

Chapter 16

Framework

1. Risks From the Use of Service Providers
2. Service Provider Risk Management Programs

1.Risks From the Use of Service Providers

- Financial institutions should consider the following risks before entering into and while managing outsourcing arrangements. **(cont'd)**

  ① **Compliance risks** arise when the services, products, or activities of a service provider fail to comply with applicable U.S. laws and regulations.

  ② **Concentration risks** arise when outsourced services or products are provided by a limited number of service providers or are concentrated in limited geographic locations.

  ③ **Reputational risks** arise when actions or poor performance of a service provider causes the public to form a negative opinion about a financial institution.

1.Risks From the Use of Service Providers

- Financial institutions should consider the following risks before entering into and while managing outsourcing arrangements.

④ **Country risks** arise when a financial institution engages a foreign-based service provider, exposing the institution to possible economic, social, and political conditions and events from the country where the provider is located.

⑤ **Operational risks** arise when a service provider exposes a financial institution to losses due to inadequate or failed internal processes or systems or from external events and human error.

⑥ **Legal risks** arise when a service provider exposes a financial institution to legal expenses and possible lawsuits.

2.Service Provider Risk Management Programs

- Effective programs to manage outsourcing risks usually include the following core elements:**(cont'd)**

  ① Risk assessments;

  ② Due diligence and selection of service providers;

  ③ Contract provisions and considerations;

  ④ Incentive compensation review;

  ⑤ Oversight and monitoring of service providers; and

  ⑥ Business continuity and contingency plans.

2.Service Provider Risk Management Programs

- The overall due diligence process includes a review of:
  - Business background, reputation, and strategy
    - ✓ Evaluate experience, check its references to ascertain its performance record, and verify any required licenses and certifications.
  - Financial performance and condition
    - ✓ recent financial statements
    - ✓ The adequacy of its insurance coverage and review of the financial condition of any subcontractors.
  - Operations and internal controls
    - ✓ Privacy protection of the financial institution's confidential information
    - ✓ Maintenance and retention of records
    - ✓ Business resumption and contingency planning

2.Service Provider Risk Management Programs

- Elements of well-defined contracts and service agreements usually include:**(cont'd)**

① Scope: the rights and responsibilities of each party

② Cost and compensation

③ Right to audit

④ Establishment and monitoring of performance standards

⑤ Confidentiality and security of information

⑥ Ownership and license

⑦ Indemnification: the loss results from service provider's negligence

⑧ Default and termination

⑨ Limits on liability: Service providers may want to contractually limit their liability

2.Service Provider Risk Management Programs

- Elements of well-defined contracts and service agreements usually include:

⑩ Dispute resolution

⑪ Insurance: Service providers should have adequate insurance and provide financial institutions with proof of insurance.

⑫ Customer complaints

⑬ Business resumption and contingency plan of the service provider

⑭ Foreign-based service providers

⑮ Subcontracting

- ✓ If agreements allow for subcontracting, the same contractual provisions should apply to the subcontractor.

Associated with Money Laundering and Financing of Terrorism

Chapter 17

Framework

1. Best Practices related to ML/FT Risk

1.Best Practices Related to ML/FT Risk

- Application of **standard practices**
  - Governance Arrangements
    - ✓ The board of directors should approve and oversee risk assessments, policies, organization, risk management and compliance in the specific context of ML/FT.
    - ✓ To that end, a chief ML/FT officer should be appointed.
  - As in other risk areas, banks are expected to have three lines of defense
    - ✓ Business units
    - ✓ The risk function and/or the function under the chief MUFT officer
    - ✓ Internal auditors and/or external equivalents

1.Best Practices Related to ML/FT Risk

- Application of best practices with **risk assessment**
  - All relevant risk factors at the country, sector, bank and business relationship levels should be considered. Characteristics of the customer base, products and services offered, and delivery channels should be considered.
  - For each customer or business relationship, a profile of normal activity should be built to support identification of abnormal activity.
  - Risk assessments should be documented for potential inspection by authorities.
  - International banks should be attentive to national risk assessments and country reports.

1.Best Practices Related to ML/FT Risk

- Application of best practices with **customer due diligence and acceptance**
  - Written policies and procedures should exist to ensure that a customer is not accepted, and business is not done, until the customer's identity has been satisfactorily established
  - **Politically exposed persons (PEP),** such as former high government officials, may pose higher risk
  - Consider the potential customer's background, occupation, source of wealth and income, and country of origin and residence
  - Though information about a customer's previous banking relationships may be helpful, but not sufficient
  - Banks may be permitted to rely on third parties for some customer due diligence but should take be ultimately responsible

1.Best Practices Related to ML/FT Risk

- Application of best practices with r**isk mornitoring**
  - A profile of normal activity and transactions must be built to aid identification of abnormal activity, such as unusual business relationships and transactions.
  - Changes in a customer's risk profile should trigger changes in the intensity of monitoring.
  - The larger and more complex the bank and its businesses, and the more international its operations, the more likely that automated monitoring applications will be needed.
  - Especially where required by law, suspicious activity revealed by monitoring should be reported to appropriate law enforcement authorities.
  - **Wire transfers** are accomplished by sending payment messages among banks. Information about the originating bank and the customer should appear in the messages

Regulation of the OTC Derivatives Market

Chapter 18

Framework

1. Clearing Process in OTC markets
2. Post-Crisis Regulatory Changes
3. Impact of the Changes

1.Clearing Process in OTC markets

- Central Clearing: **the CCP acts as an intermediary and enters into offsetting transactions with the two companies**
  - Initial Margin is calculated so that there is a 99% probability that it will cover market moves over five days.
  - Variation margin is the collateral posted to reflect the **change** in the value of a derivatives portfolio.
  - Cash, or securities can be posted instead of cash with a *haircut*.
- Bilateral Clearing
  - Typically this is an ISDA master agreement. An annex, known as the credit support annex (CSA), defines collateral arrangements.
  - Netting states that all transactions between two parties can be considered to be a **single transaction**
    - ✓ **Netting reduces credit risk**
    - ✓ **Netting can also save initial margin**

2.Post-Crisis Regulatory Changes

- **Reasons for regulatory change**
  - The OTC derivatives market was considered by many to have been partly responsible for the 2008 credit crisis. When the G20 leaders met in Pittsburgh in September 2009 in the aftermath of the 2008 crisis, they wanted to reduce systemic risk by regulating the OTC market.
- As a result, there are **three major changes** affecting OTC derivatives:**(cont'd)**
  - ① A requirement that all standardized OTC derivatives be cleared through CCPs.
  - ② A requirement that standardized OTC derivatives be traded on electronic platforms.
  - ③ A requirement that all trades in the OTC market be reported to a central trade repository.

2.Post-Crisis Regulatory Changes

① A requirement that **all standardized OTC derivatives be cleared through CCPs.**

- Standardized derivatives include **plain vanilla interest rate swaps** (which account for the majority of OTC derivatives traded) and default swaps on credit indices.
- The purpose of this requirement is to reduce **systemic risk**.
- It leads to derivatives dealers having **less credit exposure to each other** so that their interconnectedness is less likely to lead to a collapse of the financial system.

2.Post-Crisis Regulatory Changes

② A requirement that **standardized OTC derivatives be traded on electronic platforms.**

- This is to improve **transparency**.
- If there is an electronic platform for matching buyers and sellers, the prices at which products trade should be readily **available to all market participants**. E.g.
  - ✓ Swap execution facilities (SEFs) in the United States
  - ✓ Organized trading facilities (OTFs) in Europe
- In practice, standardized products once they have been traded on these platforms are passed automatically to a CCP.

2.Post-Crisis Regulatory Changes

③ A requirement that **all trades** in the OTC market **be reported to a central trade repository**.

- This requirement provides regulators with important information on the risks being taken by participants in the OTC market. (lesson from AIG)

➢ The **first two of these requirements** apply only to **cleared transactions**, which occurs between two financial institutions (or between a financial institution and a nonfinancial company that is considered to be systemically important because of the volume of its OTC derivatives trading), while the **third one** apply to all trades.

2.Post-Crisis Regulatory Changes

- The rules regarding **uncleared trades**
  - Regulations, which are being implemented between 2016 and 2020, require uncleared trades to be subject to rules on the **margin** that has to be posted.
    - ✓ Both **initial margin and variation margin** must be posted for uncleared trades by both sides.
    - ✓ Variation margin was fairly common in the OTC market pre-crisis, but initial margin was rare.
    - ✓ When entering into a transaction with a **much less creditworthy counterparty**, a derivatives dealer might insist on the counterparty posting initial margin. But the posting of initial margin by both sides was almost unheard of in the bilaterally cleared market.

3.Impact of the Changes

- Three major impacts on the changes
  - Liquidity
    - ✓ Most of the collateral required will have to be in the form of cash or government securities, so the collateral posted at any given time will be a drain on liquidity.
  - Rehypothecation
    - ✓ Rehypothecation will be restricted, which allows initial margin to be rehypothecated once, but only if certain conditions are satisfied. Variation margin can be rehypothecated.
  - The Convergence of OTC and Exchange-Traded Markets
    - ✓ Similarity in platforms and clearing process.
    - ✓ exchanges are increasingly offering less standard product

The Basel Accord

199-310

Capital Regulation Before the Global Financial Crisis

Chapter 19

Framework

1. Basel I
2. 1995&1996 Amendments
3. Basel II
4. Solvency II

1.Basel I

- **The Basel I Accord laid down 2 new terms regarding capital:**
  - **Cooke Ratio** as one of the primary regulatory requirement. The Cooke ratio was used to compute minimum capital that a bank was required to keep vis-à-vis the risk associated to its on & off-balance sheet assets called risk-weighted assets (RWA), a measure of the bank's total credit exposure.
  - **Risk-Weighted Assets (RWA)** is a bank's assets weighted according to risk. The total (credit) risk-weighted assets for a bank will be sum of its On & Off balance sheet risk-weighted assets. Credit risk exposures can be divided into three categories:
    - ✓ Those arising from on-balance sheet assets (excluding derivatives)
    - ✓ Those arising for off-balance sheet items (excluding derivatives)
    - ✓ Those arising from over-the-counter derivatives

1.Basel I

- **Risk Weights for On-Balance-Sheet Items**

Risk Weight (%)	Asset Category
0	Cash, Gold Bullion, Claims on OECD Governments such as Treasury Bonds or Insured Residential Mortgages.
20	Claims on (Loans to) OECD Banks and OECD Public Sector Entities such as Securities issued by U.S. Government Agencies or Claims on Municipalities.
50	Uninsured Residential Mortgage Loans
100	All Other Claims such as Corporate Bonds and Less-Developed Country Debt, Claims on non-OECD Banks.

Example

- The asset of a bank consist of $100 million of corporate loans, $10 million of OECD government bonds, and $50 million of residential mortgages. The total risk-weighted assets is?
- Solution:

$$1.0\times100+0.0\times10+0.5\times50 = 125\text{million}$$

1.Basel I

- **Risk Weights for Off-Balance-Sheet Items (non-derivative)**
  - This includes bankers' acceptances, guarantees, and loan commitments.
  - A **credit equivalent amount** is calculated by applying a conversion factor to the principal amount of the instrument.

    Off-balance sheet asset × Conversion Factor(%)

    ✓ Instruments that from a credit perspective are considered to be similar to loans, such as bankers' acceptances, have a **conversion factor of 100%**.

    ✓ Others, such as note issuance facilities (where a bank agrees that a company can issue short-term paper on pre-agreed terms in the future), have **lower conversion factors**.
  - Risk-weighted asset can be calculated by multiplying **credit equivalent amount** with **risk weight.**

1.Basel I

➢ Risk Weights for Off-Balance-Sheet Items (over-the-counter derivative)

- Such as an interest rate swap or a forward contract.
- Credit equivalent amount= Max(V, 0) + αL
  - ✓ Alpha is determined by the nature of the asset

Remaining Maturity	Interest Rate(%)	Foreign Exchange Rate & Gold(%)	Equity (%)	Precious Metals (except Gold) (%)	Other Commodities(%)
<1	0.0	1.0	6.0	7.0	10.0
1 to 5	0.5	5.0	8.0	7.0	12.0
>5	1.5	7.5	10.0	8.0	15.0

- Risk-weighted asset can be calculated by multiplying **credit equivalent amount** with **risk weight.**
  - ✓ The risk weights are similar to **Risk Weights for On-Balance-Sheet Items** except that the risk weight for a corporation is 0.5 rather than 1.0.

Example

- A bank has entered into a $100 million interest rate swap with a remaining life of four years. The current value of the swap is $2.0 million. Compute the credit equivalent amount of the swap contract and the RWA if:
  - a) The counterparty is a non OECD bank;
  - b) The counterparty is an OECD bank.
  - c) The counterparty is a corporate customer.
- Solution:

  Credit equivalent amount = Max(V, 0) + αL=2+0.5%×100=2.5million
  - a)The counterparty is a non OECD bank : 2.5×100%=2.5million
  - b) The counterparty is an OECD bank: 2.5×20%=0.5million
  - c) The counterparty is a corporate customer: 2.5×50%=1.25million

2.1995&1996 Amendments

- **As Basel I was being developed,**
  - the 1987 stock market crash had not yet occurred,
  - value-at-risk (VaR) was not in widespread use,
  - quantitative market risk management was in its infancy.
- **The 1995&1996 Amendment was established then to**
  - Take netting into consideration when calculate RWA
  - Added a capital charge for market risk

2.1995&1996 Amendments

- At the beginning, the 1988 Basel Accord did not take netting into account, the **credit equivalent amount** for a portfolio of derivatives is:

$$\sum_{i=1}^{N}[\max(V_i, 0) + \alpha_i L_i]$$

- Later on, the 1988 Accord was modified to allow banks to reduce their credit equivalent totals when enforceable bilateral netting agreements were in place.
  - **Step 1:** Calculate the NRR(net replacement ratio, same with netting factor):
  - **Step 2**: Calculate the credit equivalent amount is:

$$\max(\sum_{i=1}^{N} V_i, 0) + (0.4 + 0.6 \times NRR)\sum_{i=1}^{N} \alpha_i L_i$$

2.1995&1996 Amendments

- The amendment separates the bank's assets into two categories, **the trading book and the banking book.**
  - The trading book represents the bank portfolio with financial instruments that are intentionally held for short-term resale and typically marked to market.
  - The banking book consists of other instruments, mainly loans, that are held to maturity and typically valued on a historical cost basis.
- **Added a capital charge for market risk using either**
  - a **standardized model**
    - ✓ Five categories of market products with no diversification
  - an **internal models approach(IMA)*, [99%, 10 day VaR]**
    - ✓ $\text{Max}(\text{VaR}_{t-1}, m_c \times \text{VaR}_{avg})+\text{SRC}$

3.Basel II

- While retaining much of Basel I, Basel II contained **four significant innovations**

I. **Risk weight formulas** for credit risk based on modern credit risk management concepts and **banks' internal risk measures**;

II. **Required capital for operational risk**, in addition to credit risk and market risk

III. In addition to minimum capital requirements (**Pillar 1**), Basel II included specific requirements for supervision related to capital and risk management (**Pillar 2**) and required public disclosures (**Pillar 3**).

IV. Repeated use of **Quantitative Impact Studies (QIS)** to fine-tune the design of the accord. In each QIS, banks contributed detailed data which was then analyzed by supervisors.

3.Basel II

- **Required capital for credit risk(cont'd)**

① The standardized approach

✓ Banks that are not sophisticated and do not have the technical expertise & resources to build their own models adopt **standardized approach**.

② The IRB approach

✓ use a bank's own internal estimates for calculation

✓ It has the potential to **reduce the capital requirement for banks** because their own estimates of risk may be lower.

◆ the capital requirement under IRB **cannot be less than 90%** of the capital requirement **the previous year.**

◆ the capital requirement under IRB **cannot be less than 80%** of the prior requirement **after two years.**

3.Basel II

① The standardized approach compared with Basel I(cont'd)

I. the risk weights depend on the assessments made by external credit assessment institutions recognized by supervisors.

✓ For country, bank and corporation customers:

	AAA to AA-	A+ to A-	BBB+ to BBB-	BB+ to BB-	B+ to B-	Below B-	Unrated
Country	0	20	50	100	100	150	100
Banks	20	50	50	100	100	150	50
Corporations	20	50	100	100	150	150	100

✓ Individual customers

◆In retail banking a general risk weight of 75% is applied.

◆If the loan is secured either by residential mortgage or by commercial real estate, a fixed risk weight of 35% & 100% is applied.

Example

- Consider the assets of a bank consist of $100 million of loans to corporations rated A, $10 million of government bonds rated AAA, $50 million of residential mortgages. Calculate the total RWA under Basel Ⅱ.
- Solution:

$$0.5\times100 + 0.0\times10 + 0.35\times50 = 67.5\text{million}$$

3.Basel II

① The standardized approach compared with Basel I

II. Adjustments for Collateral, two approaches

- ✓ **Simple Approach**
- ✓ **Comprehensive Approach**

3.Basel II

- **Simple Approach**
  - Risk weights are designated for each collateral type, subject to **a floor of 20 percent**.
  - The risk weight is **replaced by the risk weight of the collateral** for the part of the exposure covered by the collateral.

- Suppose that a $90 million exposure to a particular counterparty is secured by collateral worth $80 million. The collateral consists of bonds issued by an A-rated company. The counterparty has a rating of B+. The risk weight for the counterparty is 150% and the risk weight for the collateral is 50%. Calculate the risk-weighted assets applicable to the exposure using the simple approach.
- Solution:

$$RWA = 1.5\times(90-80) + 0.5\times80 = 55 \text{ million}$$

3.Basel II

- **Comprehensive Approach**
  - Banks adjust the size of their exposure upward to allow for possible increases and adjust the value of collateral downward to allow for possible decreases.
  - New Exposure = adjusted exposure - adjusted value of the collateral =original exposure×(1 + adjustment Factor) - original collateral×(1 – adjustment Factor)
  - counterparty's risk weight is applied to this exposure.

- Given the previous data, consider the adjustment to exposure to allow for possible future increases in the exposure is +10% and the adjustment to the collateral to allow for possible future decreases in its value is -15%. Calculate the new exposure as per Comprehensive Approach and RWA if the risk-weight to be applied to the exposure is 150%.
- Solution:

$$\text{New Exposure} = 90\times(1 + 0.1) - 80\times(1 - 0.15) = 31 \text{ million}$$

$$\text{RWA} = 31\times1.5 = 46.5 \text{ million}$$

3.Basel II

- **The IRB approach**
  - The capital requirement is derived on the basis of Value-at-Risk calculated using the one-year time horizon at a 99.9% confidence level. The VaR thus computed comprises of Expected & Unexpected Losses

$$\text{Credit capital} = \sum_{i} \text{EAD}_i \times \text{LGD}_i \times \text{WCDR}_i(99.9\%, 1\ year) - EL$$

- **Two forms of IRB**
  - Foundation IRB
    - ✓ the bank would provide only the PD, with the accord specifying values of EAD and LGD for each class of asset
  - Advanced IRB
    - ✓ the bank would provide all three values.

3.Basel II

- **Required capital for operational risk(cont'd)**
  - ① Basic Indicator Approach
  - ② Standardized Approach
  - ③ Advanced Measurement Approach

3.Basel II

① Basic Indicator Approach

- This is the simplest approach for computing operational risk capital requirement.
- It is computed by multiplying a constant factor of 0.15 with the bank's average annual gross income over the last three years, as shown in the formula below:

$$\mathrm{BIA} = 0.15 \times \left[\frac{\sum_{i=1}^{n} \mathrm{GI}_i}{n}\right]$$

Usually n=3,if GI_i<0,n is the number of positive GI.

- Average annual gross income: this is taken as the average of positive gross income numbers over the past three years. Negative values are exclude.

3.Basel II

② **Standardized Approach:** 8 business line with different beta factors

Business Line	Beta Factor
Corporate Finance	18%
Trading and Sales	18%
Retail Banking	12%
Commercial Banking	15%
Payment and Settlement	18%
Agency Services	15%
Asset Management	12%
Retail Brokerage	12%

$$K_{SA} = \left\{ \sum_{\text{years } 1-3} \max \left[\sum (GI_{1-8} \times B_{1-8}), 0 \right] \right\} / 3$$

3.Basel II

③ Advanced Measurement Approach

- Estimate a distribution of operational risk losses in **seven categories**
- The required capital computation under approach is also (similar to IRB approach for credit risk) derived as 99.9%, 1 year VaR measured using probability distribution of losses.

Operational risk capital=WCL-EL.

- Two popular approaches
  - ✓ A parametric and Monte Carlo approach, in which data are used to parameterize the bank's choice of probability distribution for incidence (e.g., Poisson) and for severity (e.g., Weibull).
  - ✓ Generate a moderate number of detailed scenarios in which losses occur, and then measure operational losses in each scenario.

3.Basel II

- **Menu of Approaches to Measure Risk**

Risk Category	Allowed Approach
Credit	Standardized Approach Internal Ratings Based Approach
Market	Standardized Approach Internal Models Approach
Operational	Basic Indicator Approach Standardized Approach Advanced Measurement Approach

3.Basel II

- **Three Pillars under Basel II**
  - **Pillar 1: Minimum Capital Requirement**
    - ✓ Banks now have a wider choice of models for computing their risk charges.
    - ✓ BCBS still tried to keep constant the total level of capital in the global banking system, at 8% of risk-weighted assets.
  - **Pillar 2: Supervisory Review Process.** Supervisors need to ensure that:
    - ✓ Banks have a process in place for assessing their capital in relation to risks.
    - ✓ Banks indeed operate above the minimum regulatory capital ratios.
    - ✓ Corrective action is taken as soon as possible when problems develops.
  - **Pillar 3: Market Discipline**
    - ✓ Emphasizes the importance of risk disclosures in financial statements.

3.Basel II

➢ Capital Ratio Requirement

- The total capital ratio must be no lower than 8%. The credit risk charge is 8% of credit risk-weighted assets. The MRC and ORC are computed using another approach.

$$\frac{\text{Total Capital}}{\text{RWA}_{\text{Credit}} + [\text{MRC}_{\text{Market}} \times 12.5] + [\text{ORC}_{\text{Op}} \times 12.5]} \geq 8\%$$

➢ Risk Weighted Assets (RWA)

- Total risk weighted assets (RWA) are determined by multiplying the capital requirements for market risk and operational risk by 12.5 and adding the resulting figures to the sum of RWA for credit risk.

Exercise

- ABC Bank's current assets and capital are provided in the table below:

Risk-Weighted Assets	USD Millions
Total Risk-Weighted for Credit Risk	889
Total Capital Charge for Market Risk	26
Total Capital Charge for Operational Risk	20
Total Capital	131

With respect to the Basel II, what is ABC's current ratio of total regulatory capital to risk-weighted assets.

A. 5.94%

B. 8.40%

C. 8.95%

D. 13.16%

Correct Answer: C

4.Solvency II

➢ Introduction

- Regulatory framework for insurance companies to prescribe minimum capital levels for investment risk, underwriting risk, and operational risk.
  - ✓ Investment risk is subdivided into market risk and credit risk.
  - ✓ Underwriting risk is subdivided into risk arising from life insurance, non-life insurance (i.e., property and casualty), and health insurance.
- Two capital requirement in Solvency II(cont'd)
  - ① Solvency Capital Requirement (SCR)
  - ② Minimum Capital Requirement (MCR)

4.Solvency II

① Capital Requirement – Solvency Capital Requirement (SCR)

- Two way to calculate SRC: The standardized approach and internal models approach(**one year, 99.5% VaR calculation**).
- If the capital falls below the prescribed SCR level then the company should, at minimum, deliver to the supervisor a plan to restore capital to above the SCR level. The supervisor might require the insurance company to take particular measures to correct the situation.

② Capital Requirement – Minimum Capital Requirement (MCR)

- The MCR will typically be between 25% to 45% of the SCR.
- If the capital at any point of time falls below the MCR then the supervisor at its own discretion can ask the company to stop engaging into any new business. Apart from imposing the restrictions on taking new business, supervisor can even liquidate the company or transfer the company's business to another organization.

and Other Regulation After the Global Financial Crisis

Chapter 20

Framework

1. Basel II.5
2. Basel III
3. Other rules after crisis

1.Basel II.5

- **Basel's concerning 1: The traditional HS VaR model has ghost effect.**
  - The Stressed Value at Risk (SVaR) is calculated by combining current portfolio performance data based on the 10-day, 99% confidence interval with the firm's historical data from a significantly financial stressed period of the same portfolio. The formula for SVaR is given as:

$$\mathrm{Max}(\mathrm{SVaR}_{t-1}, \mathrm{M_s} \times \mathrm{SVaR}_{avg})$$

  - Multiplicative Factor (M_S) is set by respective supervisory authorities depending on the risk management system quality, subject to a floor of 3.

1.Basel II.5

- **Basel's concerning 2:** Exposures in the trading book were attracting less capital than similar exposures in the banking book.
  - To address this disparity, in 2005, Regulators proposed an "incremental default risk charge(IDRC)".
  - In 2008, regulators noticed that defaults were not the only factor contributing to the 2008 crisis. The Basel committee amended its previous IDRC proposal as **Incremental Capital Charge (IRC).**
  - The IRC requires banks to calculate a **one-year 99.9% VaR** for losses from credit sensitive products in the trading book taking both credit rating changes and defaults into account.

1.Basel II.5

➢ Market Risk Capital

$$\text{Max}\left\{\text{M}\frac{1}{60}\sum_{i=1}^{60}\text{VaR}_{t-i},\text{VaR}_{t-1}\right\}+\text{Max}\left\{\text{M}_s\frac{1}{60}\sum_{i=1}^{60}\text{SVaR}_{t-i},\text{SVaR}_{t-1}\right\}+\text{SRC}_t+\text{IRC}_t$$

VaR_{avg} SVaR_{avg}

- The multiplication factor M and M_s has an absolute minimum value of 3.
  - ✓ (M) depends on the backtesting results
  - ✓ (M_S) is set by respective supervisory authorities

1.Basel II.5

➢ Comprehensive Risk Measure (CRM)

- The CRM is a single capital charge replacing the incremental risk charge and the specific risk charge for instruments dependent on credit correlation.
- very important measure for a portfolio of instruments that are sensitive to the correlation between the default risks of different assets such as
  - ✓ asset-backed securities (ABSs)
  - ✓ collateralized debt obligations (CDOs).
- CRM can be calculated with standardized approach or internal models with supervisory approval.

2.Basel III

- **There are several reasons the Committee has acted at this time, many of which are related to the problems that lead to and exacerbated the recent financial crisis:**
  - I. A gradual erosion of the amount of capital and the quality of the capital base in banks across the globe.
  - II. Procyclical deleveraging.
  - III. The inability of the banking system to handle the large off-balance sheet exposures. Excessive on- and off-balance sheet leverage at banks worldwide.
  - IV. Insufficient liquidity at many banks, which made it impossible for the banking system to absorb the shocks and ultimate trading and credit losses.
  - V. The systemic risk that resulted from interconnectedness of commercial and investment banks that in the end spread to the real economy.
  - VI. A loss of confidence in the banking system, specifically with respect to the solvency and liquidity of many financial institutions.

2.Basel III

- **Basel III has made changes in five major areas(cont'd)**

① Capital Requirements

② Introducing buffers

- ✓ capital conservation buffer
- ✓ countercyclical buffer
- ✓ special rules for globally systemically important banks (G-SIBs)

③ Leverage Ratio Capital Requirements

④ Ratios intended to improve the management of liquidity risk

- ✓ liquidity coverage ratio
- ✓ Net stable funding ratio

⑤ Contingent convertible bonds (CoCos)

2.Basel III

① Capital Requirements(cont'd)

- Total capital of a bank as per Basel III guidelines consist of:
  - ✓ **Tier 1 Equity Capital**: (also known as core Tier 1 capital) includes common share capital and retained earnings but does not include goodwill or deferred tax assets.
  - ✓ **Additional Tier 1 Capital**: consists of items, such as non-cumulative preferred stock, that were previously Tier 1 but are not common equity.
  - ✓ **Tier 2 Capital**: includes debt that is subordinated to depositors with an original maturity of five years.
  - ✓ Tier 3 capital has been completely **removed.**

2.Basel III

① Capital Requirements

- Minimum Capital Requirement
  - ✓ Tier 1 equity capital must be at least **4.5%** of risk-weighted assets at all times.
  - ✓ Total Tier 1 capital (Tier 1 equity capital plus additional Tier 1 capital) must be at **6%** of risk-weighted assets at all times.
  - ✓ Total capital (total Tier 1 plus Tier 2) must be at least **8%** of risk-weighted assets at all times.

2.Basel III

② Introducing buffers(cont'd)

- Capital Conservation Buffer(CCB)
  - ✓ The banks are expected to build this buffer capital during normal times to compensate losses incurred during period of stress.
  - ✓ It is core Tier 1 capital equal to 2.5% of risk weighted assets.
- Countercyclical Buffer(CCyB)
  - ✓ encourage banks to build up buffers in good times that can be drawn down in bad ones and to dampen the effect of **procyclical amplification**
  - ✓ The amount is defined at the discretion of the regulatory authorities of different countries but the maximum buffer as defined in the Basel III accord is 2.5% of total risk-weighted assets.
  - ✓ The buffer must be built with Tier 1 equity capital only.

2.Basel III

② Introducing buffers(cont'd)

- Banks that do not meet the capital conservation buffer or countercyclical buffers will be subject to

  ✓ constraints on capital distributions of dividends

Tier 1 Equity Capital Ratio	Minimum Percentage of Earnings Retained
4.000% to 5.125%	100%
5.125% to 5.750%	80%
5.750% to 6.375%	60%
6.375% to 7.000%	40%
7%	0%

  ✓ stock repurchases

  ✓ discretionary bonuses to staff.

2.Basel III

② Introducing buffers

- Regulations for global systemically important banks**(G-SIBS)**
  - ✓ G-SIBs are required to keep CET1 capital equal to a **baseline 4.5%** of risk-weighted assets plus a **further 2.5%** for the capital conservation buffer **plus any extra amounts (1%~3.5%)** required by national supervisors.
  - ✓ Extra amounts do not include capital requirements required by national supervisors, such as the countercyclical buffer.

2.Basel III

③ Leverage Ratio Capital Requirement

- Introduced a limit on the leverage ratio. This is because some banks had adequate capital using the Basel II rules but ran into difficulties because of their high leverage.
- It is meant to act as a supplementary measure to risk-based capital standards.

$$\text{Leverage Ratio} = \frac{\text{Tier 1 capital}}{\text{Total Exposure}} \geq 3\%$$

  - ✓ The **numerator** will consist of high-quality capital (i.e., the new definition of Tier 1 capital).
  - ✓ The **denominator** will consist of on- and off-balance sheet (derivatives, stand-by letters of credit, acceptances, and so on) items and/or exposures.
- Basel III specifies a minimum leverage ratio of 3%.

2.Basel III

④ Ratios to improve liquidity—— Liquidity Coverage Ratio(cont'd)

- The ratio of the high-quality liquid assets to the net cash outflows over 30 days must be greater than 100%.
- It allow the bank to convert assets into cash to meet liquidity needs under a stress scenario.

$$\text{LCR} = \frac{\text{High Quality Liquid Assets}}{\text{Net Cash outflows in 30 days}} \geq 100\%$$

✓ For cash inflows, banks will not be permitted to double count items,

◆i.e. if an asset is included as part of the stock of HQLA, the associated cash inflows cannot also be counted as cash inflows.

2.Basel III

④ Ratios to improve liquidity—— Net Stable Funding Ratio (NSFR)

- NSFR focuses on liquidity management over a period of one year i.e. long-term financial resources must exceed long-term commitments.

$$\text{NSFR} = \frac{\text{Amount of Stable Funding}}{\text{Required Amount of Stable Funding}} \geq 100\%$$

- **For the numerator**, depending on the type of funding source, each category of funding is multiplied by an available stable funding (ASF) factor (0%,50%,80%,90%,100%), reflecting their stability.
  - ✓ Found in debt and equity on B/S
- **For the denominator**, each category of these is multiplied by a required stable funding (RSF) factor(0,5%,20%,50%,65%,85%,100%).
  - ✓ Found in asset on B/S

2.Basel III

⑤ Contingent Convertible Bonds (CoCos)

- bonds converting to equity are "contingent" on a pre-specified event,
  - ✓ such as falling down of bank's Tier 1 capital below a certain percentage vis-à-vis its risk-weighted assets.
  - ✓ Typically, these conditions are satisfied when the company/bank is experiencing financial difficulties.
- As the event occurs, CoCos automatically get converted into equity.
- Regulators globally are keen on banks having more equity and are particularly encouraging banks to issue CoCos (but in limited quantities) because CoCos avoid the need for a bailout and hence the conversion of CoCos is sometimes referred as "bail-in".

3.Other Rules after crisis

- Capacity to conduct macroprudential policy was added through institutional reforms.
  - The Financial Stability Oversight Council (FSOC)
- Pre-crisis compensation practices were widely blamed for imprudent risk taking.
- In the United States, Dodd Frank Act took in form, some of the parts are as follow
  - **the Volcker Rule** (part of the) restricts proprietary trading and investments in hedge funds and private equity at deposit-taking financial fi rms.
  - some over-the-counter derivatives must be traded on swap execution facilities (SEFs), which are electronic platforms that promote price transparency.
  - mortgage lenders were required to determine whether borrowers have the ability to repay the loans they take.
  - issuers of securitizations were required to retain at least 5 percent of each tranche

Reforms and finalization

Chapter 21&22

247-310

Framework

1. Motivation of Basel III Reform
2. Finalizing Basel III

1.Motivation of Basel III Reform

- **The revisions seek to restore credibility in the calculation of risk weighted assets (RWAs) and improve the comparability of banks' capital ratios by:**
  - enhancing the robustness and risk sensitivity of the standardised approaches
  - constraining the use of the internal model approaches,
  - introducing a leverage ratio buffer to further limit the leverage of global systemically important banks (G-SIBs)
  - replacing the existing Basel II output floor with a more robust risk-sensitive floor based on the Committee's revised Basel III standardised approaches.

2.Finalizing Basel III

- **In December 2017, the BCBS finalized a set of reforms that include revisions to(cont'd)**

  ① the standardized approach to credit

  ② the Internal ratings-based approach

  ③ the CVA framework for counterparty credit

  ④ operational risk capital charge

  ⑤ the leveraged ratio buffer for G-SIBs

  ⑥ output floor

2.Finalizing Basel III

① the standardized approach to credit

- Risk weights for banks and corporate bonds have been adjusted, especially for the unrated.
- Covered bonds carry a risk weight of between 10% and 100%
- Specialized lending (e.g. project finance)has several buckets
- Equities have a 400% risk weight (with exceptions) and sub-debt or other instruments have a 150% risk weight.
- New risk weights were set for real estates tied to loan value and type
- New credit conversion factors were set for a range of off-balance sheet exposures.
- A definition of default was added, such as payments past due for 90 days
- Treatment of hedges and collateral was expanded into significant detail.

2.Finalizing Basel III

② the Internal ratings-based approach

- Shortcomings of the Use of Internally Modelled Approaches
  - ✓ The excessive complexity of the IRB approaches.
  - ✓ The lack of comparability in banks' internally modelled IRB capital requirements.
  - ✓ The lack of robustness in modelling certain asset classes.
- Basel III reforms
  - ✓ Removing the Use of the Advanced IRB Approach for Certain Asset Classes
  - ✓ Introducing minimum floor values for bank-estimated IRB parameters:
    - ◆ PD floors for both the F-IRB and A-IRB approaches, mostly 5%
    - ◆ LGD and EAD floors for the A-IRB approach.

2.Finalizing Basel III

③ the CVA framework for counterparty credit

- Enhance its risk sensitivity: the revised CVA framework takes into account the exposure component of CVA risk along with its associated hedges.
- Strengthen its robustness: removes the use of an internally modelled approach, and consists of:
  - ✓ a standardised approach(BA-CVA)
  - ✓ a basic approach.(SA-CVA)
- Improve its consistency: the standardised and basic approaches of the revised CVA framework have been designed to be consistent with the approaches used in the revised market risk framework.

2.Finalizing Basel III

④ Operational risk capital charge(cont'd)

- The standardised approach for measuring minimum operational risk capital requirements replaces all existing approaches in the Basel II framework.
- The new standardised approach for operational risk determines a bank's operational risk capital requirements based on two components:
  - ✓ a measure of a bank's income
  - ✓ a measure of a bank's historical losses

2.Finalizing Basel III

④ Operational risk capital charge——Calculation(cont'd)

- Step 1: Find the business indicator (BI)

$$BI = ILDC + SC + FC$$

- Step 2: Calculate the business indicator component (BIC)

$$BIC = BI \times \text{marginal coefficients.}$$

Bucket	BI Range in Euro(bn)	BI Marginal Coefficients
1	<= 1	12%
2	1 < BI <= 30	15%
3	> 30	18%

- Step 3: Find the Internal Loss Multiplier (ILM)*

$$\text{ILM} = \text{Ln}[\exp(1) - 1 + (\frac{\text{Loss Component}}{\text{BIC}})^{0.8}]$$

- Step 4: Calculate Risk Capital Requirement

$$\text{ORC} = \text{BIC} \times \text{ILM}$$

255-310

2.Finalizing Basel III

④ Operational risk capital charge——Loss data treatment

- Banks with a BI less than €1bn will set ILM equals to 1, which is not affected by loss data.
- Banks with a BI greater than €1bn are required to use loss data as a direct input into the operational risk capital calculations.
- Banks should use losses net of recoveries in the loss dataset.
- Internally generated loss data calculations must be based on a 10-year observation period.

2.Finalizing Basel III

⑤ Buffer for Global Systemically Important Banks

- The finalised Basel III reforms introduce a leverage ratio buffer for G-SIBs to mitigate **the externalities created by G-SIBs**.
- The leverage ratio G-SIB buffer is set at 50% of a G-SIB's risk- weighted higher-loss absorbency requirements established in Basel III.
  - ✓ For example, a G-SIB subject to a 2% risk-weighted higher-loss absorbency requirement would be subject to a 1% leverage ratio buffer requirement.

2.Finalizing Basel III

⑥ Output floor

- The revised floor places a limit on the regulatory capital benefits that a bank using internal models can derive relative to the standardised approaches.
- Risk weighted assets are calculated as the higher of
  - ✓ RWA under calculation approaches that has regulatory approval
  - ✓ 72.5% of RWA under SA

Cyber-Resilient and Operational Resilience

259-310

The Cyber Resilient Organization

Chapter 23

Framework

1. Cyber Resilience
2. Resilient Security Solutions
3. Financial Resilience

1.Cyber Resilience

- **What is Resilience**
  - Resilience is the ability to prepare for and adapt to changing conditions and withstand and **recover rapidly from disruptions.**
- **Cyber Resilience**
  - Cyber resilience analysts assess system deficiencies in disruption response, and develop means of rectifying these weaknesses through cyber security enhancements in prevention, detection, and reaction.
  - The **aim of cyber resilience** is to maintain a system's capability to deliver the intended outcome at all times, including times of crisis when regular delivery has failed.

1.Cyber Resilience

- The **cyber risk management framework** proposed by the National Institute of Standards and Technology (NIST) consists of five functions:
  - ① **Identify.** Develop an organizational understanding to manage cyber security risk to systems, people, assets, data, and capabilities.
  - ② **Protect.** Develop and implement appropriate safeguards to ensure delivery of critical services.
  - ③ **Detect.** Develop and implement appropriate activities to identify the occurrence of a cyber security event.
  - ④ **Respond.** Develop and implement appropriate activities to take action regarding a detected cyber security incident.
  - ⑤ **Recover.** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident.

1.Cyber Resilience

- Cyber security in an organization typically places emphasis on maintaining a secure perimeter and the type of expenditure for typical cyber security budgets is **shifting**.
  - Key trends include increasing emphasis on **incident response**

1.Cyber Resilience

- **Incident Response(cont'd)**

① Rapid Adaptation to Changing Conditions

- ✓ Organizations need to be agile in crisis response. Organizations need to prepare, prevent, respond, and recover from any crisis that may emerge.
- ✓ To balance risk with opportunity, corporate risk-based strategy has to include preparation for and recovery from a cyber attack.

② Cyber Risk Awareness in Staff

- ✓ **Training programs** specifically geared towards developing a cyber-resilient mindset are particularly productive.
- ✓ Even the most savvy of staff members may fall victim to psychological, emotional, and cognitive weaknesses.

1.Cyber Resilience

- **Incident Response(cont'd)**

③ Gaming and Exercises

✓ Gamification usually means awarding points to employees who do the right thing, with various forms of recognition

◆In 2017, Kaspersky awarded a young talent lab prize to the US-based creators of a gamification app designed to raise information security awareness amongst millennials.

1.Cyber Resilience

- **Incident Response(cont'd)**

④ Nudging Behavior

✓ nudge principle: encouraging good **cyber hygiene** without having to reward staff accordingly.

◆Men can be nudged to make less floor mess simply by having a marked target in the center of a urinal.

✓ staff members may be nudged to talk more about cyber security, and explained that far better cultural outcomes are then seen than with traditional annual mandatory training regimes.

1.Cyber Resilience

- **Incident Response**

⑤ Business Continuity Planning and Staff Engagement

✓ All staff members need a good understanding of business continuity issues.

✓ Those assigned specialist duties, such as planning testing and incident response, need extra specific training, as emergency responders do.

2.Resilient Security Solutions

① Resilient Software

- Resilient software should have the capacity to withstand a failure in a critical component, such as from a cyber attack, but still recover in an acceptable predefined manner and duration.
- Net-centricity can introduce complexities that lead to greater chances of errors.
- Since cyber attacker can eventually manage to find an entry point into any system, it is prudent to accept that system intrusion will occur in the future, and to plan a maximally resilient response.

② Detection, Containment, and Control

- Rapid threat detection lies at the heart of resilient cyber security.
- If threat detection can automatically instigate a reboot from a safe copy of the device's operating system. By restoring the peripheral device without business interrupt ion, cyber resilience is achieved.

2.Resilient Security Solutions

③ Minimize Intrusion Dwell Time

- Controlling dwell time means early detection with an appropriate effective response .
  - ✓ Just as with malignant cancer, the lateral spread of intrusion should also be contained and controlled, so as to minimize the number and extent of compromised systems.

④ Anomaly Detection Algorithms

- Anomaly detection algorithms use state-of-the-art artificial intelligence methods.
- Faster, cheaper, simpler – but less powerful - are signature-based detection methods .

2.Resilient Security Solutions

⑤ Penetration Testing

- A penetration is the process of conducting simulated attacks to discover how successful cyber attacks might occur.
  - ✓ Conducting a pen test to prove that a missing patch is a security issue typically raises the cost of testing, and runs the expensive risk of potential system downtime.
- The information obtained from pen testing can be used to plug security gaps, improve attack response, and enhance cyber resilience.

⑥ The risk-return trade-off

- The actual level of risk reduction achieved may in fact be lower than is optimistically perceived, given the large security budget.

3.Financial Resilience

Financial Consequences of a Cyber Attack

- A major cyber attack on a corporation can impact it in numerous adverse ways.
  - ✓ Intellectual property and other confidential information may be stolen
  - ✓ important computer system files may be corrupted or encrypted
  - ✓ denial of service may bring systems down
- The bottom line for any commercial organization is the ultimate financial cost. Each of the adverse impacts results in a financial loss to the corporation. For publicly listed corporations, the stock price is a resilience measure.

3.Financial Resilience

Financial Risk Assessment

- Companies have to make assessments of their risk and build resilience into their balance sheet to withstand the types of shock that might be foreseeable.
  - ✓ A cyber attack can cause sufficient loss to cause damage to a company's balance sheet, even for fairly sizeable organizations.
- Balance sheet resilience can be achieved by having all of the standard financial engineering processes to minimize earnings volatility, including
  - ✓ having sufficient liquidity margins
  - ✓ reducing debt ratios
  - ✓ having access to emergency loan provisions
  - ✓ being able to cut costs to meet earnings targets
  - ✓ having cyber insurance to provide a level of financial indemnity

3.Financial Risk Assessment

- **Ways to Increase a Firm's Financial Resilience**
  - Reverse Stress Testing
  - Defense in Depth
  - Enterprise Risk Management
  - Cyber Value at Risk
  - Re-Simulations of Historical Events
  - Counterfactual Analysis
  - Building Back Better
  - Events Drive Change
  - Education for Cyber Resilience
  - Improving the Cyber Profession

Cyber-Resilience: Range of Practices

Chapter 24

Framework

1. Recent Regulatory Initiatives
2. Cyber Governance
3. Practice for Cyber Risk Management
4. Communication and Sharing of Information
5. Interconnections with Third Parties

1.Recent Regulatory Initiatives

- **Recent regulatory initiatives(cont'd)**

① In March 2017, the G20 Finance Ministers and Central Bank Governors noted that " the malicious use of information and communication technologies (JCT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability" .

② The G7 issued Fundamental Elements of Cyber-security for the financial sector, and the Committee on Payments and Market Infrastructures (CPMJ) issued, jointly with the International Organization of Securities Commissions (IOSCO), guidance on cyber-resilience for financial market infrastructures (FMIs) in June 2016.

1.Recent Regulatory Initiatives

- **Recent regulatory initiatives**

③ In the European Union (EU), the European Commission's (EC) Fintech Action Plan invites the European Supervisory Authorities to consider issuing guidelines to achieve convergence on JCT risk.

④ The **Basel Committee** on Banking Supervision (BCBS) recognised the merits of approaching operational resilience beyond the purview of operational risk management and minimum capital requirements, and established the Operational Resilience Working Group (ORG) with the intention of contributing to, inter alia, the international effort related to cyber-risk in close coordination with the other international bodies involved.

2.Cyber Governance

- **Current practices** by banks and supervisors in the **governance** of a cyber risk management framework(cont'd)
  - ① Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 234 Information Security
  - ② Supervisory Requirements for IT in Financial Institutions (BaFin Circular 10/2017, BAIT)[German Banking Act]
  - ③ US Agencies' Notice of Proposed Rulemaking for New Cyber-Security Regulations for Large Financial Institutions

2.Cyber Governance

- Against this backdrop, **supervisory expectations** and **practices** were identified and analysed in the following areas relevant to governance:

  ① Cyber-security strategy

  ② **Management roles and responsibilities**

  ③ Cyber-risk awareness culture

  ④ Architecture and standards

  ⑤ Cyber-security workforce

2.Cyber Governance

② Recognition of the Importance of the Board of Directors and Senior Management

- Almost all the jurisdictions emphasise the importance of management roles and responsibilities for cyber-governance and controls.
  - ✓ Some jurisdictions have issued specific regulatory guidance and requirements addressing cyber-governance roles
- Variety of Supervisory Approaches Regarding the Second and Third Lines of Defence (3LD)
  - ✓ The majority of regulators have adopted the 3LD risk management model to assess cyber-security risk and controls.
  - ✓ However, most regulators do not prescribe precisely how responsibilities should be distributed across the lines

3.Practice for Cyber Risk Management

- **The four sun-sections set out a range of observed practices on cyber-risk management, and incident response and recovery.(cont'd)**
  - ① Methods for supervising cyber-resilience
  - ② Information security controls testing and independent assurance
  - ③ Response and recovery testing and exercising
  - ④ Cyber-security and resilience metrics.

3.Practice for Cyber Risk Management

① Methods for supervising cyber-resilience

- Risk Specialists Assess Information Security Management and Controls
  - ✓ Most jurisdictions undertake **off-and on-site** reviews and inspections of regulated institutions' information security controls to assess compliance with regulatory standards and alignment with good practice.
- Jurisdictions Increasingly Engage With Industry to Address Cyber-Resilience
  - ✓ Industry engagement is used to eit her influence industry behaviour, or to seek feedback and views to inform regulatory work.

3.Practice for Cyber Risk Management

② Information Security Controls Testing and Independent Assurance

- Mapping and Classifying Business Services Should Inform Testing and Assurance
  - ✓ A clear understanding of business services and supporting assets can be used to design testing and assurance of end-to-end business services.
- Penetration Testing
  - ✓ Tests will be tailor-made and will not result in a pass or fail-rather they will provide the tested entity with insight into its strengths and weaknesses, and enable it to learn and evolve to improve cyber-maturity.
- Taxonomy of Cyber-Risk Controls

3.Practice for Cyber Risk Management

③ Response and Recovery Testing and Exercising

- Evaluation of Service Continuity, Response and Recovery Plans and Continuous Learning
  - ✓ The majority of regulators require entities to establish a framework or policy for prevention, detection, response and recovery activities, including incident reporting.
- Joint Public-Private Exercising
  - ✓ Distinct from testing, most supervisors and banks use exercises to train and practice how they would respond to an incident.

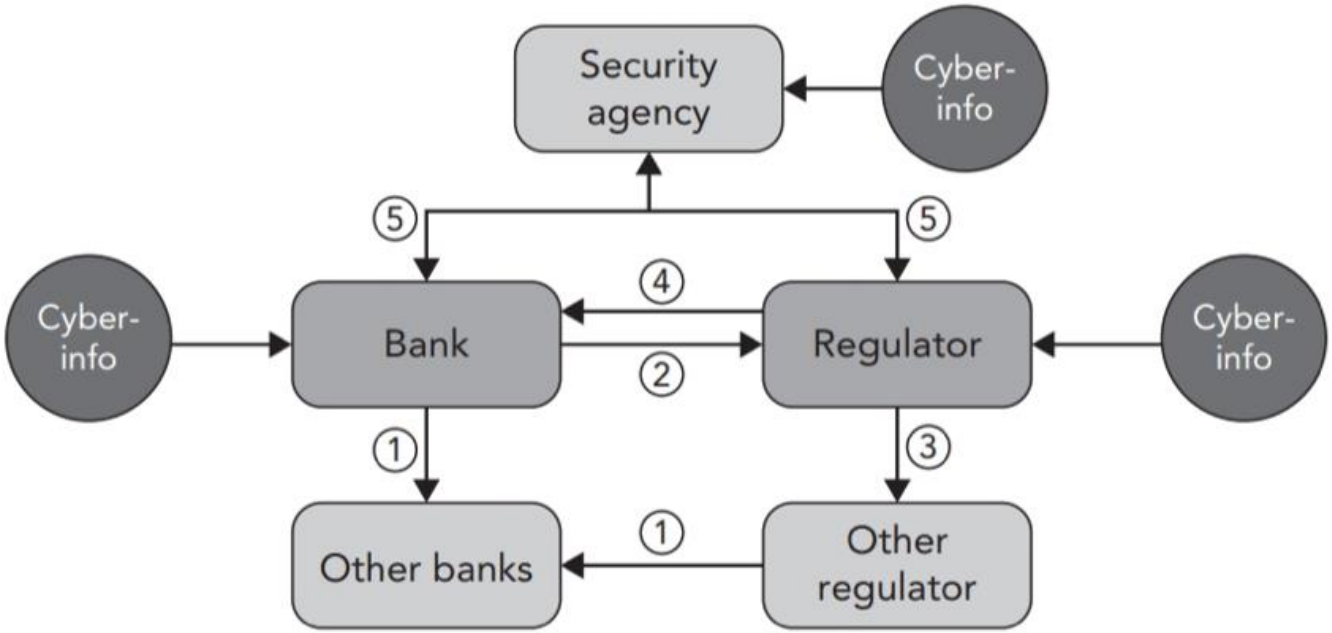
3.Practice for Cyber Risk Management

④ Cyber Security and Resilience Metrics

- Cyber-Security and Resilience Metrics are Not Yet Mature
  - ✓ Supervisory authorities also rely on entities' own management information, although this differs across entities and is not yet mature.
- Emerging Forward-Looking Indicators of Resilience
  - ✓ Backward-looking indicators comment on past performance as an indicator of future performance
  - ✓ While backward-looking metrics continue to be important, jurisdictions are increasingly recognising the need for forward-looking indicators as direct and indirect metrics of resilience

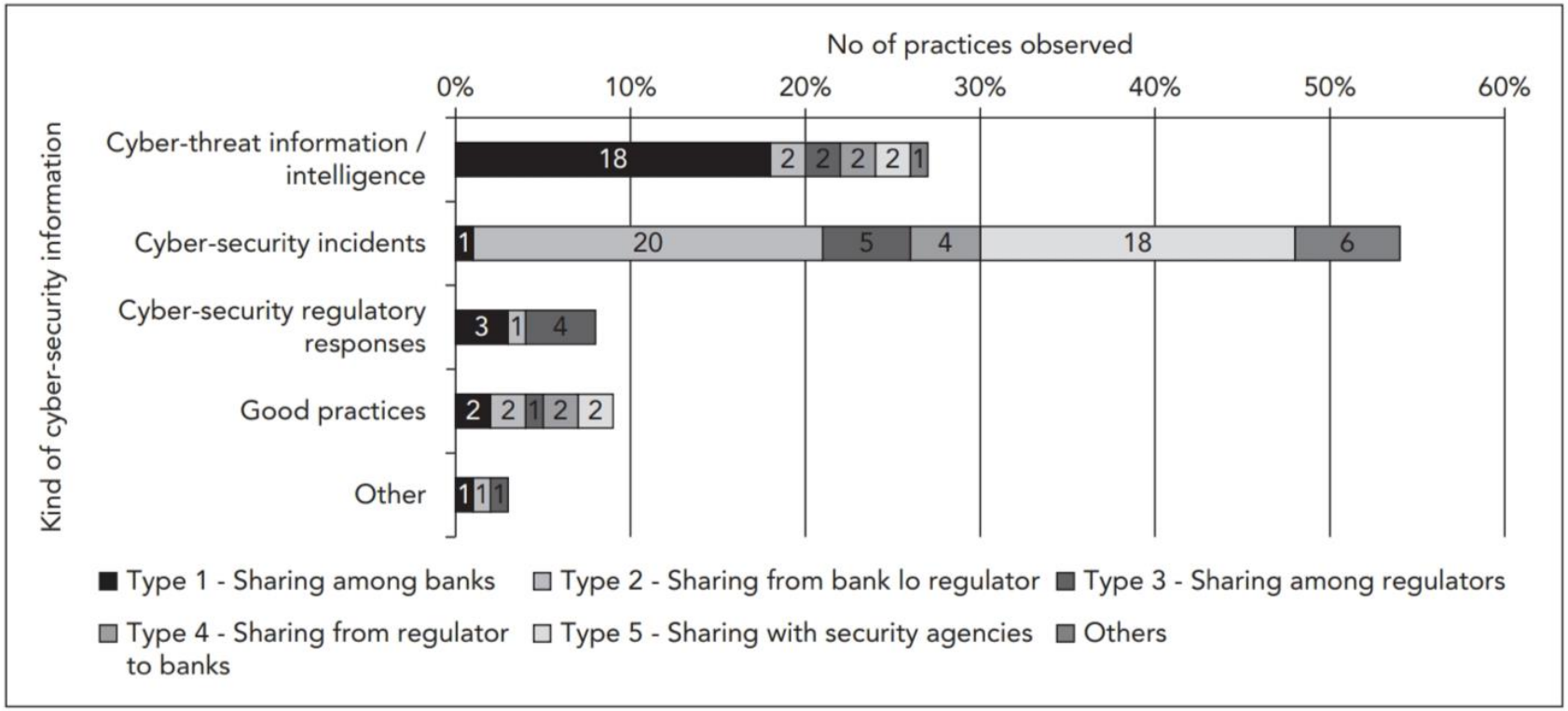
4.Communication and Sharing of Information

- **Interlinkage of different types of cyber-security information-sharing practices**



4.Communication and Sharing of Information

➢ Kinds of information shared



4.Communication and Sharing of Information

① Sharing Among Banks

- Banks share information (eg knowledge of a cyber-security threat) with peer banks through established channels, mainly to allow peer banks to take more timely action in response to similar threats.
- Sharing of information and collaboration among banks depend on the financial industry's culture and level of trust among participants.

② Sharing from Banks to Regulators

- The sharing of cyber-security information from a bank to its regulator(s)/supervisor(s) is generally limited to cyber-incidents based on regulatory reporting requirements.
- Reporting requirements are established by different authorities for specific purposes depending on their mandate

4.Communication and Sharing of Information

③ Sharing Among Regulators

- Regulators share information with fellow regulators, be they domestic or cross-border, as appropriate according to established mandatory or voluntary information-sharing arrangements.

④ Sharing from Regulators to Banks

- Information-sharing from regulators to banks occurs through established channels, based on the information the regulator receives both from banks and other sources.

⑤ Sharing with Securities Agencies

- effective communication of relevant cyber-security incidents with security agencies could facilitate broader awareness of cyber-threats in a timely manner, and enhance defensive measures against adversaries.

5.Interconnections with Third Parties

- Extensive use of third-party services increases the challenge for jurisdictions and regulated institutions themselves to have full sight of the controls in place, and the level of risk.
- Cyber-resilience practices in relation to third parties are analysed across the following areas:
  - Governance of third-party interconnections
  - Business continuity and availability
  - Information confidentiality and integrity
  - Specific expectations and practices regarding visibility of
  - third-party interconnections
  - Auditing and testing
  - Resources and skills

Building the UK Financial Sector's Operational Resilience

Chapter 25

292-310

Framework

1. Operational Resilience
2. Business Disruptions
3. Impact Tolerances

1.Operational Resilience

- **Operational resilience**
  - is the ability of an organization to continue to provide business services in the face of adverse operational events by anticipating, preventing, recovering from, and adapting to such events.
  - refers to the ability of firms, FMIs and the sector as a whole to prevent, respond to, recover and learn from operational disruptions.
  - threats and challenges
    - ✓ Technological change and in an increasingly hostile cyber environment
    - ✓ firms operate internationally or outsource a significant level of activities to third parties.

1.Operational Resilience

- **Principles for maintaining strong operational resilience(cont'd)**

  ① management and governance

  - ✓ An effective board is critical to ensuring a sound and well-run business.
  - ✓ Boards should ensure there is sufficient challenge to the executive and that they have access to people within the business with appropriate technical skills . They should also ensure the recruitment and training of suitable people for relevant executive roles, drawing on additional skills where relevant.

  ② risk management

  - ✓ Risk management should cover all types of risk, including operational, and firms and FMIs are expected to identify, monitor and manage the risks they are or might be exposed to.

1.Operational Resilience

- **Principles for maintaining strong operational resilience(cont'd)**

  ③ **internal controls for systems and processes**

  - ✓ boards and senior management must be able to exercise appropriate oversight and be confident their direction is being carried out.

  ④ **Business Continuity and Contingency Planning**

  - ✓ undertake appropriate contingency planning
  - ✓ maintain continuity plans explaining how they will respond and recover following disruption

  ⑤ **oversight of outsourcing arrangements**

  - ✓ While outsourcing can enable firms and FMIs to manage risks more effectively and at a reduced cost, it can also give rise to new risks for which they remain responsible.

2.Business Disruptions

- In setting impact tolerances, the supervisory authorities suggest that a firm's or FMI's board or senior management might prioritise those business services which, if disrupted, have the potential to:
  - Threaten the firm's or FML's ongoing viability
  - Cause harm to consumers and market participants
    - ✓ Harm to consumers (such as an inability to access cash deposits, savings, credit or other financial services) and harm to market participants (such as an inability to price trades or to complete post-sale activities) arising from operational disruptions is likely to manifest before risks to the viability of a firm or FMI start to crystallise.
  - Undermine financial stability

3.Impact Tolerances

- **Impact tolerances** would need to be expressed clearly and would be separate from any risk appetites or recovery time objectives (RTO). Impact tolerances express an upper limit where a breach is to be avoided in all but the most extreme scenarios. Risk appetites and RTOs, tend to express a desired outcome that is achieved with high probability.
  - The supervisory authorities consider that setting impact tolerances for the most important business services could:
    - ✓ support firms and FMIs in prioritizing investment and resource allocation;
    - ✓ provide a clear scope when firms and FMIs want to test their own resilience; and
    - ✓ provide a focus for supervisory engagement.

Striving for Operational Resilience

Chapter 26

Framework

1. Operational Resilience, Business Continuity and Disaster Recovery
2. Effective Operational Resilience Framework

1.Operational Resilience, BC and DR

- Resilience is fundamentally different from traditional business continuity (BC) and disaster recovery (DR).(cont'd)
  - BC and DR have historically been heavily focused on physical events, were designed and tested in organizational silos, and are, by most organizations, primarily viewed as a compliance exercise.
    - ✓ physical events: natural disaster, active shooter
  - BC and DR are limited by organizational boundaries, and are, by most organizations, primarily viewed as a "check the box" exercise rather than true risk management.

1.Operational Resilience, BC and DR

- Resilience is fundamentally different from traditional business continuity (BC) and disaster recovery (DR).
  - **Operational resilience focuses on**
    - ✓ **the adaptability to emerging threats**,
    - ✓ the dependencies and requirements for providing critical business services end-to-end (crossing organizational silos)
    - ✓ the broader economic as well as firm-specific impact of adverse operational events.
  - It requires a mindset shift in the organization away from resilience as a compliance exercise to resilience as a key organizational capability that is everyone's responsibility to maintain and continuously improve.

1.Operational Resilience, BC and DR

➢ Key differences between operational resilience and BC/DR (cont'd)

① Governance

✓ Operational Resilience Approach

- ◆ Clearly defined accountability of board and senior management
- ◆ Resilience incorporated into risk appetite statements and metrics across operational risk types
- ◆ Comprehensive and actionable reporting to drive continuous improvement

✓ Traditional Approach (BC/ DR)

- ◆ Role of board and senior management limited to post-event response
- ◆ Resilience not an explicit consideration in risk appetite statements and metrics
- ◆ "Compliance-type" update on exercises

1.Operational Resilience, BC and DR

- **Key differences between operational resilience and BC/DR (cont'd)**

  ② Organizational Focus

  ✓ Operational Resilience Approach

  - ◆Critical business services end-to-end (ignoring organizational silos)
  - ◆Broader economic impact of disruption, in addition to firm-specific impact

  ✓ Traditional Approach (BC/ DR)

  - ◆Individual business units or specific technology assets
  - ◆Firm-specific impact of disruption

1.Operational Resilience, BC and DR

- **Key differences between operational resilience and BC/DR (cont'd)**

  ③ Integration

  ✓ Operational Resilience Approach

  - ◆Comprehensive view of dependencies of critical business service on organizational assets (systems, data, third parties, facilities, processes, and people)
  - ◆Resilience considerations embedded in the upfront design of business services and organizational assets

  ✓ Traditional Approach (BC/ DR)

  - ◆View of dependencies in most cases limited to the business unit or directly linked technology assets
  - ◆Continuity and recovery capabilities bolted on to satisfy requirements

1.Operational Resilience, BC and DR

- **Key differences between operational resilience and BC/DR (cont'd)**

④ Measurement

✓ Operational Resilience Approach

- ◆Business disruption scenarios tailored to each critical service based on an aligned and forward-looking risk assessment
- ◆Tolerances for business disruption (impact tolerances) based on bespoke scenarios

✓ Traditional Approach (BC/ DR)

- ◆Standard business disruption scenarios across business units
- ◆Standard tolerances for business disruption (recovery time/ point objectives) for all scenarios

1.Operational Resilience, BC and DR

- **Key differences between operational resilience and BC/DR**

  ⑤ **Preparedness**

  ✓ Operational Resilience Approach

  - ◆Single incident response regime (unified incident command) for all incident types
  - ◆Plans and capabilities monitored, tested, and adapted continuously
  - ◆Emphasis on building trust among crisis management team to enable effective response

  ✓ Traditional Approach (BC/ DR)

  - ◆Distinct incident response regimes for different incident types, which may negatively impact response times
  - ◆Plans and capabilities tested infrequently (e.g., annually)
  - ◆Little attention paid to dynamics of crisis management team

2.Effective Operational Resilience Framework

- **Organizations that manage to establish effective operational resilience programs will be able to realize the benefits of better resilience as well as related business benefits:**
  - ① **Reduce and optimize their risk exposure**, with improved visibility into their risks, better monitoring, a more proactive approach to controls, and ability to deliver services even when things go wrong.
  - ② **Better focus the organization and drive investment towards the most important areas**, based on a prioritization of their critical business services.
  - ③ Be able to **support the innovation** agenda of the business and enable faster innovation cycles without compromising on risk management by ensuring the organization is adaptable and considers resilience up front.
  - ④ Be more effective and efficient, leveraging a clear understanding of critical service delivery **to reduce costs** (e.g., optimize outsourcing relationships), **streamline processes** (e.g., introduce tools and automation), and **enhance efficacy** (e.g., identify and remediate steps that introduce errors).

It's not the end but just beginning.

Thought is already is late, exactly is the earliest time.

感到晚了的时候其实是最快的时候。

问题反馈

- 如果您认为金程**课程讲义/题库/视频**或其他资料中**存在错误，欢迎您告诉我们，**所有提交的内容我们会在最快时间内核查并给与答复。
- **如何告诉我们？**
  - 将您发现的问题通过电子邮件告知我们，具体的内容包含：
    - ✓ 您的姓名或网校账号
    - ✓ 所在班级（eg.2005FRM一级长线无忧班）
    - ✓ 问题所在科目（若未知科目，请提供章节、知识点）和页码
    - ✓ 您对问题的详细描述和您的见解
  - 请发送电子邮件至：academic.support@gfedu.net
- **非常感谢您对金程教育的支持，您的每一次反馈都是我们成长的动力。**后续我们也将开通其他问题反馈渠道（如微信等）。