操作风险与弹性

FRM二级培训讲义-强化班

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

Part 1: Operational Risk Management (CH1~CH6)

1. Three line of defense
2. 11 Principles of Operational Risk Management
3. ERM Definitions
4. Why ERM works?
5. Implementation of ERM
6. The Chief Risk Officer
7. Key Challenges in Implementing RAF
8. Mindset of Culture and Conduct
9. Improving Conduct and Culture
10. Regulators Expectations
11. Risk Culture and Corporate Culture
12. Drivers and Measurement

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

3. 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.

4.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

4.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…

5.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.

5.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

5.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

6.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.

6.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.

7.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.

7.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

8.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, on the other hand, is intangible and ubiquitous; as such, it requires deep understanding of the strategy, operating model, and values of the organization.
- **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.

8.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.**
  - lapses in customer protection, anti-money-laundering deficiencies
  - **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,
- **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
- **Bank culture and conduct are more important than ever, to repair trust and reputational issues and fulfill the role of banks in society.**

9.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

9.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.
  - ✓ 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.

9.Improving Conduct and Culture

③ Staff Development and Promotions

- 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.
- with advanced analytics, **surveillance technology** aims to detect or predict potential conduct events.

10.Risk Culture and Corporate Culture

Corporate culture and risk culture

- **Corporate culture**: Literature often refers to corporate culture as the missing link to fully understand how organizations act.
- **Risk culture**: 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 **interacts with** dominant corporate culture.

11.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".

12.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.

Framework

Part 2: Model Risk and Data Quality (CH7~CH11)

1. Seven Categories of OpRisk
2. Four Elements of the OpRisk Framework
3. Organization of Risk Departments
4. Types of Erred Data
5. Key Dimensions of Data Quality
6. Data Quality Management
7. The Causes of Model Risk
8. The 2005 Credit Correlation Episode
9. Elements of Effective Process to Manage Model Risk
10. Rating Model Validation

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.

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.

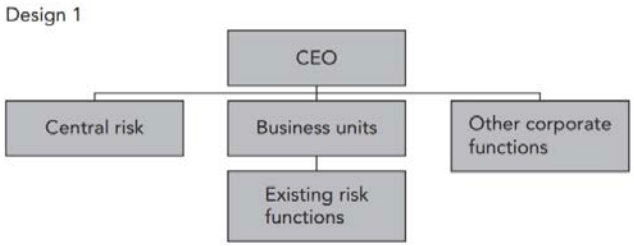
2.Four Elements of the OpRisk Framework

④ Scenario analysis

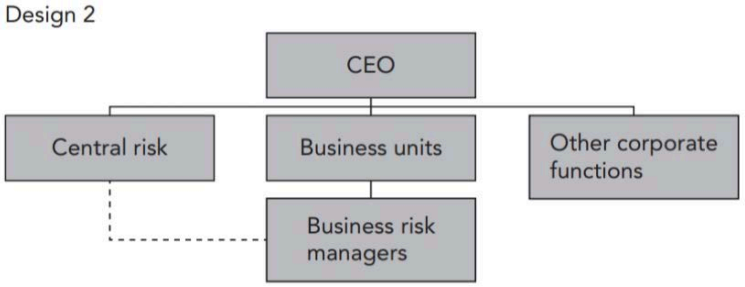
- These scenario estimates are usually gathered, through expert opinions. The Challenges exist when there are behavior biases among experts.
  - ✓ Presentation Bias
  - ✓ Availability bias.
  - ✓ Anchoring bias.
  - ✓ "Huddle" bias or anxiety bias
  - ✓ Gaming
  - ✓ Over/under confidence bias
  - ✓ Inexpert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

3.Organization of Risk Departments

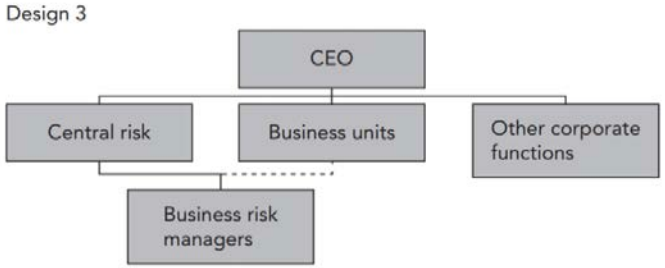
- The organizational design would usually hint at the strength and degree of development of an OpRisk framework at a firm.



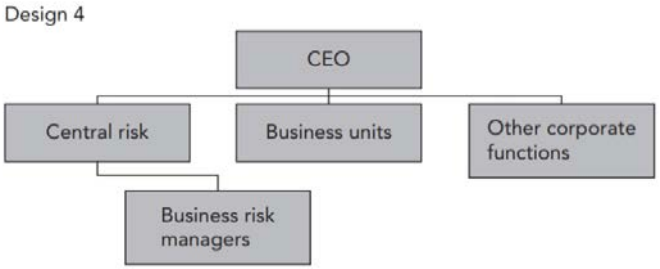
Design 1-Central Risk Function as Coordinator



Design 2-Matrix reporting-the "dotted lines“



Design 3-Solid reporting lines to Central Risk Management



Design 4-Strong Central Risk Management

4.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

5.Key Dimensions of Data Quality

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

① Accuracy

② Completeness

③ Consistency: Two data values drawn from separate data sets must not conflict with each other. There are three types of consistency:

- ✓ Record level: one set of data values and another set within the same record.
- ✓ Cross-record level: one set of data values and another set in different records.
- ✓ Temporal level: one set of data values and the same set within the same record at different points in time.

④ Reasonableness

⑤ Currency

⑥ Uniqueness

6.Data Quality Management

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

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

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.

7.The Causes of Model Risk

- **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.

7.The Causes of Model Risk

- **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.

7.The Causes of Model Risk

- **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.

7.The Causes of Model Risk

- **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**.

8.The 2005 Credit Correlation Episode

➢ Major Strategy

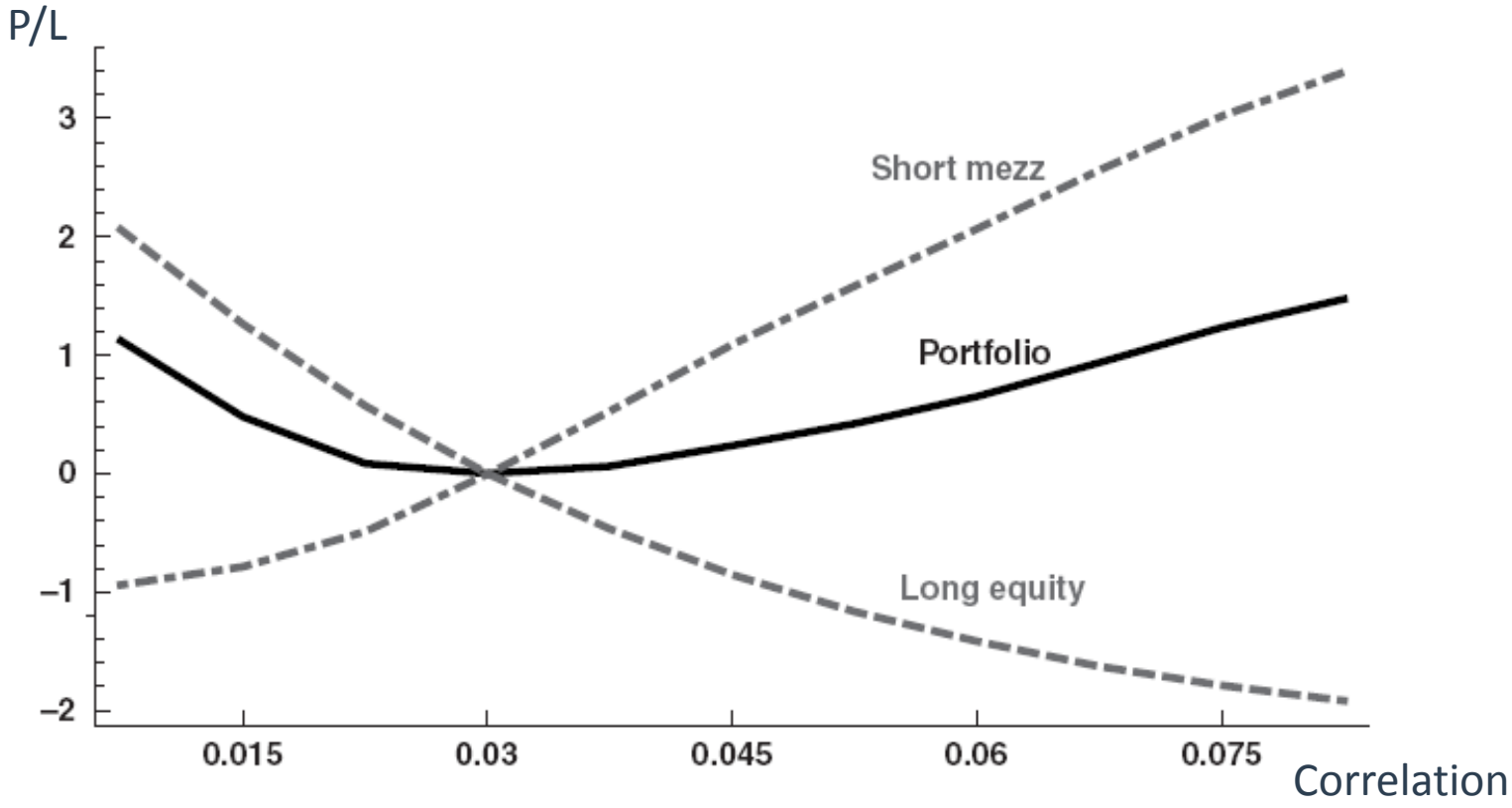
- A popular trade especially among hedge funds and proprietary trading desks was:
  - ✓ Sell protection on the equity tranche of the CDX.NA.IG
  - ✓ Buy protection on the junior mezzanine tranche of the CDX.NA.IG
- The trade was thus long credit and credit-spread risk through the equity tranche and short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

8.The 2005 Credit Correlation Episode

- **Default-risk-neutral**
  - 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.

8.The 2005 Credit Correlation Episode

- **Default-risk-neutral**



8.The 2005 Credit Correlation Episode

- **Risks behind**
  - 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.

Model Risk

- **Three elements of effective process to manage model risk (cont'd)**
  - A robust model development, implementation, and use.
    - ✓ **Model testing**
  - A sound model validation process.
    - ✓ Evaluation of conceptual soundness
    - ✓ Ongoing monitoring.
      - **Benchmarking** is the comparison of a given model's inputs and outputs to estimates from alternative internal or external data or models.
    - ✓ Outcomes 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
  - A good governance

10.Rating Model Validation

- **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.

10.Rating Model Validation

- **Qualitative Validation**
  - Rating Systems Design
  - Data Quality
- **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**

Framework

Part 3: Economic Capital Management and Other Related Issues (CH12~CH18)

1. Risk Capital
2. Risk-Adjusted Return on Capital
3. Adjusted RAROC
4. Benefits of Economic Capital Framework
5. Capital in Bank Holding Company
6. Stress Testing Evolution
7. Best Practices Related to ML/FT Risk
8. Post-Crisis Regulatory Changes

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

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

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

➢ 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.

4.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.

4.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.

5.Capital in Bank Holding Company

- **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.

6.Stress Testing Evolution

- **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)

6.Stress Testing Evolution

➢ 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.

7.Risks From the Use of Service Providers

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

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**

③ **Reputational risks**.

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 the provider's country.

⑤ **Operational risks**.

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

8.Service Provider Risk Management Programs

- Effective programs to manage outsourcing risks usually include the following core elements:

① Risk assessments;

② **Due diligence and selection of service providers;**

③ **Contract provisions and considerations;**

- ✓ Indemnification: the loss results from service provider's negligence
- ✓ Business resumption and contingency plan of the service provider
- ✓ Subcontracting

④ Incentive compensation review;

⑤ Oversight and monitoring of service providers; and

⑥ Business continuity and contingency plans.

7.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

7.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

7.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

8.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.

8.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.

8.Post-Crisis Regulatory 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

Framework

Part 4: The Basel Accord (CH12~CH18)

1. Basel I
2. 1995&1996 Amendments
3. Basel II
4. Solvency II
5. Basel II.5
6. Basel III
7. Finalizing Basel III
8. Other Rules After Crisis

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**

$$RWA = \sum Asset_i \times Risk\ Weight_i$$

- **Risk Weights for Off-Balance-Sheet Items and over-the-counter derivatives**
  - A **credit equivalent amount** is calculated first

$$RWA = \sum CEA_i \times Risk\ Weight_i$$

2.1995&1996 Amendments

- **The 1995&1996 Amendment was established then to**
  - Take netting into consideration when calculate RWA
  - Added a capital charge for market risk
    - ✓ the bank's assets are separated into two categories
      - ◆The **trading book**
      - ◆The **banking book**
    - ✓ 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

I. 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.

- the risk weights depend on the assessments made by external credit assessment institutions recognized by supervisors.
  - ✓ External rating, tenor and the counterparty
- Adjustments for Collateral, two approaches
  - ✓ **Simple Approach** and **Comprehensive Approach**

3.Basel II

II. Required capital for credit risk(cont'd)

② The IRB approach

✓ use a bank's own internal estimates for calculation

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

✓ 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

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:

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

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

III. 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**

3.Basel II

➢ Pillar 1: Minimum Capital 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.

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)
  - ✓ Solvency Capital Requirement (SCR)
    - ◆deliver to the supervisor a plan to restore capital to above SCR
  - ✓ Minimum Capital Requirement (MCR)
    - ◆stop engaging into any new business

5.Basel II.5

➢ Market Risk Capital

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

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
- 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.

6.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)

6.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.**

6.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.

6.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
  - ✓ It is core Tier 1 capital equal to 0~2.5% of risk weighted assets.
- Banks that do not meet the CCB or CCyB will be subject to constraints on capital distributions of dividends, stock repurchases and discretionary bonuses to staff.

6.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.

6.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%.

6.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.

6.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

6.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".

7.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(more detail risk weights)

  ② the Internal ratings-based approach(more restrains)

  ③ the CVA framework for counterparty credit(take hedging into account)

  ④ operational risk capital charge(Cont'd)

  ⑤ the leveraged ratio buffer for G-SIBs(increase 50%)

  ⑥ output floor($RWA_{IRB} \geq RWA_{SA}$)

7.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

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

7.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.

8.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

Framework

Part 5: Cyber-Resilient and Operational Resilience (CH23~CH26)

1. Cyber Resilience
2. Cyber Resilient Security Solutions
3. Financial Resilience
4. Practice for Cyber Risk Management
5. Communication and Sharing of Information
6. Operational Resilience
7. Business Disruptions
8. Impact Tolerances
9. Operational Resilience, BC and DR

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

- **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

④ Nudging Behavior

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

⑤ Business Continuity Planning and Staff Engagement

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

2.Cyber 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 interruption, cyber resilience is achieved.

2.Cyber 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.Cyber 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.
- 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

4.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

- ✓ **off-and on-site** reviews

② Information security controls testing and independent assurance

- ✓ Penetration Testing
- ✓ Taxonomy of Cyber-Risk Controls

③ Response and recovery testing and exercising

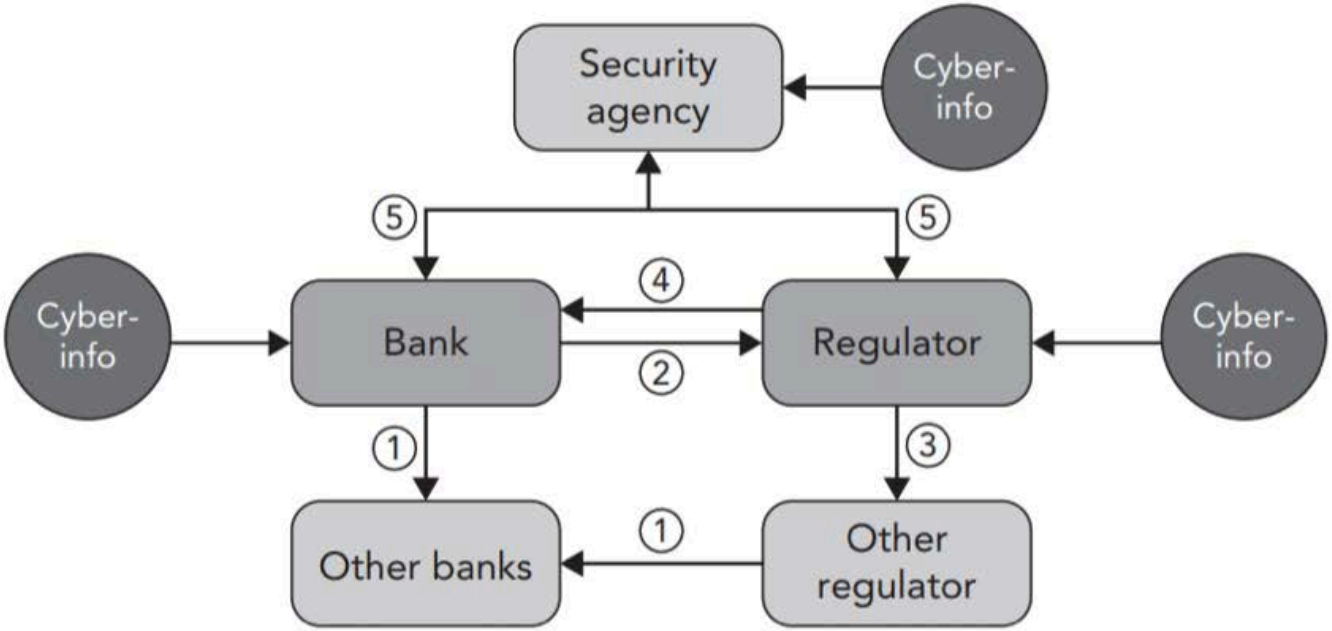
- ✓ Joint Public-Private Exercising

④ Cyber-security and resilience metrics.

- ✓ the need for forward-looking indicators

5.Communication and Sharing of Information

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



6.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.

7.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 FMI'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

8.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.

9.Operational Resilience, BC and DR

- Traditional business continuity (BC) and disaster recovery (DR).
  - 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.
  - 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.
- **Operational resilience focuses on the adaptability to emerging threats.** 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.

9.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

9.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

9.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

9.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

9.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

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）。