操作风险与弹性

FRM二级培训讲义-强化班

101% Contribution Breeds Professionalism

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 (整体的)

Part 1: Holistic Overview of Operational Risk and Resilience (CH1~CH7)

1. Operational risk management framework
2. Operational resilience and framework
3. Risk Identification
4. Risk Assessment Tools
5. Quantitative Risk Measurement
6. Risk mitigation
7. Risk Reporting

◆ 1.Operational risk management framework

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

- This definition includes legal risk but excludes strategic and reputational risk. Regulators may have excluded strategic and reputational risk from operational risk to make the measurement of operational risk as objective as possible.

✓ **Reputational risk** often refers to the damage to reputation that follows some operational incidents. It is an indirect risk.

✓ **Strategic risk** can be nuanced between the risk of losses due to making wrong strategic choices and the risk of losses due to the failed execution of the strategy. Strategic risk is in fact operational risk in the boardroom.

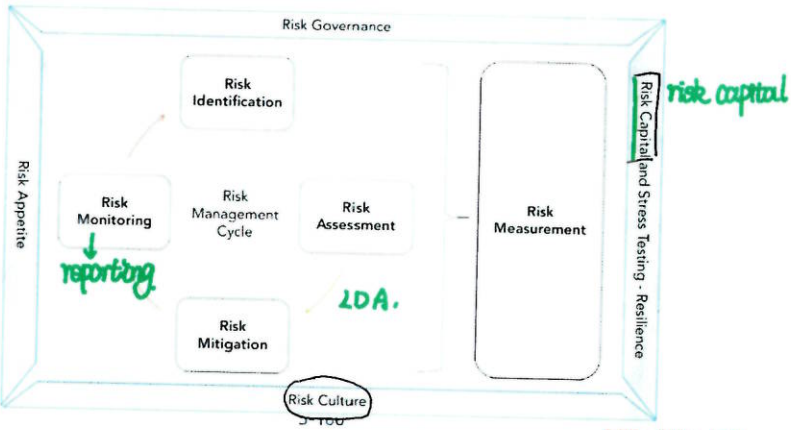
✓ **Legal risk** is linked to the enforceability or breach of contracts, their relevance, laws and legislations, and the risk of loss in case of breaches or errors.

✓ Compliance relates to following not only the law but also all the rules and regulations applicable to a given activity.

◆ 1.Operational risk management framework

➢ **Include RMC and four elements: risk governance, risk appetite, risk culture, risk capital and stress testing.**

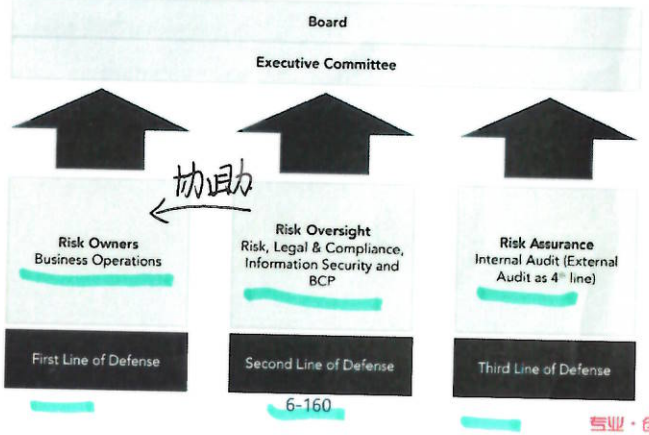
- Risk governance, culture, and appetite sets the priorities for and guides ERM.



◆ 1.Operational risk management framework

➢ **Risk governance**

- Risk governance prescribes the roles and responsibilities of individuals in the three lines of defense, and organizes decision-making and reporting, generally through committees.



1.Operational risk management framework

- **Responsibilities of an effective first line of :**
  - The risk owner
  - **Identifying** and assessing the materiality of operational risks inherent in the business.
  - **Establishing** appropriate controls.
  - **Assessing** the design and effectiveness of these controls.
  - **Monitoring** and **reporting** the business units' operational risk profiles.
- **Line 1.5 or 1.b**
  - Risk specialists (risk champions or risk correspondents or stewards) in each business department to interact with the risk function which are particularly common in larger organizations.

1.Operational risk management framework

- **Difference between line 1 and line 2**
  - The relationship between the first and the second line of defense is probably the aspect of the **3LoD model** that has generated the most debate.
  - Many regulators require a second line to be "independent" from the first line, to provide "oversight and challenge" of the risk management activities performed in the first line.
    - ✓ Pure independence of the second line of defense raises the question of potential redundancy with internal audit.
    - ✓ It can be very difficult to operate effective oversight and challenge before properly understood.
  - Even then, the second line of defense can maintain its independence from the first line of defense, by providing guidance and asking questions, but without preempting the answers.
  - The first line owns the final sign-off on risks assessment and controls, this is not the role of the second line. The first line owns the risks and the second line owns the methodology.

1.Operational risk management framework

- **The Role of the Board for Operational Risk and Resilience**
  - **General administration** of the firm, including risk management.
  - Validating the **operational risk management framework** and ensuring a periodic revision of the ORMF.
  - Setting the **risk appetite** of the firm and for making sure that it operates within the limits of its risk appetite.
  - Establishing a **risk management culture** that is communicated effectively to the firm.

◆ 1.Operational risk management framework

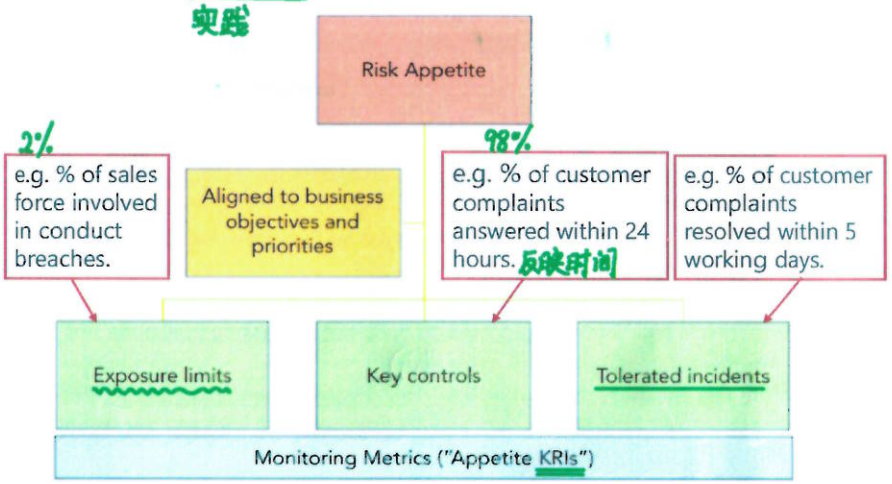
➢ **Regulatory expectation for risk appetite**

- The board is responsible for determining and defining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives.
- **Risk appetite and tolerance statements**
  - ✓ need to be easy to communicate and understand.
  - ✓ need to justify the reasons for taking, limiting, or avoiding certain types of operational risk.
  - ✓ need to be in alignment with the bank's strategy and business plans.
- Risk appetite should be forward-looking and subject to scenario and stress testing and have a view of what events might push the bank outside the limits of it risk appetite and tolerance.

↑ update.

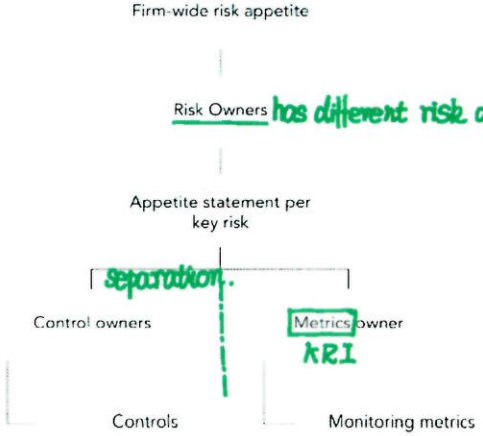
◆ 1.Operational risk management framework

➢ **Structure of actionable risk appetite**



◆ 1.Operational risk management framework

➢ **Risk appetite governance structure**



1.Operational risk management framework

- Besides the management of risks, the other fundamental role of ERM in financial services is to ensure the solvency and sustainability of an institution through appropriate capital funding to cover the unexpected losses that can materializes in any of the main risk types.
- The measurement of enterprise risk translates into the following elements of an enterprise risk management framework and activities:
  1. **Regulatory capital and supervision**
  2. **Economic capital**
  3. Risk-adjusted return on capital (RAROC) thresholds
  4. Capital aggregation and diversification

1.Operational risk management framework

- **Operational Risk in Basel II: Pillar 1: Regulatory Capital**
  - ✓ Pillar 1 details the calculations that determine the minimum level of capital that banks need to cover the risk of unexpected losses from credit, market, and operational risks, and the minimum ratios required to limit liquidity risks.
    1. Basic Indicator Approach
    2. Standardized Approach

    } ORC is a portion of gross income
    3. Advanced Measurement Approach
       - ◆Operational risk capital=WCL(99.9%, 1 year)-EL.
    4. Simple Measurement Approach(2023.1.1 comes into force)
       - ◆Consider both income and operational loss data

1.Operational risk management framework

- **Operational Risk in Basel II: Pillar 2 Capital for Operational Risk**
  - Pillar 2 acts as a somewhat qualitative complement to a regulator's assessment of an institution's risk profile.
  - ✓ Adjust the capital requirement calculated in Pillar 1 with an add-on that reflects more fairly the nature and extent of the regulated entity's risk exposure.
  - ✓ Review the arrangements, strategies, processes, and mechanisms implemented by a firm to comply with its regulatory requirements.
  - ✓ Consider the nature, scale, and complexity of a firm's activities.
  - ✓ Evaluates any further risks revealed by stress testing.

◆ 1.Operational risk management framework

- **Operational Risk in Basel II: Pillar 3: Market Discipline**
  - ✓ Pillar 3 details rules on mandatory yearly or quarterly information disclosures by financial institutions regarding their financial situation and risk information.
  - ✓ The purpose of Pillar 3 is to encourage market discipline, especially among investors in more risky firms that are required to hold larger amounts of capital to cover their increased risk-taking.

◆ 1.Operational risk management framework

➢ **Principles for the Sound Management of Operational Risk**

- From the very beginning of the regulatory regime, regulators have recognized the shortcomings of using only regulatory capital to cover operational risks.
- Indeed, no amount of capital may be enough to cover the losses generated by disasters due to operational failures in the absence of sound management.
- As such, operational risk **is the only risk type** for which management principles are included in the Pillar 1 regulation, emphasizing that good operational risk management is mandatory, not optional.

Basel Requirement:

	MCR	Risk mgt framework
Credit	✓	X
Market	✓	X
Operational	✓	✓

◆ 1.Operational risk management framework

➢ **Principles for the Sound Management of Operational Risk**

12 Principles(updated in 2021.3 on RPSMOR):
1. **Culture** led by the board of directors and implemented by senior management
2. Maintenance of a sound and proportionate **ORM framework(ORMF)**
3. **Board** review and approval of ORMF
4. **Risk Appetite and tolerance statement** for operational risk to be approved and periodically reviewed by the board
5. Senior management role in **ORM policies** and systems development and implementation
6. Comprehensive identification and assessment of operational risk in material activities
7. **Change management** process adequately resourced and articulated
8. **Regular monitoring** of operational risk profile and exposures
9. Strong **control environment**: internal controls, mitigation, training, and risk-transfer strategies
10. Robust information and **communication technology (ICT)** management program, in line with ORMF
11.Business **continuity plans** in place and linked with ORMF
12. **Public disclosures** on approach to ORM and risk exposures

◆ 1.Operational risk management framework

➢ **The Importance of Risk Culture for Regulators**

- Banks with a strong culture of risk management and ethical business practices are less likely to experience damaging operational risk events and are better placed to effectively deal with those events that occur.
- In the eyes of regulators, risk culture is closely associated with good conduct and ethics, and falls under the responsibilities of the board, applicable to and attested by all employees.
- A strong risk culture must be documented through policies and codes, applicable to everyone in the organization.
- The board of directors and senior management are expected to promote ethical behavior that convincingly reinforces
  - ✓ Codes of conduct and ethics,
  - ✓ Compensation strategies,
  - ✓ Training programmes to support operational risk management.

◆ 2. Operational resilience and framework

➢ **Operational resilience** relates to the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover from, and learn from operational disruptions.

➢ With the increase of cyber risk and the occurrence of several high-profile cybersecurity attacks, there has been a shift in the industry's mindset toward accepting that severe operational disruptions are inevitable, at least occasionally.

➢ **Different Regulatory expectations :**

- First Regulatory Guidance on Operational Resilience: The UK
- US Regulation
- BCBS Principles on Operational Resilience
- Other Regulators on Other Aspects of Resilience: ECB and MAS

◆ 2. Operational resilience and framework

➢ **First Regulatory Guidance on Operational Resilience: The UK**

- **Continuity of business services:** This element is the closest to the classic approach of business continuity planning and prevention by mitigating the risk of disruption of critical business provisions.
- **Important business services:** Firms are required to identify the services that, if disrupted, would cause "intolerable levels of harm to consumers or market integrity" and to ensure the continuity of these services within tolerance levels.
- **Impact tolerance levels:** Firms are asked to quantify the amount of disruption that could be tolerated in the event of an incident. Tolerance levels also aim to help senior management and the board set their own standards for operational resilience, prioritize, and make investment decisions."
- **Management of disruption:** The response to disruption, the maintenance of trust by key stakeholders, and clarity of communication in times of crisis are other important elements of resilience for firms that contribute to the stability of the system.
- **Lessons learned**: Financial firms are required to learn from past events.

◆ 3. Risk Identification

① **Heterogenous** 异质性. (所不同的).

- Operational risk is a set of eclectic risks, with different causes, consequences, and distributions of losses. Even within a risk category, operational risk events can be very different.
  - ✓ External fraud incidents range from stolen credit cards to ransomware. Internal fraud incidents include cash theft and rogue trading.

② **Idiosyncratic** (独特性)

- Operational risk types such as EDPM are driven or mitigated by the quality of a firm's processes and systems. Largely though, operational risk can be mitigated or elevated by a firm's ability and willingness to manage it.
- However, even for very risk-averse organizations, operational risk cannot be entirely eliminated through avoidance, hedging, or insurance.

提升

③ **Heavy tailed**

- Operational risk materializes, for most event types, in a multitude of small losses, and a small number of large losses several orders of magnitude bigger than the median of the distribution.

低频高损

高频低损

◆ 3. Risk Identification

OR events 之间相关
OR 与 CR 与 MR 相关.

④ **Interconnected** (高度相关)

- The different types of operational risk are partially correlated because several of them share common internal causes, such as weaknesses in certain controls, human errors, or poor risk culture; or common external causes, such as economic, political, and environmental events.
- In addition, operational risk connects with market risk and credit risk.

⑤ **Dynamic**

- The nature and intensity of the many operational risk exposures depend on the activities of an organization or industry and they evolve with these activities.
- The evolution of operational risk follows the development of the industry itself.
  - ✓ TSB failures and Covid-19

Trust and saving bank.

◆ 3. Risk Identification

➢ **Scope of Risk Identification**

主 ● **Top-down risk identification** (3种方法) 主要管理层

① Business-specific risk identification: **exposures and vulnerabilities**
② The risk wheel: brainstorming tool to encourage **Domino effect** 头脑风暴
③ Emerging risk identification: horizon scanning

次/辅 (次流) ● **Bottom-up risk identification** 免费的经验教训!

① Event and loss data analysis: **Near misses**
② Risk and Control Self-Assessment (RCSA)
③ Process mapping (流程)

- The **reconciliation** of top-down and bottom-up generates a comprehensive view of the operational risk profile. 和解.

◆ 3. Risk Identification

➢ **Extreme Risk Identification: Scenarios/stress-test identification**

- **Scenario/ stress-test identification** is a natural progression from the risk identification exercise. It is the first step of scenario analysis, a core component of operational risk and capital assessment.
- Regulatory Guidance on Scenario Analysis for **Operational Risk** and **Resilience**
  - ✓ Scenario analysis is a method to identify, analyze and measure a range of scenarios, including low probability and high severity (低频高损) OR. events, some of which could result in severe operational risk losses.
  - ✓ Banks should prepare forward-looking business continuity plans (BCP) with scenario analyses associated with relevant impact assessments and recovery procedures.

◆ 3. Risk Identification How to select Scenarios?

➢ **Brainstorming Techniques**

① **The preparation phase** historical data

- Compiling a "**preparation pack**" of documents that will help later for the selection and assessment of scenarios.
- With the help of an **external expert** to mitigate:
  - ✓ **Myopia:** the over-estimation of recent events
  - ✓ An excessive focus on scenarios driven by external causes

② The generation phase

- The first phase of a scenario workshop
- Aimed at producing a long list of scenarios.

③ The intermediary phase

- **Scenario selection** in which some scenarios are consolidated, and others eliminated or added.

④ The final phase

- compare the scenarios with an industry list of scenarios, to determine whether it has omitted any relevant scenarios or risk drivers.

◆ 3. Risk Identification

➢ **Describing Operational Risks**

- **Taxonomies** are an articulated way to express risks in successive levels of detail.

➢ **① The Basel Taxonomy**

- **Level 1** is the highest-level category;
- **Level 2** is a detailed version of level 1;
- **Level 3** provides examples of risk.

✓ The Basel Committee only recognizes **the first two levels as regulatory** categories. Level 3 provides examples and illustrations.

◆ 3. Risk Identification level 1:

Event Type	Acronym	Examples	Frequency	Severity
1. Internal fraud	IF	Fraud and unauthorized activities by employees	2%	2%
2. External fraud	EF	Theft and fraud, hacking damage	30%	9%
3. Employment practices and workplace safety	EPWS	Contract termination issues, discrimination, employer's liability	15%	5%
4. Clients, products, and business practices	CPBP	Client misinformation, complaints, and discounts due to errors, product misspecification	22%	52%
5. Damage to physical assets	DPA	Destruction of equipment, natural disasters, losses	1%	1%
6. Business disruption and system failures	BDSF	IT breakdown, outages	2%	5%
7. Execution, delivery, and process management	EDPM	Processing errors, missing documentation, vendor disputes	28%	27%

(流程)

◆ 3. Risk Identification

(全读)

➢ Basel Categories Levels 1, 2 and 3 regarding IF, EF and EPWS

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/deiscrimination events, which involves at least one internal party.	Unauthorised Activity	Transaction not reported (intentional) Trans type unauthorised (w/monetary loss) Mismarking of position (Intentional)
		Theft and Fraud	Fraud / credit fraud / worthless deposits Theft / extortion / embezzlement / robbery Misappropriation of assets Malicious destruction of assets Frogery Check kiting Smuggling Account take-over / impersonation / etc. Tax non-compliance / evasion (wilful) Bribes / kickbacks Insider trading (not on firm's account)
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	Theft/Robbery Forgery Check kiting
		Systems Security	Hacking damage Theft of information (w/monetary loss)
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee Relations	Compensation, benefit, termination issues Organised labour activity
		Safe Environment	General liability (slip and fall, etc.) Employee health & safety rules events Workers compensation
		Diversity & Discrimination	All discrimination types

◆ 3. Risk Identification

➢ Basel Categories Levels 1, 2 and 3 regarding CPBP

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Clients, Products & Business Practices	Lossess arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations Suitability / disclosure issues (KYC, etc.) Retail consumer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender Liability
		Improper Business or Market Practices	Antitrust Improper trade / market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laudering
		Product Flaws	Product defects (unauthorised, etc.) Model errors
		Selection, Sponsorship & Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory Activities	Disputes over performance of advisory activities

3. Risk Identification

➢ **Basel Categories Levels 1, 2 and 3 regarding to DPA, BDSF and EDPM**

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Disasters and other events	Natural disaster losses Human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	Hardware Software Telecommunications Utility outage/disruptions
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution & Maintenance	Miscommunication Data entry, Maintenance or loading error Missed deadline or responsibility Model / system misoperation Accounting error / entity attribution error Other task misperformance Delivery failure Collateral management failure Reference Data Maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer Intake and Documentation	Client permissions / disclaimers missing Legal documents missing / incomplete
		Customer / Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
		Trade Counterparties	Non-client counterparty misperformance Misc. non-client counterparty disputes
		Vendors & Suppliers	Outsourcing Vendor disputes

3. Risk Identification

➢ **The Evolution of Risks in the Financial Industry** { ① Basel ② ORX.

① ● **The Basel classification** does not fully reflect the current risk exposures across the financial sector anymore.

- ✓ E.g. The 2007-2009 financial crisis underlined t he need for stronger regulation, with a particular focus on selling practices and information to customers.

② ● In 2019, **Operational Risk data exchange(ORX)** published a new reference taxonomy, reflecting the changes in the industry and risk types.

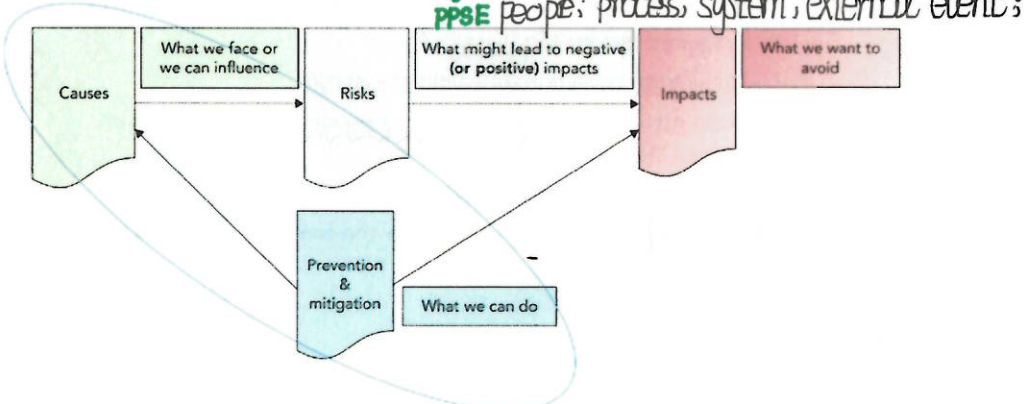
- ✓ It presents 14 level 1 risk types compared to 7 from Basel, and some level 2 risks have been elevated to level 1 given their prominence in today's world.
- ✓ Level 1 risk type: People, Physical Security & Safety, Business Continuity, Financial Crime.....

3. Risk Identification

➢ **Structure of Taxonomies**

- Best practice is to distinguish and separately categorize the different components of uncertainties: **causes, risks, impacts, and controls.**

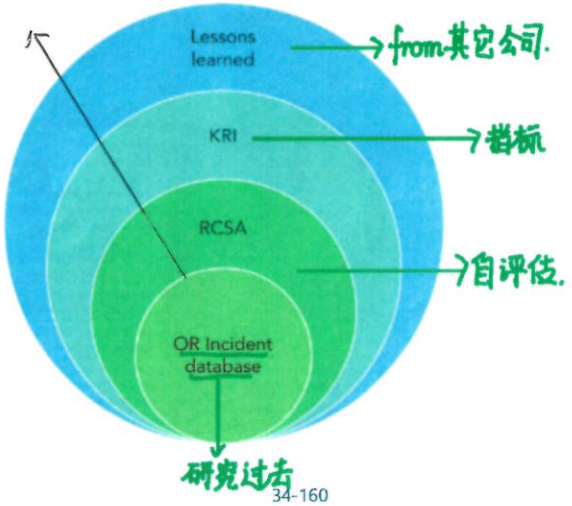
PPSE people; process, system, external event;



◆ 4. Risk Assessment Tools

➢ **Concentric circle of an operational framework (2000).**

前瞻.



◆ 4. Risk Assessment Tools

➢ **The Challenges of Comprehensive Data Collection**

① Regulatory Requirements Regarding Operational Risk Data Collection
② Incident Data Collection Process
③ Comprehensive Data
④ Dates of Incidents and Settlement Lags
⑤ Boundary Event Reporting
⑥ Data Quality Requirements
⑦ Data Features of Operational Risk

◆ 4. Risk Assessment Tools

① Regulatory Requirements Regarding Operational Risk Data Collection

- The Basel Committee for Banking Supervision (BCBS) lists eight criteria for data quality and collection processes under the SA.
  - ✓ a required history of 10 years of data;
  - ✓ A minimum collection threshold of €20,000;
  - ✓ mapping to the Basel event-type categories when reporting on internal losses;
  - ✓ the requirement to report dates of occurrence and recovery
  - ✓ processes "to independently review the comprehensiveness and accuracy of loss data."

◆ 4. Risk Assessment Tools

③ Comprehensive data

- ✓ A bank's internal loss data must be comprehensive and capture all material activities and exposures from all appropriate subsystems and geographic locations.
- ✓ The Basel committee does not define "material activities and exposures," but sets a minimum threshold for loss reporting at €20.000.
- ✓ Regulators generally only require the recording of losses directly identifiable as negative financial effects of operational incidents.
  - ◆ The term used," non-financial" impact, is particularly misleading because the indirect consequences of many material operational risk events have real financial implications. for example：名誉上.
- ✓ **Grouped losses** are distinct operational risk events connected through a common cause. 由于相同原因.

潜在漏洞

◆ 4. Risk Assessment Tools

④ Dates of incidents and settlement lags

- ✓ Banks must provide information on gross loss amounts for each operational loss event as well as the reference dates of the event.
- ✓ Each operational incident has four important dates:
  - a) Date of occurrence: when the event first happened (出现)
  - b) Date of discovery: when it is first identified (发现).
  - c) Date of reporting: when it enters the reporting database
  - d) Date of accounting: when the financial impact enters the general ledger hard to estimate loss.
- ✓ In extreme cases, there can be years between a) and b): "salami frauds". 小的损失 salami-欺诈.
- ✓ The gap between a) and b) reflects the visibility of issues in the organization, whereas the gap between b) and c) shows how diligently operational incidents are reported to the risk function. 勤勉程度.

◆ 4. Risk Assessment Tools

⑤ Boundary Event Reporting

- The Basel Committee provides useful guidance on boundary events as follows.
  - ✓ Operational loss events related to credit risk and that are accounted for in credit risk RWAs (Risk Weighted Assets) should not be included in the loss dataset.
  - ✓ Operational loss events that relate to credit risk, but are not accounted for in credit risk RWAs should be included in the loss dataset.

CR与OR 任选其一

  - ✓ Operational risk losses related to market risk are treated as operational risk for the purposes of calculating minimum regulatory capital under this framework and will therefore be subject to the standardized approach for operational risk.

OR与MR 放在OR.

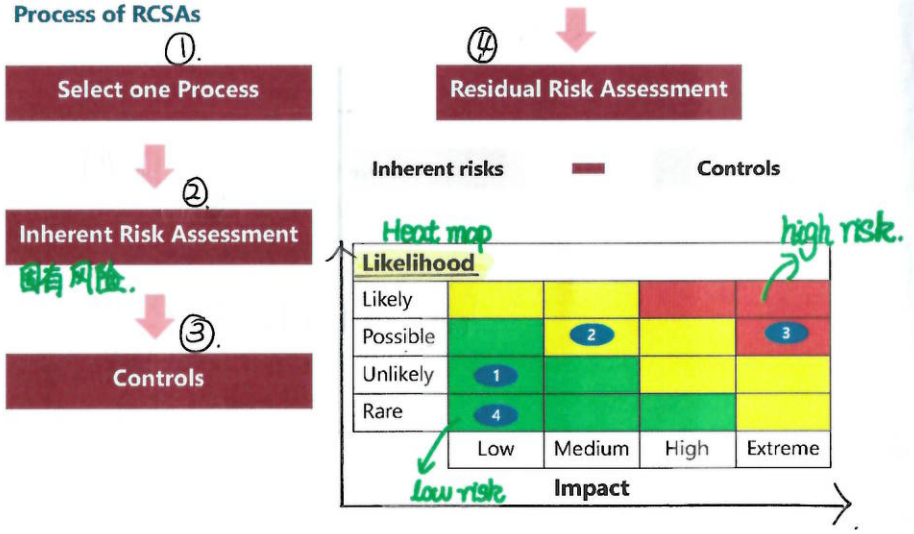
◆ 4. Risk Assessment Tools

➢ **Risk and Control Self-Assessment (RCSA)** 自评估.

- RCSA is a qualitative assessment exercise, using a simple and accessible tool.
- The RCSA refers to evaluating the likelihood and impact of operational risk faced by a business including both
  - ✓ the firm's risk exposures before the impact of existing controls has been assessed (**inherent risks**) → control.
  - ✓ those that remain after the evaluation of the controls in place (**residual risks**). → 5 residual risk 比较 → 预防 control.
    - likelihood ↑ → preparation control.
    - impact ↑ → corrective control.

◆ 4. Risk Assessment Tools

➢ **Process of RCSAs**



◆ 4. Risk Assessment Tools

三. ➢ **Key Risk Indicators**

- KRIs are monitoring metrics that signal the increase/decrease in the level of a risk, either in potential impact or in likelihood.

➢ **Examples of KRIs used in measuring likelihood include:**

- Increase in number of transactions per staff (risk of errors)
- Drop in customer satisfaction scores (risk of client attrition)
- Increase in the level of sales required for sales staff to achieve a performance objective (risk of fraud)

➢ **Examples of KRIs measuring impact include:**

- Increase in the level of proprietary company knowledge held by a key employee (higher impact of discontinuity or loss of knowledge in case of departure or sickness)
- Increase in sensitivity of data held on given server (higher impact in case of data leakage or loss)
- Increase in value generated by top-10 clients (higher impact in case of client attrition)

◆ 4. Risk Assessment Tools

➢ **Interaction among KPIs, KRIs, and KCIs**

- KPIs, KRIs, and KCIs overlap in many instances, especially when they signal breaches of minimum standards.

➢ **The failure of a control function is jointly a KPI, a KRI, and a KCI.**

- A poor performance will often become a source of risk.
- A key control failure always constitutes a source of risk.

➢ **KRI roles** key risk indicator.

- KRI thresholds and governance reflect the risk appetite and tolerance levels of an organization.
- The strength of an organization's KRI program reflects the maturity of its risk management function.
- Collection and reporting of comprehensive, preventive, and reliable KRIs provides useful information on the organization's level of risk management and control.

◆ 5. Quantitative Risk Measurement

➢ **Quantitative risk assessment**

- Causal analysis of scenarios 因果推断.
  - ✓ Fault Tree Analysis (FTA) 故障树 "and condition"
    - ◆a series of conditions that can either happen simultaneously alternatively "or" condition
- Factor Models

① ✓ FAIR methodology：找到所有的风险因子. (内容).

② ✓ Swiss cheese: control layering
  - ◆Assessing independence of controls is at least as important as assessing reliability of each individual control.

③ ✓ Root-cause analysis and Bowtie tool
  - ◆**"5-why" analysis:** why did this happen?

◆ 5. Quantitative Risk Measurement

➢ **Limitations and Constraints** steps 7 classes Basel.

① Data are split into risk classes (due to the heterogeneity of operational risk events) through a unit of measure (UoM). 分割 同质性个.
  - ✓ Finer segmentation leads to more homogenous data and more granular models, but it also reduces the amount of data available to estimate the models, leading to greater uncertainty in the results and increased complexity in the aggregation process.

② The distributions of severity and frequency of operational losses are typically assumed to be independent and modeled separately. (两者独立). UoM

③ Convolution is used to build loss distribution.

④ UoMs are aggregated using copulas, which are generalizations of correlations and can be used to model advanced dependency structures.

market risk

◆ 5. Quantitative Risk Measurement

➢ **Loss Distribution Approach (LDA) for Operational Risk**

- Frequency Modeling ①
  - ✓ Frequency in operational risk is commonly modeled with a Poisson distribution or Negative binomial distributions.
- Severity Modeling fat tail. ②
  - ✓ Severity distributions of operational risk are continuous, asymmetric, and heavy-tailed to account for the characteristics of operational risk losses: a large number of small events and a few very large losses.
    - ◆Log-normal distribution
    - ◆Weibull
    - ◆Generalized Pareto Distributions (GPD)

◆ 5. Quantitative Risk Measurement

➢ **The final challenge applies to extreme loss and data collection.**

➢ **Modeling the tail of an operational loss distribution**

- **Extreme Value Theory**
  - ✓ Block Maxima (Fisher-Tippet)
  - ✓ Peak-over Threshold (POT)

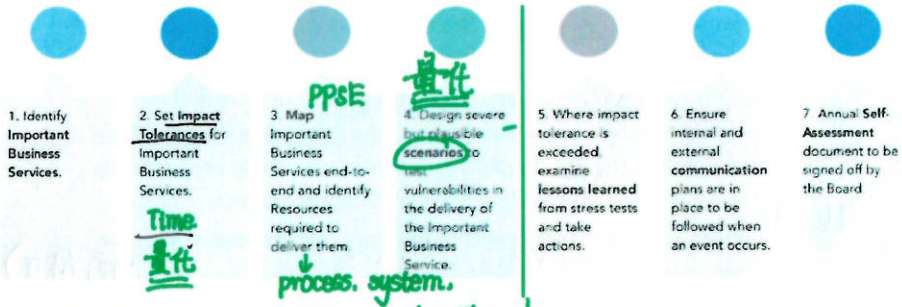
➢ **Data used to build an operational loss distribution**

- **Using Internal and External Loss Data**
  - ✓ Internal loss data is the backbone of LDA because of more relevant to the organization.
  - ✓ External loss data from peers can be supplemented. (补充)
    - ◆ The comparability of the number, types and size of members, the reporting threshold for incidents in the database.
- **Mixing Internal and External Loss Data**
  - ✓ **Scaling:** the adjustment for the size of losses to the size of the institution, or to other dimensions.
  - ✓ **Cut-off mix:** refers to the severity threshold at which external data are included in the model. (应用threshold) >5w
  - ✓ **Filtering:** relates to the criteria for losses to be filtered in or out of the calculation set of the institution performing the modeling.

数据处理

◆ 5. Quantitative Risk Measurement

➢ **Key steps for operational resilience.** 运营弹性



➢ **Business Impact Analysis**

- A BIA is the assessment of consequences of disruption of a process or a service, but also on the resources needed to develop recovery strategies.
- The BIA identifies both the operational and financial impacts resulting from the disruption of business functions and processes.

5. Quantitative Risk Measurement

➢ **Single points of failure (SPOF) are relevant KRIs for resilience.**

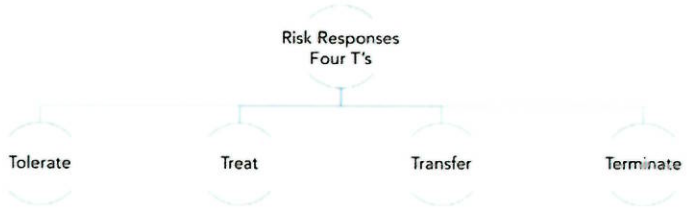
- Key employee dependency
  - Number of key employees without back-ups, without documented processes, with unique knowledge and skills, for example:
    - Coders
    - Pricing modelers
    - Cybersecurity specialists
    - Technical engineers (including physical assets)
- Key supplier dependency/low substitutability/high switching costs, such as:
  - IT/cloud providers
  - Data provider/data custodians
  - Payment platform
  - Internet/electricity/water providers
- Key systems dependency
  - Critical path mapping, dependency nodes

Models (因果: logic, process
因子:
LDA → AMA上的主要模型
Business impact analysis : resilience

6. Risk Mitigation

➢ **Risk response**

- **Tolerate(accept):** accepting the risk as it is.
- **Treat(mitigate):** encapsulating all the types of risk mitigation, mostly internal controls.
- **Transfer:** moving the risk to another party (external insurance).
- **Terminate(avoid):** removal of all risk exposure by discontinuing a product or ceasing operations in certain countries.



6. Risk Mitigation (分四类)

➢ **Preventive controls** ① Control.

- intended to reduce the likelihood of an incident.

➢ **Detective controls**

- designed to alert if an incident occurs, accelerate its resolution, and limit the impact of the incident to the firm or its stakeholders.

➢ **Corrective controls:**

- mitigating technique designed to lessen the impact to the institution when adverse events occur. They do not influence the likelihood of a risk happening, but lessen the pain if it does.

➢ **Directive controls** (指令性控制)

- include all the prescriptions and rules to execute a process.

◆ 6. Risk Mitigation

➢ **Control design**

- **Types of weakly designed controls include the following:**
  - ✓ **Optimistic controls:** large tasks before DDL 乐观的control. 稀释
  - ✓ **Collective controls:** "four-eyes check" diluting accountability.
  - ✓ **More of the same:** adding more controllers with the same design.
- **Control testing:**
  - ✓ **Self-certification or inquiry:** limited to secondary controls or controls related to low risk environments.
  - ✓ **Examination:** This requires supporting evidence and documentation.
  - ✓ **Observation:** involves real-time oversight. 监督.
  - ✓ **Reperformance:** "mystery shopping". 业绩再现.

◆ 6. Risk Mitigation process ②

① Prevention through design (PtD)

- Also called safety by design, is about inserting, right at the process design phase, the methods and structure that will minimize the risk of incidents.
  - ✓ Examples include checklists, communication protocols, standardization, and optimized work environments or systems design.

◆ 6. Risk Mitigation

② Typology and Mitigation of Human Error

a) **Skilled-based: slip** → 疲倦
   - ✓ Involuntary (tiredness)

b) **Rule-based: mistakes** (rule is wrong)
   - ✓ "Strong, but wrong"

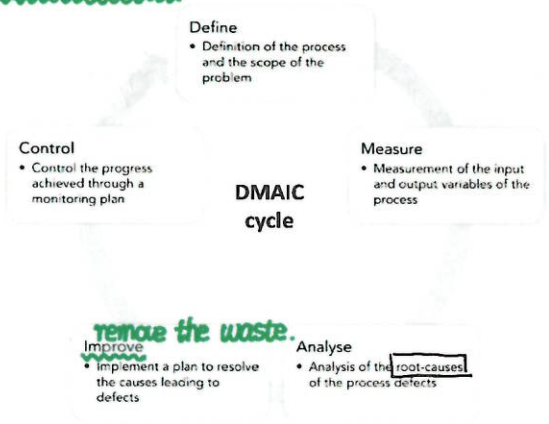
c) **Knowledge-based: mistakes** (IQ问题)
   - ✓ Wrong choice of action facing a new situation

Skill-based (SB): Slips	Rule-based (RB): Mistakes	Knowledge-based (KB): Mistakes
• Involuntary • Caused by inattention, distraction, environment, tiredness, etc. • Controls for SB errors: • Improved, supportive environment, re-engineered processes, adjusted pace, etc.	• *"Strong, but wrong"* • Wrong action based on flawed rules • Caused by wrong incentives, flawed products, misleading instructions, etc. • Controls for RB errors: change the rule	• Wrong choice of action when confronted by a new situation • Caused by lack of training, knowledge of the environment, causes and/or consequences of actions • Controls for KB errors: training, documented procedures, help file, escalation rules

◆ 6. Risk Mitigation

③ **Lean Six Sigma** 6σ (法律系统中任何的变异)

- A method that analyses processes and collaborative tasks to optimize workflow and improve performance by systematically removing waste and reducing variation.



专业 · 创新 · 增值

◆ 6. Risk Mitigation

④ **Quality improvement**

- **Represented by PDSA cycle (Deming wheel).**
  - ✓ **Plan:** objective; questions and predictions; develop a plan to improve the model (who, what, where, when)
  - ✓ **Do:** carry out the plan; document problems and unexpected observations; begin data analysis
  - ✓ **Study:** complete the data analysis; compare data to predictions; summarize what was learned lessons learnt.
  - ✓ **Act:** what changes are to be made? next cycle?

专业 · 创新 · 增值

◆ 6. Risk Mitigation New product.

➢ **Stages of involvement of risk function during a project's life.**

- **Initial stage (before kick-off):**
  - ✓ Risk identification and assessment: workshop facilitation, for important and critical projects
  - ✓ Mitigation and monitoring plans
- **Project life:**
  - ✓ monitoring and risk update, regular meetings with the risk team and the project team to update risk identification and assessment findings for important and critical projects.
- **Project closure:**
  - ✓ Debriefing, evaluations of project deliverables, analysis and documentation of the risks, lessons learned.

专业 · 创新 · 增值

◆ 6. Risk Mitigation ③ 业务连续性

➢ **Contingency planning (Plan B)**

- Contingency planning is a component of business continuity, disaster recovery, and of corrective risk management, the planning phase of corrective and directive controls.
- Specific forms of contingency planning are business continuity management (BCM) and disaster recovery plans (DRP). These are most relevant when we consider operational resilience.

前瞻性 → 危机处理小组。 事后。

◆ 6. Risk Mitigation

➢ **Event and crisis management**

- To manage a crisis or a large operational event effectively, organizations need to demonstrate three essential qualities:
  - ✓ **Speed:** Crises can spread very quickly (for instance, in case of a cyberattack)- the response must be swift, decisive, and appropriate.
  - ✓ **Competence:** Always use a suitably qualified specialist for each job.
  - ✓ **Transparency:** It is important as trust is gained and maintained by telling the truth and always being open and honest.
- In crisis model, firms should have at a minimum two types of incident response teams:
  - ✓ **A technical team** (or recovery team), composed of specialists who assess the incident and focus on restoring normal processes as quickly as possible.
  - ✓ **A communication team** (external or internal), which deals with the media and the different stakeholder groups, including employees.

◆ 6. Risk Mitigation ④ Transfer.

➢ **Two methods to transfer risks:**

- **External Insurance:** An organization agrees to pay a regular premium in exchange for being compensated should a certain risk materialize.
- **Outsourcing:** The process of delegating some of the company's tasks to a third party under a contractual agreement, such as IT server management, cloud computing, data centers, or call centers.

➢ **External Insurance**

- **For small losses:** Many large institutions either self-insure small losses via a captive subsidiary or just absorb the volatility.
- **For large losses:** Financial institutions mainly use external insurance to cover extreme operational risk "tail" events, such as cyber risks, business discontinuity, or major class action lawsuits.

➢ **Outsourcing**

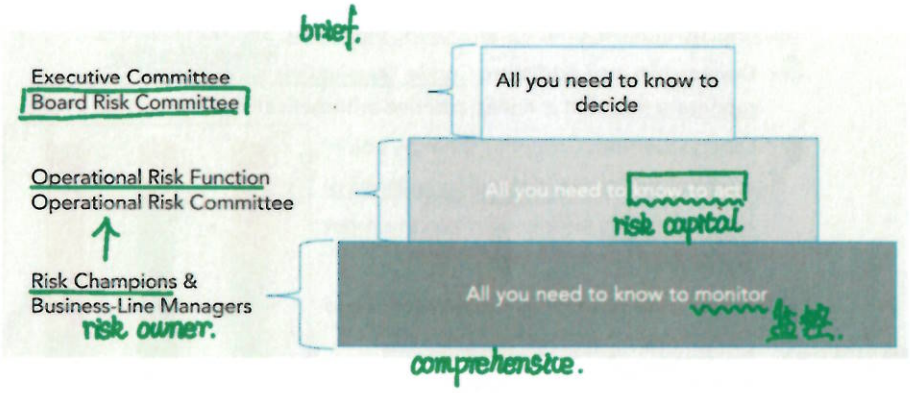
- **For traditional banks:** internalize credit decisions and allocations but outsource some of their ICT activities.
- **For FinTech banks:** more likely to manage their own technology platforms, but outsource credit risk decisions to other specialists.

◆ 6. Risk Mitigation

- Important elements such as reputational damage cannot really be outsourced (nor repaired) through insurance.
- **Reputational Risk Management**
  - Good practice in reputation management is, as usual, a combination of detective, preventive, and corrective measures
    - ✓ Detective controls, such as monitoring customer complaints on social media
    - ✓ Prevention, such as
      - ◆ Image building: positive narrative, value and ethos
    - ✓ corrective measures
      - ◆ Communication: Three R's: Regret, Reason, Remedy
  - There is an upside to crises when they are managed well: They are opportunities to learn and opportunities to shine.

◆ 7. Risk Reporting : Risk

- **THE "REPORTING CAKE"**



◆ 7. Risk Reporting

- **Considerations of operational reporting**
  - **Reports should be neither too large nor too small.**
    - ✓ **If too large:** significant risk of overlooking key pieces of information. Too much information can bury key insights.
    - ✓ **If too small:** it can become meaningless.
  - There is little uniformity in operational reporting across firms:
    - ✓ Some organizations dedicate much of their attention to the narrative of past risk events and the frequency and severity of financial losses.
    - ✓ whereas others are **more forward-looking** in their analysis and concentrate on risk outlook, key risk indicators, and action plans.

新兴

scenario analysis.

◆ 7. Risk Reporting

➢ **Main Components of Operational Risk Reporting**

① Top-10 risks and risk outlook in risk inventory
② Heatmap and risk register KCSA.
③ Risk appetite metrics → KRI
④ KRIs and issue monitoring Action.
⑤ Incidents and near misses
⑥ Action plans and follow-up
⑦ Emerging risks and horizon scan finding

◆ 7. Risk Reporting ★

➢ **Aggregating qualitative risk data**

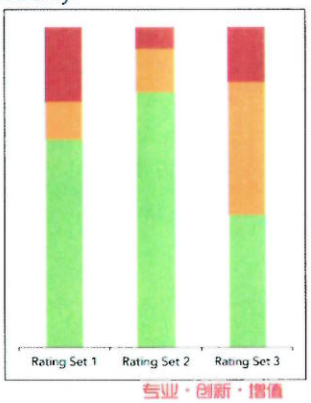
- The challenge is that risk scores, color ratings, and other indicators are discrete, qualitative, unfit for arithmetic treatment. Solution includes:

① ✓ **Conversion and addition:** Convert qualitative metrics into → Quantitative. monetary unit that is linear, additive arithmetically.

② ✓ **Categorization:** Grouping them by color or score avoids the misleading collapse of heterogeneous information into improper aggregate.

③ ✓ **Worst-case reporting:** Conservatism and prudent form, appropriate when risk tolerance is minimal, disadvantage is potentially over-alarming.

low frequency
high severity



◆ 7. Risk Reporting

➢ **Ways to overcome these challenges**

④ ● **Identify and analyze regularly large number of small losses** to

- ✓ detect a potential breach in control or a structural flaw in a process that would warrant an action plan.
- ★ ✓ If these losses occur randomly, without any specific structure, and are structurally limited, stable and repetitive, their average cost can be passed through to the customers as part of the cost of services.

● **Benchmarking operational losses**

不同公司横头数据可比性

- ✓ Reporting operational losses as a percentage of gross income, of total cost, total budget, or in basis points of capital facilitates the comparability.

● **No averages because of its asymmetric distributions**

- ✓ Averages hide the heterogeneity. The bias in operational loss averages is often caused by outliers.
- ✓ Better alternatives to averages are the median and the first and third quartiles of the distribution.

◆ 7. Risk Reporting

➢ **Ways to overcome these challenges**

- **Combined assurance:** The three lines of defense should work together to provide combined assurance to the board (RAG).

Risk Assessment Units (risk type or assessment scope)	First line review (assessment, testing, attestation)	Second line review (oversight, deep dive, testing)	Third line review (internal audit)
Cyber risk			
Compliance	no data		
Operational resilience			
Fraud			
Legal			no data
Third-party management and outsourcing			
Business Unit 1		no data	
Business Unit 2			
Legal entity A			
Legal entity B			no data
Project 1			
Project 2			
...			

Framework

Part 2: Focus Areas (CH8~CH16)

1. Cyber threats and Resilience
2. Financial Crime and Fraud
3. Third-Party Risk Management
4. Investor Protection
5. Model Risk and Model Validation

◆ 1. Cyber threats and 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 threats and Resilience

➢ 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 劳动力

◆ 1. Cyber threats and Resilience

➢ **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 渗透测试.
- ✓ Taxonomy of Cyber-Risk Controls

分类,术语 (统一术语)

③ Response and recovery testing and exercising

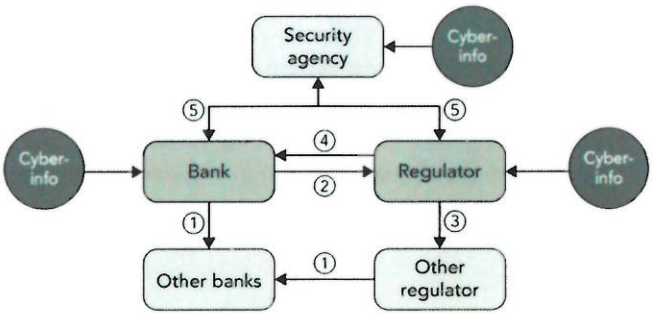
- ✓ Joint Public-Private Exercising

④ Cyber-security and resilience metrics.

- ✓ the need for forward-looking indicators

◆ 1. Cyber threats and Resilience

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



1. Cyber threats and Resilience

- 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

1. Cyber threats and Resilience

- **Taxonomy of ISR using a four-quadrant approach**

DATA INCIDENTS	THEFT or CORRUPTION	LOSS or UNVOLUNTARY DISCLOSURE
External causes or Third parties	1.Digital: Hacking, Virus infection, phishing and other cyberattacks 2.Physical: Theft, social engineering	3. Disaster, systems disruptions, third-party failure
Internal causes	4. Theft and transfer of digital or physical information by infiltrated employee or contractor 5. Departing employees take proprietary information or intellectual property from the firm (mishandled exits)	**Digital** 6. Database loss, back-up loss 7. Loss of devices by staff members 8. Errors when sending documents (e-mail recipients or attachments) **Physical** 9. Loss of printed documents (e.g., by accidentally disposing of them in a wastebasket) 10. Errors or accidental mentions of confidential information when communicating to outsiders 11. Loss of archives

1. Cyber threats and Resilience

- **Cybersecurity frameworks are often mandatory, or at least strongly encouraged, for companies that want to comply with industry related regulations.**
  - Three cybersecurity standards dominate the market:
    a) The US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)
    b) The Center for Internet Security Critical Security Controls (CIS)
    c) The International Standards Organization (ISO) frameworks ISO/IEC 27001 and 27002

◆ 1. Cyber threats and Resilience

➢ **Information controls can be grouped into two broad categories: Behavioral controls and Technical controls**

- **Behavioral controls**: these address human behaviors and fallibility when it comes to handling and protecting information.
  - ✓ The controls include awareness campaigns, rules of conduct and prudence for employees and contractors, online training, password management, supervision, and sanctions.
- **Technical controls**: these relate to all technical aspects of systems, either for prevention or detection.
  - ✓ Preventative controls relate to system architecture, access, firewalls, encryption, passwords and patching, and are essentially directed at external threats.

◆ 1. Cyber threats and Resilience

➢ **Equifax Case Study**

Date time	Events
2015	An internal audit detected a backlog of 8,500 unpatched vulnerabilities resulting from severe weaknesses in the patch management process.
2016-05	Equifax's W-2 Express website had already been hacked, resulting in the leak of 430,000 names, addresses, social security numbers, and other types of personal information.
2017-03-08	An alert was sent to Equifax on March 8
2017-03-10	Hackers breached Equifax's networks by exploiting a vulnerability in one of the systems (Apache Struts) via Equifax 's online dispute portal.
2017-09-07	Equifax issued a public announcement that their networks had suffered a data breach that exposed the personal information of 143 million customers, a number later increased to 147 million.
2019-07	Equifax agreed to pay up to $700 million in fines and compensation, $300 million of which was distributed to the individuals whose personal information had been exposed during the breach.

◆ 1. Cyber threats and Resilience

➢ **Lessons Learned from the Equifax Case Study**

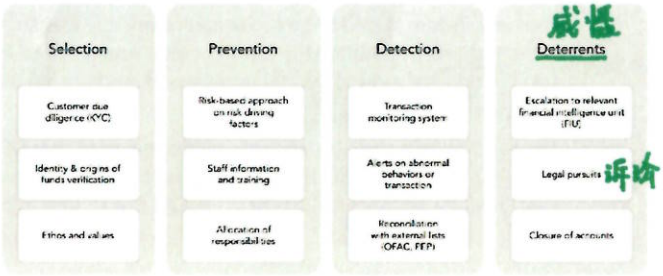
- A lack of a comprehensive inventory of IT assets.
- Failure of risk management policy enforcement, and specifically the failure to enforce the patch management policy.
- Inconsistent communication among employees on the remediation of security vulnerabilities.
- An expired SSL certificate designed to inspect encrypted network traffic.
- Poor external communication as part of the crisis management.

2. Financial Crime and Fraud

- In the UK, the Financial Conduct Authority's (FCA) Handbook defines financial crime as: *any kind of criminal conduct relating* to money or to *financial* services or *markets, including any offence involving:*
  - a) *fraud* or *dishonesty;* or
  - b) *misconduct in, or misuse of information relating* to, a *financial market; or*
  - c) *handling the proceeds of crime; or*
  - d) *the financing of* terrorism;
  - In other words, financial crime covers internal fraud and external fraud (points a and b) alongside what is generally referred to as money laundering (point c) and terrorism financing (point d).
- **The European Directive (EU 2015/949):** The action of organizing, facilitating, or concealing activities of money laundering (i.e., using funds or converting them to conceal their illicit origin) is regarded by the authorities as money laundering.

2. Financial Crime and Fraud

- **Controls for Internal Fraud Management and AML Risk Management**
  - Selection, prevention, detection and deterrents
  - The three phases in money laundering are placement, layering, and integration or extraction.
- **Controls for External Fraud Management**
  - Hiring an expert team



2. Financial Crime and Fraud

- 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.
  - Application of best practices with risk monitoring
    - ✓ **Wire transfers** are accomplished by sending payment messages among banks. Information about the originating bank and the customer should appear in the messages.
    - ✓ Changes in a customer's risk profile should trigger changes in the intensity of monitoring.

◆ 2. Financial Crime and Fraud

➢ 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

◆ 2. Financial Crime and Fraud

- USAA Federal Savings Bank (FSB) incurred a fine of $140 million from two separate consent orders reached with the Financial Crimes Enforcement Network (FinCEN) and the Office of the Comptroller of the Currency (OCC).

Date time	Events
The first quarter of 2021	A new transaction monitoring system implemented by USAA FSB has continued to prove problematic, according to FinCEN.
The end of 2021	the new system is said to be too sensitive and creates an unmanageable number of alerts and cases, and resulted in a total backlog of around 90,000 unreviewed alerts and 6,900 unreviewed cases. 积压.
March, 2022	the banking and compliance press published news that USAA Federal Savings Bank (FSB) incurred a fine of $140 million from two separate consent orders reached with the FinCEN and the OCC.

◆ 2. Financial Crime and Fraud

➢ **Lessons Learned from the Case Study:**

- The fines were due to a lack of control over AML risk, not because of demonstrated AML cases.
- Regulatory findings and sanctions mean costly AML remediation programs, often called lookbacks, in which the bank must review all client files for a specified period, verify client information, file suspicious activity reports (as they are called in the United States), and even close suspicious accounts. take actions about alerts.
- Additionally, the COVID-19 pandemic triggered changes in customer and business behavior, in particular a rise in remote transactions, that make it more difficult for financial institutions to identify anomalies.

◆ 3. Third-Party Risk Management

- **TPRM(Third-Party Risk Management)** relates to the identification, assessment, mitigation, and monitoring by organizations of the risks that arise from the use of third parties.
- The risk of "third party failure" is a level 2 category of the seventh event type of the Basel taxonomy "Execution, Delivery and Process Management" (EDPM)
- The evolution in recent years
  - financial firms have increasingly outsourced core processes
    - ✓ Many banks use third-party relationships, particularly with Fin Techs
  - Outsourcing to a company in a different legal jurisdiction brings with it not only country risk but also compliance and legal risk.
  - The COVID-19 pandemic increased the reliance on outsourcing even more and brought to the forefront the risks from international supply chain disruptions

◆ 3. Third-Party Risk Management

- 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.

◆ 3. Third-Party Risk Management

- 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.

六个风险.

(赔偿)

(自己司)

◆ 3. Third-Party Risk Management

- **Case Study 1: Capital One Data Breach** 缺口
  - Federal authorities ultimately arrested a former AWS cloud services employee for breaking into the bank's server. The former employee of AWS was charged with stealing "140,000 Social Security numbers and 80,000 bank account numbers in the breach."
- **Lessons Learned from the Case Study 1:**
  - The increase in breaches involving cloud databases and services is the result of poor security hygiene. 卫生.
  - Even though the major cloud service providers have built strong security into their offerings, it is still the business's responsibility to handle risk management, monitoring, backups, and maintenance.

◆ 3. Third-Party Risk Management

- **Case Study 2: OCC fines Morgan Stanley**
  - Morgan Stanley, through its Morgan Stanley Bank and Morgan Stanley Private Bank, received a $60 million fine imposed by the OCC due to failures in the risk management and oversight 疏忽. of vendors in the decommissioning of two wealth management business data servers in 2016. MS → □□ → vendor → data leakage. 清空格式化.
- **Lessons Learned from the Case Study 2:**
  - The bank did not exercise adequate due diligence in selecting the third-party vendors and did not adequately monitor the vendors' performance.

◆ 4. Investor Protection

- Compliance with financial laws and regulations usually falls into the fourth event type of the Basel taxonomy for operational risk, "Clients, Products and Business Practices" (CBPB).
- More specifically, compliance with investor protections generally falls into subcategories
  - Suitability, Disclosure & Fiduciary
  - Improper Business or Market Practices 市场操纵

4. Investor Protection

➢ **Regulatory Expectations**

- MIFID (Markets in Financial Instruments Directive) and MIFID II in EU
  - ✓ Alongside the reinforcement of investor protection, MIFID II set out additional requirements on public disclosure of data on trading activity, and on disclosure of transaction data to regulators and supervisors.
- Dodd-Frank in USA
  - ✓ Whistleblowers were granted increased protections under the act.
  - ✓ The **Volcker Rule** intends to prevent commercial banks from engaging in speculative activities and proprietary trading for profit.
  - ✓ Finally, the Consumer Financial Protection Bureau (CFPB) was created as an independent financial regulator to oversee consumer finance markets, including mortgages, student loans, and credit cards.

4. Investor Protection

➢ **Case Study 1: Statistics and Record Fines Cases**

- UBS was required to buy back$ 11 billion in securities and pay$ 150 million in penalties as part of the resolution of multi-state litigat ion, which charged UBS with "misrepresenting auction rate securities to investors as safe, cash-equivalent products, when in fact they faced increasing liquidity risk."
- The record for the largest fine for spoofing is held by JP Morgan, fined $920 million by the CFTC (Commodity Futures Trading Commission) in September 2020 by US regulators for "spoofing" in the precious metals and US Treasury markets.

➢ **Lessons Learned from the Case Study 1:**

- The case study illustrates how opinions and regulations have changed over time; before the advent of regulations on investor protection, practices like spoofing were accepted as normal.

4. Investor Protection

➢ **Case Study 2: FINRA Fines Deutsche Bank Securities**

- The Financial Industry Regulatory Authority (FINRA) Fines Deutsche Bank Securities, Inc. $ 2 Million for Best Execution Violations.
- FINRA found that, between 2014 and 2018, Deutsche Bank Securities was routing customer orders to exchanges through its smart order router.
  - ✓ This indirect routing of orders created delays of execution in customers' market orders and also caused lower fill rates.

◆ 4. Investor Protection

➢ **Lessons Learned from the Case Study 2:**

- Regulators tend to apply punitive fines such that the penalty more than offsets the benefits accumulated.
- The fines are aimed to act as deterrent for further deviations and have a signaling power to peer firms to encourage them to adjust their processes and monitoring practices to ensure compliance.

◆ 5. Model Risk and Model Validation

➢ **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.

◆ 5. Model Risk and Model Validation

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

① The model may have **fundamental errors**(conceptual error).

- ✓ 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**(execution risk).

- ✓ 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.

5. Model Risk and Model Validation

➢ **Three elements of effective process to manage model risk (cont'd)**

① A robust model development, implementation, and use.

✓ 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.

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.

5. Model Risk and Model Validation

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.

5. Model Risk and Model Validation

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.

◆ 5. Model Risk and Model Validation

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.

◆ 5. Model Risk and Model Validation

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.

◆ 5. Model Risk and Model Validation

➢ Model Risk Management Function

- To balance the cost and burden of model validation with the need to ensure that model risk is adequately addressed, MRM functions assign models to different tiers according to the risk they pose to the institution.
  - ✓ Models in the highest tiers will be reviewed in detail, with the validation team performing comprehensive back-testing and assessing the model for replicability of output.
  - ✓ These high-tier models also undergo more frequent full scope validations, usually every 2 to 3 years.
  - ✓ Lower-tier models are subject to a similar process but with the depth and frequency of the various actions tailored to the tier.
  - ✓ All models, independently of their tier, undergo an annual review of the environment, the data, and other important elements to ensure that no material changes since last validation.

5. Model Risk and Model Validation

➢ **Case Study 1: Gaussian Copula and CDO Pricing**

- In the early 2000s, David X. Li gave a method on the pricing of CDOs without calculating underlying asset correlations.
  - ✓ Li's uses CDS prices to infer the correlation of assets.
  - ✓ CDSs had been in existence for only about a decade, providing a very short and relatively benign sample
- When markets started showing signs of weakness in 2008, the correlations implied by the CDSs, and consequently the CDO prices, swung dramatically, resulting in a collapse of the market.
- In actuality, the problem was not with the formula itself, but with the fact that banks failed to update the copula model with the new correlation estimates implied by the higher CDS prices, and instead continued to price CDOs using the old assumptions.

5. Model Risk and Model Validation

➢ **Lessons Learned from the Case Study 1:**

- MRM always needs to replicate the model to ensure that no coding errors exist and that the prices generated are the intended ones,
- but its more critical responsibility is that of challenging the assumptions upon which the model relies and ensuring that users understand its limitations.

5. Model Risk and Model Validation

➢ **Case Study 2: Barclays' Acquisition and the Excel Spreadsheet Error**

- Lehman Brothers filed for bankruptcy on September 15, 2008. Three days later, Barclays Capital offered to acquire a portion of the US bank's assets, including some of Lehman's trading positions.
- A junior law associate at Cleary Gottlieb was tasked with reformatting the Excel file to a PDF document so it could be uploaded to the court's website. Already working on a tight schedule, he was not aware of those hidden rows, which were visible again in the PDF file.

➢ **Lessons Learned from the case study 2:**

- It is an excellent example of why even seemingly simplistic tools or models still need the right review, challenge and controls.

◆ 5. Model Risk and Model Validation

➢ **Case Study 3: NASA Mars Orbiter**

- NASA lost a $125 million Mars orbiter because a Lockheed Martin engineering team used English units of measurement, while the agency's team used the more conventional metric system for a key spacecraft operation.

➢ **Lessons Learned from the Case Study 3:**

- This is an error in the "assumptions" of the model, the choice of the unit (metric vs. imperial).
- It is equally undeniable that a small subset of these mistakes could result in catastrophic losses, such as the loss of the Mars orbiter.

◉ Framework

Part 3: Capital planning (CH17~CH20)

1. Risk-Adjusted Return on Capital
2. Modeling Diversification Effect
3. Economic Capital Implementation
4. Capital Plan in BHC
5. Stress Testing

◆ 1. Risk-Adjusted Return on Capital

➢ **What is risk capital?** 用来覆盖 unexpected loss = UC - EL.

- **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
    ↓ UL ↓ strategic risk loss
- Regulatory Capital
  ↳ Basel, by Supervisoring,

1. Risk-Adjusted Return on Capital

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

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

(risk-free return).
Unexpected loss.
⇑
存的 Economic Capital

- **After tax risk-adjusted return** → Expected loss.

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

→ Liquidity risk.

  - ✓ **Transfers** correspond to transfer pricing mechanisms, primarily between the business unit and the treasury group
- **Economic capital**= Risk capital + Strategic capital

每单位的经济资本economic capital所产生的回报.

ROE: Return on Equity
ROA: Asset.
ROC: Capital
} 度量业绩.

1. Risk-Adjusted Return on Capital

➢ **The use of RAROC** (应用).

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.

≥ if RAROC. is below the cost of equity, then there is no value being added.

② **performance evaluation** (业绩评估).

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

RAROC 与单位EC的成本对比 { Common Equity. / Preferred Equity

1. Risk-Adjusted Return on Capital

➢ **Hurdle Rate** Benchmark的

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

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

  - ✓ The **cost of preferred equity,** r_{PE}, is simply the yield on the firm's preferred shares. r_{PE} = dividend/price
  - ✓ The **cost of common equity,** r_{CE}, is determined via a model such as the CAPM.

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

◆ 1. 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.

◆ 1. Risk-Adjusted Return on Capital

➢ **Adjusting the traditional RAROC** (不同项目之间比较).

- 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.

$$\text{Adjusted RAROC} = \text{RAROC} - \underbrace{\beta_E(R_M - r_f)}_{\text{systemic risk}} \geq r_f.$$

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

↑ ARAROC↑, 项目越好.

↓ ARAROC ≥ r_f, 项目做

Summary:

◆ 1. Risk-Adjusted Return on Capital

RAROC:

- RAROC = Revenue − cost − EL − tax + return on EC. ± transfer / EC.
- 应用
  - 前 → budget, (RAROC > Hurdle rate)
  - 后 → evaluate. (RAROC > Hurdle rate)

➢ **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.

- ARAROC: ARAROC = RAROC − β(Rm − rf).
  应用: ARAROC ↑, 项目好↑
  ARAROC > rf, 接受项目.

1. Risk-Adjusted Return on Capital

➢ **Best Practices in Implementing RAROC Approach**

④ **Maintaining the integrity of the process.**

✓ a rigorous process of data collection and centralization of financial information (严格的)

⑤ **Combine RAROC with qualitative factors.**

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

⑥ **Put an active capital management process in place.**

(资本的 diversification)

2. 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**

UL firm ≤ Σ UL Business line ≤ Σ UL risks.

➢ **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. (认为 $\rho=0$)

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?

3. Economic Capital 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 (初步的) stage.

④ **Dependency Modeling in Credit Risk**

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

⑦ Credit risk in trading book

◆ 3. Economic Capital Implementation

➢ **Challenges within Economic Capital Implementation**

⑤ **Evaluating Counterparty Credit Risk**

big data.

- ✓ 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

⑥ **Assessing Interest Rate Risk in the Banking Book** 长期→credit risk.

- ✓ 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

market risk.

⑦ Credit risk in trading book.

↓ Basel 解决 3. fundamental review of trading book.

◆ 3. Economic Capital Implementation

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

① **Credit Portfolio Management**

② **Risk Based Pricing**

③ **Customer Profitability Analysis**

④ **Management Incentives**

EC的治理问题

◆ 3. Economic Capital Implementation

➢ **Concerns with regard to governance of economic capital framework(cont'd)** ↳Board

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;

3 business units : $\rho_{ij} = 0$

- ✓ 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. Economic Capital Implementation

➢ **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.

◆ 4. Capital Plan in BHC 视同为银行

Bank Holding Company.

➢ **Capital in Bank Holding Company** ⇒Bank.(银行控股公司)

- 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.

◆ 4. Capital Plan in BHC

➢ **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:资本金来源

✓ a clear definition and estimation of available capital resources.

④ Sufficient Capital Adequacy **Impact** Assessment

⑤ Comprehensive Capital Policy and Capital Planning

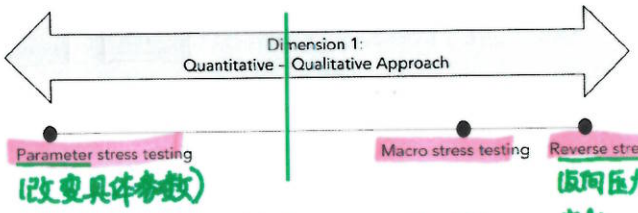
⑥ Robust Internal Controls

⑦ Effective Governance

◆ 5. Stress Testing

➢ **A Stress-Testing Taxonomy** (分类)

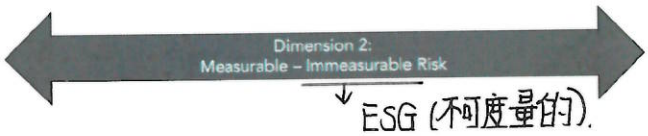
- **Dimension 1: Quantitative-Qualitative Approach Dimension**



$y=b_0+b_1x+\varepsilon$. (改变具体参数) (反向压力测试) 到底遭遇什么情况.

定性.

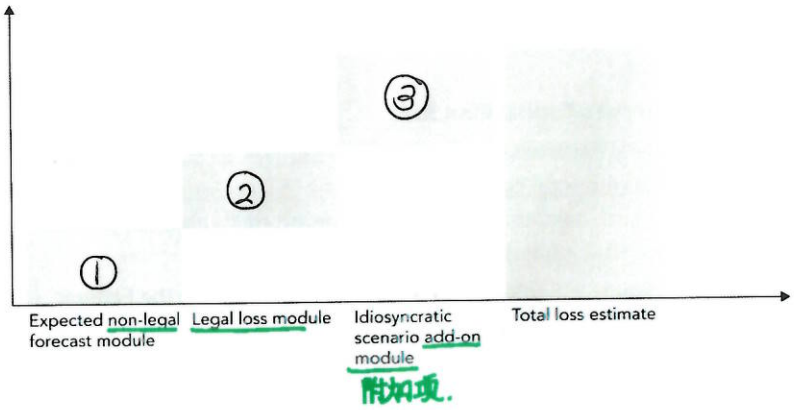
- **Dimension 2: Measurable-Immeasurable Risk** (不可计量)



ESG (不可度量的).

◆ 5. Stress Testing

➢ **Operational Risk Stress-Testing Framework**



附加项.

◆ 5. Stress Testing 操作风险压力测试

➢ **Stress-testing models**

- **The expected non-legal loss forecast module** is composed of two sub-components: the output from a quantitative model and an expert refinement.
  - ✓ Quantitative model: frequency and severity (a preferred approach).
    - ◆Regression(has risk drivers) and LDA can be applied
    - ◆Severity can be more complex to model than frequency as severity is highly impacted by tail events.
  - ✓ Once the model produces stressed losses, an expert refinement needs to be performed using scenario analysis. (修正)
- This **legal loss module** has a particular challenge associated with the delay between the onset of adverse macroeconomic conditions and the time when banking institutions suffer legal losses.

资本金压力测试.

5. Stress Testing

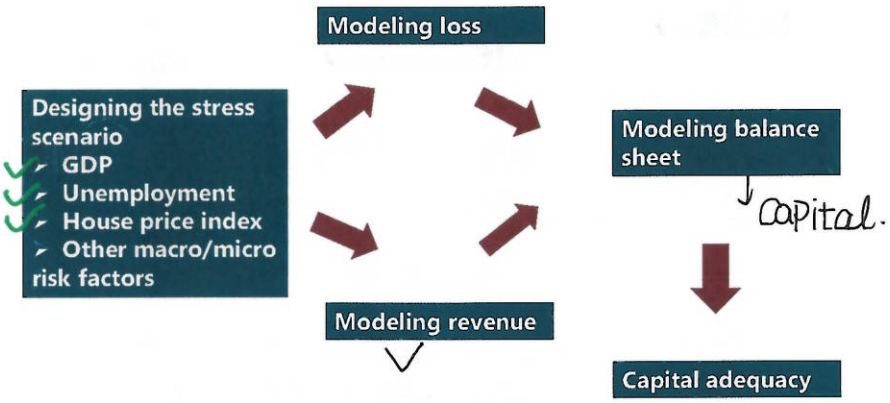
➢ **The time line of three stress testing process** Economic Capital.

- SCAP(US, March 2009) Financial Crisis前
  - ✓ 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.

Housing price index (HPI)

- EBA(EU, July 2011)
  - ✓ Retail and corporate only
- CCAR(US, March 2012) 之后
  - ✓ asking banks to develop their own stress scenario(s)

5. Stress Testing



5. Stress Testing

(一致性)

➢ **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.

Framework

Part 4: The Basel Accord (CH21~CH24)

1. Basel I
2. 1995&1996 Amendments
3. Basel II
4. Solvency II
5. Basel II.5
6. Basel III
7. Finalizing Basel III

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. Cooke ratio (资本充足率) Capital/RWA = Cooke Ratio (风险加权资产)
  - **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

Tier 1 Capital.
Tier 2.

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 (CEAi)

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

2. 1995&1996 Amendments

- **The 1995&1996 Amendment was established then to** Asset × risk weight.
  - 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** → market risk capital
      - ◆The **banking book** → credit risk → RWA
    - ✓ 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]**
        - ☐ $\text{Max}(VaR_{t-1}, m_c \times VaR_{avg}) + SRC$ default in T.B.
          昨天值. (3,4). 60天. specific risk charge.

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.

Pillar 2: supervision.
Pillar 3: Public disclosure.

3. Basel II

$RWA = \sum \begin{cases} \text{Assets} \\ \text{CEA} \end{cases} \times \text{weights}$ (修正)

- 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. (外部评级)
      - ✓ External rating, tenor and the counterparty
    - Adjustments for Collateral, two approaches
      - ✓ **Simple Approach** and **Comprehensive Approach**

◆ 3. Basel II

I. 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.

灵活度高.

◆ 3. Basel II

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

3种.

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:

自接剔除.

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

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

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

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%

3. Basel II

③ **Advanced Measurement Approach** (使用loss data).

- 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. frequency

Operational risk capital=WCL-EL.
↓LDA

- 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). → Pareto, lognormal, Generalized Gamma, Transformed beta, Weibull distributio
  - ✓ Generate a moderate number of detailed scenarios in which losses occur, and then measure operational losses in each scenario.

frequency.

BIA
↓ 修正
SA
↓ 新增.
AMA

frequency: Poisson and negative Binomial distribution

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. 最低标准
- **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 (Total Capital ≥ 8%·RWA + MRC + ORC

➢ **Pillar 1: Minimum Capital Requirement** ⇒ no diversification.

- 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) 资本金要求 × 12.5
  - ✓ 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.

Total Capital

RWA total risk = RWA credit + RWA (market) + RWA (operational)

RWA market = MRC market × 12.5

142-160

Basel II:
OR, CR, MR.
MCR (Pillar I).
{ 99% (10 days)
  99.9% (1yr).

◆ 4. Solvency II

➢ **Introduction** CR, MR ↑ 保险公司特有的.

- 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, 25%~40% of SCR)
    - ◆ stop engaging into any new business

143-160

◆ 5. Basel II.5

➢ **Market Risk Capital** ①

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

② → VaR_{avg} → SVaR_{avg} Stress VaR.

- 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.

144-160

◆ 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

◆ 6. Basel III

① Capital Requirements(cont'd)

- Total capital of a bank as per Basel III guidelines consist of:

T1

- ✓ **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.

T2

- ✓ **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

short term

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

long term.

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 ✗

分母

3131 6700 502101

6. Basel III

➢ **Contingent Convertible Bonds (CoCos)** 有条件的可转换 bond (自救机制).

- 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.

financial crisis.

- 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'.

➢ **Living wills** (生前遗嘱)

◆ 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($RWA_{IRB} \geq 72.5\% \times RWA_{SA}$)

◆ 7. Finalizing Basel III

① the standardized approach to credit Asset x risk weight

- improving its granularity and risk sensitivity.
  - ✓ For example, the Basel II standardised approach assigns a flat risk weight to all residential mortgages.
  - ✓ In the revised standardised approach mortgage risk weights depend on the loan-to-value (LTV) ratio of the mortgage;
- reducing mechanistic reliance on credit ratings, by requiring banks to conduct sufficient due diligence, and by developing a sufficiently granular non-ratings-based approach for jurisdictions that cannot or do not wish to rely on external credit ratings; 资本金最低限额
- providing the foundation for a revised output floor to internally modelled capital requirements (to replace the existing Basel I floor) and related disclosure to enhance comparability across banks and restore a level playing field.

◆ 7. Finalizing Basel III · 内部法，增加限制 → SA.

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 (input) values for bank-estimated IRB parameters such as PD and LGD floors
  - ✓ provided greater specification of parameter estimation practices to reduce RWA variability.

7. Finalizing Basel III

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

- Step 1: Find the business indicator (BI)

GI =). BI = ILDC + SC + FC

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

BIC = BI × marginal coefficients. → effective coefficient

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

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

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

- Step 4: Calculate Risk Capital Requirement

$$ORC = BIC \times ILM$$

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.

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。