CHARTERED INSTITUTE FOR SECURITIES & INVESTMENT

Managing Operational Risk in Financial Institutions

Effective from 11 November 2025

© Chartered Institute for Securities & Investment

Objective of the Examination

The objective of the examination is to ensure that candidates demonstrate the ability to apply the knowledge, theory and practical techniques required in order to investigate an operational risk incident, manage operational risk in the long term, model appropriate behaviours to support operational risk management in the workplace and effectively recommend and contribute to measures to enhance the operational risk culture and operational risk management in the workplace.

The examination will test candidates' knowledge and understanding of the following elements:

- The Operating Environment
- Organisational Considerations
- Operational Risk Management
- Risk Management Process
- Operational Risk Incidents
- Regulation of Operational Risk

Syllabus Structure

The unit is divided into **elements**. These are broken down into a series of **learning objectives**.

Each learning objective begins with one of the following prefixes: **know**, identify, **understand**, **apply**, **be able to analyse**,. These words indicate the different levels of skill to be tested. Learning objectives prefixed:

- **know** requires the candidate to recall information such as facts, rules and principles

- **understand** requires the candidate to demonstrate comprehension of an issue, fact, rule or principle

- **apply** requires candidates to be able to apply their knowledge to a given set of circumstances in order to present a clear and detailed explanation of a situation, rule or principle

- **be able to analyse** requires the candidate to review the information content in detail and draw conclusions

Candidate Update

Candidates are reminded to check the 'Candidate Update' area of the Institute's website (cisi.org/candidateupdate) on a regular basis for updates that could affect their examination as a result of industry changes.

Examination Specification

Each examination paper is constructed from a specification that determines the weightings that will be given to each element. The specification is given below.

It is important to note that the numbers quoted may vary slightly from examination to examination as there is some flexibility to ensure that each examination has a consistent level of difficulty. However, the number of questions tested in each element and / or case study should not change by more than two.

Title of Exam		
Element 1	The Operating Environment	7
Element 2	Organisational Considerations	8
Element 3	Operational Risk Management	6
Element 4	Risk Management Process	6
Element 5	Operational Risk Incidents	6
Element 6	Regulation of Operational Risk	7
TOTAL		**40 Questions**

Assessment Structure

The unit will be assessed by a 1 hour examination of 40 multiple choice questions drawn from across the syllabus.

Candidates sitting the exam by Computer Based Testing may have, in addition, up to 10% additional questions as trial questions that are not separately identified and do not contribute to the result. Candidates will be given proportionately more time to complete the test.

The examination will require candidates to give consideration to the full range of solutions and products as well as the instruments on which the solutions are based.

The unit is tested at level 4 on the Regulated Qualifications Framework.

Summary Syllabus

Element 1 The Operating Environment

1.1 Basel II

1.2 The relationship between Operational and Financial risks

1.3 Operational Risk in Financial Institutions

1.4 Balance sheet analysis

1.5 Risks of off-balance sheet activity

1.6 Horizon Scanning

Element 2 Organisational Considerations

2.1 Corporate governance

2.2 Role of organisational structures in operational risk management

2.3 Role of key personnel in operational risk management

2.4 Roles and responsibilities of the support and control functions

2.5 Raising risk awareness

2.6 Workforce planning

2.7 Methods of personal communication within a financial services institution

2.8 Employee commitment to the operational risk management framework

2.9 Whistleblowing within financial services

Element 3 Operational Risk Management

3.1 Key aims of operational risk management

3.2 Policy principles, application and scope

3.3 Business objectives and risk appetite

3.4 Interdependencies in the risk management process

3.5 Operational risk impact

3.6 Relationship between cause, event and impact

Element 4 Risk Management Process

4.1 Relationship between governance, policy, process, framework and risk culture

4.2 Embedding a risk framework in an organisation

4.3 Practical constraints of operational risk framework implementation

4.4 Techniques employed in identifying operational risk

4.5 Techniques to assess and measure operational risk

4.6 Operational risk response

4.7 Techniques to monitor and report on operational risk

4.8 Techniques to monitor and report on operational risk

Element 5 Operational Risk Incidents

5.1 Operational risk consequences

5.2 Risk escalation and incident management

5.3 Risk indicators and incident investigation

5.4 Root cause analysis

5.5 Internal control failures

5.6 Remedial action plan

5.7 Internal and external event data

5.8 Regulatory breaches

Element 6 Regulation of Operational Risk

6.1 Financial institutions regulation

6.2 Scope of lead UK and international regulatory standards

6.3 Recovery and resolution plans

6.4 Risk modelling and regulatory compliance

6.5 Development of operational risk standards

6.6 Legislative and regulatory requirements

Element 1 The Operating Environment

1.1 Basel II

On completion, the candidate should:

1.1.1 apply the Bank for International Settlements (BIS) definition of operational risk to determine risk categories within a financial services organisation

1.2 The relationship between Operational and Financial risks

On completion, the candidate should:

1.2.1 know the relationship between Operational and Financial risks

1.3 Operational Risk in Financial Institutions

On completion, the candidate should:

1.3.1 understand the general business models and associated risks of the following key types of financial services institutions:

- Insurance
- Retail banking
- Investment banking
- Investment management
- Stockbroking/ wealth management/ financial planning

1.4 Balance sheet analysis

On completion, the candidate should be able to:

1.4.1 analyse a financial institution's balance sheet to determine:

- assets
- liabilities
- liquidity

- gearing
- concept and role of capital

1.5 Risks of off-balance sheet activity

On completion, the candidate should be able to:

1.5.1 analyse the risks associated with off-balance sheet activity in:

- Financial futures
- Forward contracts
- Option contracts
- Swaps
- Caps and collars
- Securitisation / loan sales
- Exchange traded funds

1.6 Horizon Scanning

On completion, the candidate should be able to:

1.6.1 understand emerging risks and potential responses

1.6.2 analyse the effect of change driven by:

- Fintech
- Consumer demand
- ESG
- Business continuity

1.6.3 *analyse* the effect of corporate restructuring on business operations

1.6.4 *understand* the relationship between regulatory change, business change and risk

Element 2 Organisational Considerations

2.1 Corporate governance

On completion, the candidate should:

2.1.1 *understand* the role of Corporate Governance in financial services organisations

- UK corporate governance code
- Listing rules

2.2 Role of organisational structures in operational risk management

On completion, the candidate should be able to:

2.2.1 *analyse* the principles, application and limitations of the following organisational structures for the management of operational risk

- Three lines of defence
- Front, middle and back office (end-to-end risk management)
- Business unit (silo-based risk management)
- Enterprise wide
- Internal outsourcing
- External outsourcing/ third party suppliers

2.3 Role of key personnel in operational risk management

On completion, the candidate should:

2.3.1 *understand* the role of the following key personnel, groupings and reporting lines:

- Board of Directors including chairperson and non-executive directors (NEDs)
- Chief Executive Officer (CEO)
- Audit committee
- Board risk committee
- Chief Risk Officer

- Head of Operational Risk
- Operational risk committee
- Operational risk management function
- New business approval committee
- New product approval committee

2.4 Roles and responsibilities of the support and control functions

On completion, the candidate should:

2.4.1 *understand* the roles and responsibilities of the wider support and control functions in managing operational risk:

- Compliance
- Internal audit
- Legal
- Credit
- Human Resources
- Marketing
- Treasury
- Operations
- Business continuity
- Health and Safety
- Technology
- Information security
- General operational resilience

2.5 Raising risk awareness

On completion, the candidate should be able to:

2.5.1 understand how to build an operational risk aware culture via:

- training and education
- organisation-wide communication
- reinforcing lessons learnt

2.6 Workforce planning

On completion, the candidate should:

2.6.1 *know* the role of workforce planning:

- Succession planning
- Capacity management
- Retention
- Key person dependencies
- Talent management
- Relocation
- Remote working

2.6.2 know FCA expectations regarding:

- Remuneration and performance management
- Diversity and Inclusion

2.7 Methods of personal communication within a financial services institution

On completion, the candidate should:

2.7.1 *understand* the following methods of personal communication within a financial institution:

- Risk awareness workshops
- Exit interviews
- 360° reviews
- Salary review
- Staff satisfaction surveys
- Risk intranet

2.8 Employee commitment to the operational risk management framework

On completion, the candidate should:

2.8.1 *understand* the benefit of employee commitment to the operational risk management framework:

- importance of personal accountability and responsibility
- Role of integrity in decision making
- Fostering of a risk aware and conduct culture

2.9 Whistleblowing within financial services

On completion, the candidate should be able to:

2.9.1 know:

- regulatory requirements for whistle blowing/ speaking up
- the benefits of whistle blowing/ speaking up within the financial services environment

Element 3 Operational Risk Management

3.1 Key aims of operational risk management

On completion, the candidate should:

3.1.1 understand the key aims of operational risk management

3.1.2 understand the business benefits for the management of operational risk

3.2 Policy principles, application and scope

On completion, the candidate should be able to:

3.2.1 know:

- the purpose of an operational risk policy
- how an operational risk policy is developed

3.2.2 understand the scope and practical limitations of policy frameworks for managing operational risk

3.3 Business objectives and risk appetite

On completion, the candidate should be able to:

3.3.1 know the relationship between business objectives and risk appetite

3.4 Interdependencies in the risk management process

On completion, the candidate should be able to:

3.4.1 *analyse* the interdependent stages of the risk management process:

- Risk appetite setting
- Risk identification
- Risk assessment and measurement
- Risk response
- Risk monitoring
- Risk reporting and escalation

3.5 Operational risk impact

On completion, the candidate should be able to:

3.5.1 *understand* the operational risk impact of the following:

- Inherent and residual risk
- Direct and indirect losses
- Financial and non-financial impacts
- near misses and risk events resulting in unintended gains
- Exposure against risk appetite

3.6 Relationship between cause, event and impact

On completion, the candidate should be able to:

3.6.1 *understand* the relationship between cause/event/impact

Element 4 Risk Management Process

4.1 Relationship between governance, policy, process, framework and risk culture

On completion, the candidate should be able to:

4.1.1 understand how the relationship between the governance framework, operational risk policy, risk management process and the operational risk framework influences the firm's risk culture

4.2 Embedding a risk framework in an organisation

On completion, the candidate should be able to:

4.2.1 *understand* the stages employed in embedding a risk framework within an organisation

4.3 Practical constraints of operational risk framework implementation

On completion, the candidate should:

4.3.1 *understand* the practical constraints of implementing an operational risk management framework

4.4 Techniques employed in identifying operational risk

On completion, the candidate should be able to:

4.4.1 *apply* the techniques employed in identifying operational risk

4.5 Techniques to assess and measure operational risk

On completion, the candidate should be able to:

4.5.1 *apply* the techniques employed in assessment and measurement of operational risk

4.6 Operational risk response

On completion, the candidate should be able to:

4.6.1 understand operational risk management responses:

- Risk acceptance
- Risk transfer
- Risk avoidance
- Risk mitigation

4.7 Techniques to monitor and report on operational risk

On completion, the candidate should be able to:

4.7.1 *apply* the techniques employed in operational risk monitoring, reporting and escalation

Element 5 Operational Risk Incidents

5.1 Operational risk consequences

On completion, the candidate should be able to:

5.1.1 *analyse* the operational risk consequences of the following:

- Regulatory non-compliance
- Non-compliance with internal policy guidelines
- Fraud and theft
- Technological failures
- Customer dissatisfaction
- Delayed processing and documentary omissions
- Reputational risk
- Data protection breach

5.2 Risk escalation and incident management

On completion, the candidate should be able to:

5.2.1 know*:*

- risk escalation
- incident management reporting

5.3 Risk indicators and incident investigation

On completion, the candidate should be able to:

5.3.1 *understand* the use of risk indicators in incident investigation

5.4 Root cause analysis

On completion, the candidate should:

5.4.1 *analyse* an operational risk event to determine its root cause:

- Process
- People
- Systems
- External events

5.5 Internal control failures

On completion, the candidate should be able to:

5.5.1 *analyse* internal control failures

5.6 Remedial action plan

On completion, the candidate should:

5.6.1 understand*:*

- the stages of remedial action plan implementation
- the stages of monitoring and reviewing action plans post-implementation

5.7 Internal and external event data

On completion, the candidate should be able to:

5.7.1 *understand* the uses of internal and external event data

5.8 Regulatory breaches

On completion, the candidate should be able to:

5.8.1 know potential regulatory breaches associated with an operational risk incident

Element 6 Regulation of Operational Risk

6.1 Financial institutions regulation

On completion, the candidate should:

6.1.1 *understand* the importance of regulating financial institutions and the role of financial services regulation towards the consumer

6.2 Scope of lead UK and international regulatory standards

On completion, the candidate should:

6.2.1 *understand* the scope of the:

- Financial Conduct Authority (FCA)
- Prudential Regulatory Authority (PRA)
- International Organisation of Securities Commissions (IOSCO)
- Committee on Payments and Market Infrastructures (CPMI)
- Financial Stability Board (FSB)

6.3 Recovery and resolution plans

On completion, the candidate should:

6.3.1 *understand* the uses of recovery and resolution plans in reducing the impact of institutional failure on customers

6.4 Risk modelling and regulatory compliance

On completion, the candidate should:

6.4.1 *understand* the role of risk modelling in regulatory compliance:

- Stress Testing
- Reverse Stress Testing
- Scenario Analysis
- Internal and external data modelling

6.5 Development of operational risk standards

On completion, the candidate should be able to:

6.5.1 *understand* the drivers and impact of the development of operational risk standards to financial institutions

6.6 Legislative and regulatory requirements

On completion, the candidate should be able to:

6.6.1 *know the* relevant legislation and regulation relating to the operational risk environment:

- Role of the Money Laundering Reporting Officer (MLRO)
- Role of the Data Protection Officer (DPO)
- Know Your Customer
- Sanctions monitoring
- Foreign Account Tax Compliance Act (FATCA)
- Investment Firms Prudential Regime (IFPR)
- Sustainability Disclosure Regulation (SDR)
- Digital Operational Resilience Act (DORA)
- Bank of England Recognised Payment Systems Code of Practice: Operational resilience

6.6.2 know how financial services organisations address operational risk in relation to the Senior Managers and Certification Regime (SMCR)

6.6.3 know how financial services organisations address operational risk in relation to:

- Money laundering
- Terrorist financing

6.6.4 know how financial services organisations address operational risk in relation to data protection

6.6.5 know how financial services organisations address operational risk in relation to:

- Foreign Account Tax Compliance Act (FATCA)
- Investment Firms Prudential Regime (IFPR)
- Sustainability Disclosure Regulation (SDR)
- Digital Operational Resilience Act (DORA)
- Bank of England Recognised Payment Systems Code of Practice: Operational resilience