THE INSTITUTE OF OPERATIONAL RISK

CERTIFICATE IN OPERATIONAL RISK MANAGEMENT

An ATHE Level 4 Qualification

COURSE WORKBOOK

ENTERPRISES

CONDITIONS

About the Certificate in Operational Risk Management

The ATHE Level 4 Certificate in Operational Risk Management is an Ofqual regulated, professional qualification. The qualification is designed for students who have completed secondary education. Relevant work experience would be useful, but is not essential. The qualification is intended to provide students with an introduction to operational risk management, the tools used in the process, and how operational risk management fits into the wider risk management activities of the typical firm. The Certificate has been developed by the Institute of Operational Risk in collaboration with ATHE (an

awarding organisation regulated by Ofqual) as a core component of its mission to develop the discipline of operational risk management.

The Certificate is assessed as Qualification Credit Framework (QCF) Level 4, equivalent to European Qualification Framework (EQF) Level 5.

About the Institute of Operational Risk

The Institute of Operational Risk (IOR) is an association of operational risk professionals focused on the development of the practice of operational risk management through the ongoing development of its members and by engaging with industry participants to shape industry in the area of operational risk management. More information is available at www.ior-institute.org or email Education@ior-institute.org for general enquiries.

About IOR Enterprises Limited

IOR Enterprises Limited is a wholly owned subsidiary of the Institute of Operational Risk, focused on the delivery of various commercial initiatives on behalf of the IOR and its members.

IOR Enterprises Limited

2 Old College Court, 29 Priory Street, Ware, Hertfordshire, SG12 0DE UNITED KINGDOM

Registered in England and Wales under Company Registration Number 09954828

Published in the United Kingdom by IOR Enterprises Limited.

Certificate in Operational Risk Management Course Workbook (Online) ISBN 978-0-9935943-0-4

Table of Contents

Appendix 3: Certificate in Operational Risk Management – Exam Questions - Example..... 249

Introduction

This Course Workbook has been designed specifically for the Certificate in Operational Risk Management. The content of the Workbook has been structured in accordance with the approved syllabus of the Certificate and, as such, provides a sound foundation across all core operational risk management practices.

The Workbook is structured so that each chapter of the Workbook draws upon the preceding chapter(s) and it is thus recommended that study be undertaken in sequential chapters. References to other texts and reference material are included throughout the Workbook and students are strongly advised to make use of such further material to increase their knowledge and understanding of the subject matter. A suggested list of reading for those who wish to extend their knowledge is given at the end of the Workbook. Certain of the reference materials are available to students for download from the IOR's website, while other texts can be obtained commercially or from various public libraries or online forums.

Each chapter of the Workbook ends with a set of Key Learning Points on the topics covered in that chapter. Students are strongly advised to work through these, without making reference back to the chapter content, in order to test their knowledge and proficiency in the content of that section.

As a final check for students, a sample examination is provided at the end of the Workbook. Again, for this to have maximum benefit, students should complete it without reference to the Workbook content.

Students using the Workbook are advised to check if relevant permissions are in place to be able to access company documentation required to complete the Workplace Reflection exercises listed within the individual chapters of the Workbook. Restrictions may be in place for material deemed sensitive to safeguard company confidentiality. Additional reference material suggested to students, i.e., journal articles, may also only be accessible by paid subscription.

The Certificate has been designed to apply to operational risk management practitioners from all industry sectors. However, as much of the regulatory leadership on the topic of operational risk management has come from the financial services sector, there is a natural bias towards addressing the topic from a financial services perspective. The student should, however, be able to apply the concepts equally, irrespective of industry sector.

Chapter 1: Fundamentals of Operational Risk

Learning outcomes and assessment criteria

1.	***Understand*** the fundamentals of operational risk management.
1.1	***Examine*** the definition of operational risk.
1.2	***Identify*** the common risk types.
1.3	***Explain*** the relationship between operational risk and other risk types.
1.4	***Explain*** the different manifestations of operational risk within a firm.
1.5	***Explain*** the relationship between cause, event and impact.
1.6	***Examine*** the key components of the operational risk framework and governance structures.

Key themes

The key themes of this chapter are as follows:

- The definition of operational risk, including where operational risk fits in relation to other risk types, as well as the resultant boundary issues.
- The key components of an operational risk management framework and supporting governance structures, including an introduction to:
    - The basic operational risk management process.
    - Operational risk governance.
    - Risk and control self-assessments.
    - Key risk indicators.
    - Loss event management and recording.
    - Scenario analysis.
    - Operational risk modelling.
    - Operational risk reporting.
- Future developments.

Introduction to Chapter 1

Operational risk exists wherever there are operational processes and systems, automated or manual, complicated or simple. Any form of organised human endeavour or activity with intrinsic value may give rise to potential operational risk. However, it is only in the last few decades that operational risk management has been recognised as a discrete risk type, and it remains a very young discipline.

The emergence of the term operational risk as a discrete risk type started with the International Convergence of Capital Measurement and Capital Standards: A Revised Framework, more commonly known as Basel II, in the late 1990s (see Chapter 9, The Regulatory Treatment of Operational Risk). While primarily intended for internationally active banks, the operational risk management concepts set out in Basel II have since been incorporated into equivalent regulatory guidance and rules for the insurance sector and other areas of financial services including asset management and pension funds.

Today, most financial organisations have integrated management of operational risks within their business activities, which may be supported by centralised operational risk management function.

While operational risk emerged as a discrete risk type within financial services, the concepts of operational risk have been developed and practiced extensively within non-financial services firms. For many years non-financial services firms have invested significantly in managing their operational risks in areas such as health & safety practices, disaster management, preventing harm to customers due to product consumption, anti-corruption practices etc. Financial services firms are also realising the business benefits of managing operational risks and commercial drivers for sound operational risk management practices are now as important as regulatory drivers.

Today, given these drivers, the discipline of operational risk is maturing rapidly and many different systems, processes and management tools have been developed to support the management of operational risk. Nevertheless, the discipline still relies on some key fundamentals that all professionals involved with the management of operational risk need to know, and it is these fundamentals which are the focus of this chapter.

1.1 Examine the definition of operational risk

One of the commonly used definitions of operational risk within banking was published as part of Basel II, which defines operational risk as 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 reputation risk. Basel II explicitly frames legal risk as including (but not limited to) exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements. The definition, with slight variations, is now widely adopted across financial services firms, and we use it as our definition in this Workbook.

This definition is causal by nature; that is, it focuses on the risks arising from four primary causal factors - processes, people, systems and factors or events external to the firm. The table below highlights examples of operational risk for each causal factor covered by the definition.

Causal Factors	Examples
Processes	• New account opening documentation is sent to incorrect addresses of customers due to poorly designed processes. • Firm issues financial products to criminals/terrorists due to inadequate checks during the sales process. • Call centre staff provides incorrect advice to customers due to incorrect product documentation provided to them.
People	• Employees misuse customer assets for personal gain. • Discrimination of employees during the hiring process. • Senior managers commit financial statement fraud.
Systems	• Disruption to IT Systems due to defects in software. • Disruption to IT Systems due to attack by hackers. • Incorrect premium payments collected from customers due to error in software programme.
External	• Damage to physical assets due to a natural disaster. • Disruption to business operations due to rapid spread of a dangerous

Causal Factors	Examples
	epidemic or near-pandemic. • Damage to physical assets due to a terrorist strike.

Workplace reflection

Find out what definition is used for operational risk within your firm. Check how widely known and understood the definition is and whether any alternative definitions are used in the firm.

To expand this further the Basel II regulatory framework referred to earlier divided operational risk into seven risk event types:

- Internal Fraud - misappropriation of assets, tax evasion, intentional mismarking of positions, bribery.
- External Fraud - theft of information, hacking damage, third-party theft and forgery.
- Employment Practices and Workplace Safety - discrimination, workers' compensation, employee health and safety.
- Clients, Products, and Business Practice - market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning.
- Damage to Physical Assets - natural disasters, terrorism, vandalism.
- Business Disruption and Systems Failures - utility disruptions, software failures, hardware failures.
- Execution, Delivery, and Process Management - data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets.

One common way to classify operational risk is to consider expected vs. unexpected risks. Some operational risks may be expected because of their being inherently associated with the internal or external environment of the firm and hence may occur frequently. Examples of such risks may include:-

- Credit card fraud for a firm offering credit card products.
- Damages due to hurricanes for an asset management firm with offices in a city which experiences a hurricane season every year.
- Disruption to IT systems due to power cuts for an insurance firm with offices in a city where seasonal power cuts are normal.

As these risks are inherent part of the business environment, management of them is integrated within the planning and execution of business activities. Firms may also incorporate the risks within the pricing of their products. If the firm is unable to include the risk within their product pricing, they may raise accounting provisions, include it as part of business budgets or invest in improving the efficiency of business processes.

Some operational risks may be unexpected because they are not an inherent part of the internal or external environment of the firm and hence may occur rarely. Examples of such risks may include:

- Disruption to IT Systems due to the escalation of a cyber war between two or more countries.
- Damage to physical assets due to solar storms.
- Disruptions to business operations due to the rapid spread of a serious epidemic.

As such risks are not an inherent part of the business environment, management of such risks may involve support from specialist departments e.g. Business Continuity Management department to deal with business continuity related risks. Such risks may be managed using capital reserves, insurance or investment in controls.

1.2 Identify the common risk types

1.2.1 Risk types

There are many ways to categorise the risks faced by financial services firms and the table below highlights one way of such categorisation.

Risk Type	Description
Strategic risk	Uncertainties that may affect or may be created by an organisation's business strategy and strategic objectives. Examples of strategic risk include: • Products offered by the organisation may not meet customer needs. • Over-reliance on a single product for revenue generation. • Failure to anticipate a new competitor entering the market which intends to be very aggressive about acquiring market share.
Credit risk	The risk of loss due to counterparty default. It is restricted to default or situations where the counterparty can but refuses to make payment when due. Examples of credit risk include: • A business is unable repay a loan because of the failure of a major creditor. • A customer defaults on their mortgage payments as a result of redundancy. • Insurance company is unable to claim on a reinsurer because the reinsurer is insolvent.
Market risk	The risk of loss due to adverse economic changes in market conditions, rates or prices or fluctuations in volatility. Market risk includes price risk, volatility risk, interest rate risk and foreign exchange risk among others. Examples of market risk include: • Loss of revenue due to changes in exchange rates between sterling (GBP) and euro (EUR). • Losses in an investment portfolio due to significant drop in FTSE 100 index.

Risk Type	Description
	• Unexpected increase in debt-related interest payments due to policy changes announced by a central bank.
Liquidity risk	The risk of not having adequate funds available to meet financial commitments as they fall due. This may be caused by local or foreign economic conditions, a reduction in the firm's credit rating, or situations where the firm is interested in trading an asset but cannot do so because nobody in the market wants to trade that asset. Examples of liquidity risk include: • A significant change to the credit rating of an organisation which may result in material withdrawal of funds by customers. • A material change to the credit rating of a country which may result in panic withdrawal of funds from all banks in the country which they cannot meet. • Significant level of uncertainty in the market which may dry up demand for financial instruments held by the firm.
Insurance risk	Also known as underwriting risk. Insurance risk is the risk of a claim being made on an insurance policy or underwriting. Examples of classes of insurance risk include: business interruption, cyber crime, directors' and officers' liability, key man, motor (individual or fleet), property, professional indemnity, terrorism, unauthorised trading, as well as life and health policies.
Operational risk	The risk of loss, direct or indirect, resulting from inadequate or failed internal processes, people and systems or from external events. Examples of operational risk include: • Accepting or offering bribe. • Theft of customer data from IT Systems by hackers. • Intentional mis-selling of products/services to clients.

1.3 Explain the relationship between operational risk and other risk types

Some firms look to manage their risks in an integrated way, under an umbrella framework sometimes known as Enterprise Risk Management (ERM). This approach is based on the premise that risks are interconnected and need to be managed together in a consistent way, with clear differentiation of the boundaries between them.

The issue of ensuring clear boundaries between different risks is something that operational risk managers face day-to-day. Chapter 4 explores in more detail the need for and benefits of a clear categorisation scheme for risks. Operational risk managers often need to interact with risk managers dealing with other risk types and have to justify why some risks should be considered as part of operational risk management. Even with clearly documented boundary conditions between risk types, from time to time situations arise which are not covered by existing definitions and need resolution with other risk disciplines.

Some examples of these boundaries are:

Credit risk: A credit risk should be considered under operational risk management if the risk may be caused by, for instance, fraud related to lending facilities, procedural failures in the credit process, inadequate collateral, inadequate credit models or inappropriate loan sales practices.

Market risk: A market risk should be considered under operational risk management if the risk is caused by transactional errors, limit breaches, internal or external fraud or inadequate collateral.

Liquidity risk: A liquidity risk should be considered under operational risk management if the risk may be caused due to non-economic factors (for example due to forecasting issues, unsuitable or mismatched investment strategies, model issues or timing issues).

Insurance risk: An insurance risk should be considered under operational risk management if the risk may be caused due to result of failure to follow policy or protocols, errors in actuarial modelling or inadequate documentation.

Strategic risk: A strategic risk should be considered under operational risk management if the risk is caused by errors in strategic business judgement, inappropriate or inadequate corporate governance, incomplete due diligence, inappropriate or incorrect advice, inappropriate management decisions or lack of management oversight.

The examples listed above highlight that the causal factors of other risks can be used to determine whether the risks should also be considered under operational risk management. If the causes of any type of risk relates to people, process, systems or non-economic external factors – then it can also be considered under operational risk management. Another example to understand this is mentioned

below:

Boundary Examples: -

1. A firm has advanced a sum of money to a customer and the customer defaults and fails to repay the loan. What caused the firm to lose the money?

- If the customer's business failed and, as a result, the customer lost everything and was unable to repay the firm, then the answer is simple, it is a pure credit loss.

- If, however, the customer failed to repay the firm because the loan agreement contained a technical deficiency which the customer was able to rely upon in court, the cause is the documentation error, which makes the loss an operational loss.

2. At the start of the trading day, a firm submits an order to purchase 1 million shares of an organisation at £1.20 per share, expecting the share price to increase to £1.26 during the trading day and sell the shares at that price point.

- Due to an error in the trading system, 3 orders of 1 million shares each were submitted. So the firm ended up buying 3 million shares at £1.20 per share.

- At the end of the day, the price declined to £1.10 and as the firm only wanted to hold the position for one trading day, it had to sell the position at this price. So the firm sold 3 million shares at price of £1.10 per share which resulted in a loss of £300,000.

- As the firm only wanted to purchase 1 million shares initially, only 1/3 (£100,000) of the trading loss can be attributed as market risk related loss.

- As 2 million additional shares were purchased due to trading system error, 2/3 (£200,000) of the trading loss should be attributed to operational risk.

Instances like this occur frequently in operational risk management, and need both careful analysis and the right questions being asked to ensure they are correctly categorised and reported.

Appendix 3: Certificate in Operational Risk Management – Exam Questions - Example

Students are recommended to test their knowledge of the topics covered in this Course Workbook, in preparation for the examination to attain the Certificate, by completing the following questions without referring to the answers on the last page of the Workbook. A total of 30 questions need to be answered correctly in order to achieve a pass mark in the formal examination.

Students may complete the example exam within the Workbook or refer to the APMG website to take the example exam online and gain familiarity with the system prior to the formal exam sitting. Instructions are included in the Student Handbook.

Self-Study Multiple Choice Questions

1. Which of the following causal factors is included in the Basel II definition of operational risk?

A. Strategy.
B. Systems.
C. Reputation.
D. Projects.

2. Which of the following is a primary risk type?

A. Strategic risk.
B. Reputational risk.
C. Conduct risk.
D. Legal risk.

3. Which of the following is an example of an operational risk?

A. Loss of revenue due to volatility in exchange rates.
B. Loss of revenue due to disruption to IT systems within bank branches.
C. Loss of revenue due to lack of demand for products.
D. Loss of revenue due to lowering of interest rates by the central bank.

4. What does a bow-tie model cover?

A. Cause, Event, Impact.
B. Event, Financial Impact, Non Financial Impact.
C. Primary Cause, Secondary Cause, Event.
D. Financial Impact, Reputational Impact, Legal Impact.

5. Which of the following pairs is a component of the risk management process?

A. Identification and response.
B. Dispute resolution and impact assessment.
C. Business planning and change management.
D. Strategic objectives and business continuity.

6. Which of the following would be an indicator of a robust risk culture within a firm?

A. Covering risk culture related topics within the operational risk policy.
B. Developing an e-learning course on the topic of risk culture.
C. Including risk culture related topics within the annual financial statement report.
D. Management of risk is an integral part of decision making.

7. Which of the following communicates how the management of operational risk can enable the firm to achieve its business objectives?

A. Operational risk appetite statement.
B. Operational risk policy.
C. Operational risk framework.
D. Operational risk process.

8. What is the prime function of an external audit?

A. To ensure that controls are effective.
B. To provide assurance on financial statements.
C. To provide assurance on the risk management framework.
D. To provide assurance on the internal audit function.

9. For which of the following is the firm's governing body primarily responsible?

A. Establishing a clear strategy and risk objectives for the organisation.
B. Assessing exposure to each operational risk to ensure it is within risk appetite.
C. Providing assurance that controls are being implemented.
D. Developing the operational risk framework.

10. Which of the following are all main categories of external change?

A. Legal, political, climate, organisational changes.
B. Technological, regulatory, economic, media changes.
C. Environmental, political, regulatory, legal changes.
D. Political, social , scientific, technological changes.

11. Which of the following reflects an expectation from customers as to how a firm manages its operational risk?

A. Customers can choose from a wide variety of products or services.
B. Customers are able to easily compare competitive products or services.

C. Customers are treated fairly and products or services perform as expected.

D. Customers should be able to purchase products or services on the internet.

12. Which of the following is a definition of risk appetite?

A. Risk appetite is a fundamental part of risk management because it provides evidence that a risk event has materialised.

B. Risk appetite is the amount and type of risk that an organisation is willing to pursue or retain in order to achieve its objectives.

C. Risk appetite is a loss resulting from inadequate or failed internal processes, people and systems or from external events.

D. Risk appetite is a process of classifying risks in a consistent way which enables the aggregation, analysis and reporting of risks.

13. What are the key elements of a firm's risk appetite framework?

A. Risk appetite statements, targets, metrics and policies.

B. Risk identification, risk assessment, monitoring and reporting.

C. Risk categorisation, risk events, risk indicators, RCSA and scenarios.

D. Risk reduction, risk acceptance, risk avoidance and risk transfer.

14. The purpose of a risk appetite statement is to:

A. Communicate that the organisation expects no risks to be taken.

B. Communicate to employees and external stakeholders, in a clear, concise, and understandable way, the organisation's risk appetite.

C. Communicate to external stakeholders only, in a clear, concise, and understandable way, the organisation's risk appetite.

D. Communicate to employees only, in a clear, concise, and understandable way, the organisation's risk appetite.

15. Which combination of the following methods may be used to express an organisation's appetite for operational risk in a quantitative way?

1. Thresholds for key control indicators.
2. Probability and impact risk matrices.
3. VaR models of operational risk capital.
4. Limits on reported operational losses.

A. 1, 2 and 3
B. 1, 2 and 4
C. 1, 3, and 4
D. 2,3 and 4

16. In relation to determining and implementing an operational risk appetite framework the role of the Chief Risk Officer is to:

A. Sign off the operational risk appetite statement that is produced as part of the operational risk

appetite framework.

B. Ensure that the organisation's operational risk appetite framework is consistent with its frameworks for any other key areas of risk (e.g., market or insurance risk).

C. Provide the governing body with a recommended risk appetite framework for approval.

D. All of the above.

17. Please indicate which of the following is a key objective in creating a risk data categorisation structure:

A. Knowledge of staff.

B. Allow free-formatting of data.

C. Simplicity of the taxonomy.

D. Acceptance by management.

18. Which of the below is an example of a risk categorisation scheme based on processes?

A. Customer onboarding, customer servicing, transactions, payments.

B. Physical, procedural, information security, legal & regulatory.

C. Commercial banking, commercial credit, commercial loans.

D. Branch, intermediary, online, call centre.

19. Which of the following data categorisation element types would be most relevant for identifying key risk indicators?

A. Financial impact type.

B. Causal type.

C. Non-financial impact type.

D. Control type.

20. Which of the following is the biggest challenge in the development of a data categorisation structure?

A. Getting management buy-in.

B. Where data categorisation takes place.

C. Effort to use and available staff time.

D. Consistent application of the taxonomy.

21. RCSA helps a firm to manage key risks it faces. This involves:

A. Identification of all key risks and related controls.

B. Evaluation of risks and controls and formulate appropriate actions.

C. Identification, assessment, monitoring and reporting risk with related controls.

D. Articulating the risk profile for internal governance and external reporting requirements.