

IRM's Level 4 International Certificate in Operational Risk Management

Qualification Syllabus

August 2024



A man with a beard, wearing a blue button-down shirt, is sitting at a desk in an office, focused on his laptop. The background shows a blurred office environment with shelves and a plant. The image is overlaid with a large, semi-transparent blue shape that contains the main text.

Build your career as a risk professional

Training with the IRM

With training courses covering a wide range of enterprise risk management topics, our courses are delivered by industry experts so you can immediately apply the latest in best practice techniques. As well as being practical and interactive, the courses allow you to log CPD hours and some offer accreditation.

Contents

About the Institute of Risk Management	1
IRM Qualification Aims	1
IRM Professional Standard	3
Time Constraints	4
Collaboration in the Design of the Qualification	4
Key Dates	4
Language Requirements	4
Support for Teaching and Learning	4
Qualification Structure	6
Entry Requirements	7
Equality and Diversity	7
Qualifications Delivery	7
Complaints	7
Overview	8
Assessment	28
Appendix 1	31
Appendix 2	32





1. About the Institute of Risk Management (IRM)

The IRM, is the leading professional body for risk management. The IRM is an independent, not-for-profit organisation that champions excellence in managing risk to improve organisational performance. IRM does this by providing Professionally recognised qualifications and training, publishing research and guidance and by setting professional standards across the world. IRM's members work in all industries, in all risk disciplines and across the public, private and not-for-profit sectors.

2. IRM Qualification Aims

IRM qualifications are aimed at practising or aspiring managers and leaders who are in decision making roles or working as risk management practitioners. The qualifications provide students with a broad knowledge and practical skills in operational risk management, which can be immediately applied in the workplace.

IRM qualifications provide a holistic, flexible, and module-based approach which is assessed by using either a combination of multiple-choice questions and written assignments in its certificates, and written assignments for the diplomas. However the IRM's Level 4 International Certificate in Operational Risk Management (ICORM) has 9 units which are assessed with multiple-choice questions.

The IRM's Level 4 International Certificate in Operational Risk Management (ICORM) is a Professional Level 4 qualification designed to introduce students to the fundamental theory, management, and application of Operational Risk Management to ensure timely organisational success. This enhances an organisation's ability to achieve its objectives and ensure sustainability based on transparent and ethical behaviours.

2.1 Aims of the IRM's Level 4 International Certificate in Operational Risk Management are to:

- Develop students' knowledge, understanding and skills needed to recognise and manage operational risks in an organisation.
- Develop enquiring minds, to ensure that students have the ability and confidence to work across different business functions in an organisation to recognise lead, manage and respond to operational risks in their departments and across the organisation; and
- Develop transferable skills including communication, problem solving, adaptability, time management, organisational and research skills.

2.2 IRM qualifications address these aims by:

Designing learning to impart knowledge through academic theory and practical application:

- Units 1 to 9 of the IRM's Level 4 International Certificate in Operational Risk Management provide the foundations of operational risk management through the examination of core principles and concepts which can effectively and practically be embedded within an organisation.

The 9 units explore various aspects of operational risk management in detail and meet the aims as follows:

- Each unit consists of a several lessons which provide knowledge in bite-size pieces.
- Each unit is accompanied by relevant references to essential and further reading material in books and articles supporting the lessons being taught.
- Each unit includes references to materials students are expected to access and assimilate (essential) and further reading materials that will widen their knowledge of the subject.
- The Certificate is delivered over a 3-6 month period, which requires skill in time management, which is supported by the planning materials in the Student Handbook.
- Undertaking the activities and engaging in the discussion forums for this qualification support students in completing and understanding challenging academic materials.
- Enabling students to be better able to be involved in and implement risk management processes.
- Undertaking the activities allows students to apply the theory taught to improve their confidence in their risk management knowledge.
- Each unit has been designed by qualified risk managers, who are expert practitioners in the field of risk management and engaged in academic activities outside of the IRM.
- The outline specification for the certificate has been shared with previous students and external risk management professionals to test the validity and value of the subject matter, in line with students and potential and existing employer expectations.

2.3 Providing activities (sometimes called assessment of learning) is a formal method to evaluate learning by comparing learning to a standard or benchmark. This is typically at the end of a unit or period to progress students to next unit:

- Each unit includes an activity that allows students to understand what they have been taught through the lessons.
- The qualification course materials include an introduction and a summary video followed by access to exemplar questions, providing them with knowledge of the examination format and the expectations of the IRM.

3. Guided learning hours and total qualification time

3.1 Guided learning hours (GLH) are where the module coach provides guidance towards the learning aim being studied online. It also includes any forms of assessment hours which are supervised by the module coach or other education or training provider.

- The IRM's Level 4 International Certificate in Operational Risk Management = 10 GLH

3.2 Total Qualification Time (TQT) is a total of independent learning hours + GLH as above.

- The IRM's Level 4 International Certificate in Operational Risk Management = 150 TQT

4. IRM Professional Standards

The IRM professional standards are designed so that they can be used by anyone involved in risk management. They are flexible and can be adapted and used in all types of organisations, sector, and geographical regions.

The IRM Professional Standards has four functional areas broken down into risk functional area components. They are:

- Insights and context:
 - risk management principles and practice
 - organisational environment
 - external operating environment.
- Strategy and performance - developing a risk management strategy to meet organisational needs:
 - risk management strategy and architecture
 - risk management policy and procedures
 - risk culture and appetite
 - risk performance and reporting.
- Risk management process:
 - risk assessment
 - risk treatment.
- Organisational capability:
 - communication and consultation
 - change management
 - people management.

The standards are written as outcomes of competent performance which is the need for relevant knowledge to achieve the standards. For more in-depth information on the Professional Standards of the IRM, please refer to our website <https://www.theirm.org/what-we-do/about-us/professional-standards/>

5. Time Constraints

Once students register and pay, they will have 12 months in which to complete the IRM's Level 4 International Certificate in Operational Risk Management.

6. Collaboration in the Design of the Qualification

- Prof. Dr Thomas Kaiser – Professor Kaiser Risk Management Consulting
- Sam Brindley – Total Processing Group (Insurance)

7. Key Dates

The assessment dates are March, June, September and December every year.

8. Language requirements

The qualification is delivered and assessed in the English language. If English is not the student's first language, IRM recommends they have an Academic IELTS score of 6.0 (with no elements less than 5.5) or equivalent evidence of competence in the English language before beginning their studies.

9. Support for Teaching and Learning

This course is self-directed distance learning so that students have the flexibility of studying at their own pace.

9.1 Virtual Learning Environment (VLE)

The IRM provides learning materials for all units on the VLE, (Moodle). Students also have access to openly available essential and further reference materials. The Module coach also have full access to all learning materials to prepare themselves for supporting students. Access to the next unit is provided to students once a unit is completed.

9.2 Webinars/Videos

Students are given free access to a range of webinars and videos. They also have access to the discussion forums to interact with fellow students, coaches and the IRM student support team.

9.3 Student Handbook

Students have access to a student handbook which contains a range of background, guidance and key information that prepares them for successful study and attaining the qualification. Some sections of the handbook are advisory, helping students to organise and refine their study and examination skills. Some sections contain essential information that students must be aware of and careful to follow.

The essential information is indicated with an asterisk (*) in the contents list, and on the title page of each relevant section. Students should read the handbook in its entirety before they start studying.

9.4 Student Membership

Students who have enrolled in the IRM's Level 4 International Certificate in Operational Risk Management course, automatically become student members of the Institute of Operational Risk IOR, an IRM affiliate. This membership entitles students to several benefits including:

- Access to news and information on the latest developments in the risk profession, in the form of the Enterprise Risk, IRM's quarterly magazine.
- Thought leadership by participating in IRM consultation exercises to assist in supporting, informing, and influencing the regulatory framework in which risk management operates.
- Events and networking to debate and share experiences with peers in the global risk management community.
- Online discussion forum to enable students to network with other students globally and discuss studies in virtual student groups.
- Demonstrating to employer's student's commitment to knowledge progression and supporting the organisation.

The IRM student support team can be contacted by telephone or email to assist with any administrative issues related to studies. Students completing and passing the examination of the IRM's Level 4 International Certificate in Operational Risk Management can use the letters CIOR after their names and automatically become Certificate Members of the Institute of Operational Risk (IOR).

This membership will need to be renewed each year.

10. Qualification Structure

The IRM's Level 4 International Certificate in Operational Risk Management is regulated by Ofqual, England's Office of Qualifications. Qualification number: 610/4673/5

10.1 Qualification Requirements and Rules of Combination

The IRM's Level 4 International Certificate in Operational Risk Management qualification structure has been designed to support students to address their own developmental needs and interests. The Qualification has nine (9) units.

Students need to complete all the units in this qualification as follows:

Unit Number	Unit Title	Approximate Learning Hours
Unit 1	Introducing Operational Risks and Management	15
Unit 2	Operational Risk Controls	15
Unit 3	Operational Risk Management: Monitoring and Reporting	20
Unit 4	Risk Culture	20
Unit 5	Operational Risk Strategy and Appetite	20
Unit 6	Operational Risk Categorisation and Event Data	15
Unit 7	Operational Risk Assessment Methods	15
Unit 8	Operational Risk Monitoring and Reporting	15
Unit 9	Operational Risk Event Management	15

11. Entry Requirements

Although the IRM does not have any specific formal entry requirements, it ensures that students have sufficient capability at the right level to undertake the learning and assessment.

The IRM may consider students prior learning when considering acceptance to IRM qualifications. See the IRM Recognition of Prior Learning Policy.

Please note, the qualification is offered in English therefore a reasonable knowledge of the English language is important. If English is not the student's first language, it is recommended that they have an Academic IELTS score of 6.0 (with no elements less than 5.5) or equivalent evidence of competence in the English language before beginning their studies.

12. Equality and Diversity

The IRM ensures that students are provided with equal opportunities to access all qualifications and assessments, by considering and providing reasonable measures and special consideration for all.

The IRM endeavours to ensure that all processes, structure, content and arrangements for content, coaching, assessment, and awarding of certificates:

- Ensure access and equality of opportunity without affecting the integrity of the qualification.
- Guarantees fair assessment for all students, including those requiring special considerations.
- Complies with the UK Equality and Diversity legislation by ensuring that there is no discrimination on grounds age, disability, gender identity or gender reassignment, marriage or civil partnership, pregnancy or maternity, race or ethnic origin, religion or belief, sex, or sexual orientation.

For further information, please see the IRM's Equality and Diversity Policy and Reasonable Adjustments Policy.

13. Qualification Delivery

The IRM ensures that students have access to a full range of information, advice, and guidance to support them in completing the qualification.

14. Complaints

Complaints can be emailed to the relevant individual directly to resolve the issue swiftly. Please see our complaints policy in the Student Handbook.

If dissatisfied with the response, an appeal can be sent to the Chief Operating Officer (COO) ensuring that name, address, and telephone number, names, and details of the complaint itself are included. Complaints are acknowledged within five working days of receipt and the matter is investigated and action is decided on and taken. A further appeal can be made which is escalated to the Chief Executive Officer (CEO) who acknowledges receipt of the complaint within seven days and arranges an Appeal Review Panel within fourteen days.

15. Overview

The IRM's Level 4 International Certificate in Operational Risk Management, introduces the concepts of risk and operational risk management and how they are effectively managed, monitored and reported. Risk culture of organisations is explored to ascertain whether an organisation has the assurance to face the operational risks that it may face. Risk strategy is examined as to how an organisation manages its operational risks. Risk appetite of different organisations is explored. Finally risk categorisation and data collection is examined and how risks events are managed.

Units		Learning Aims
Unit 1	Introducing Operational Risks and Risk Management	Explore operational risk in different contexts.
Unit 2	Operational Risk Controls	Investigate Operational Risk controls
Unit 3	Operational Risk Management, Monitoring and Reporting	Examine Operational risk management, monitoring and reporting
Unit 4	Risk Culture	Analyse the risk culture of organisations
Unit 5	Operational Risk Strategy and Risk Appetite	Explore risk strategy and appetite.
Unit 6	Operational Risk Categorisation and Event Data	Explore the nature and use of event data and its categorisation.
Unit 7	Operational Risk Assessment Methods	Understand scenario analysis in operational risk management
Unit 8	Operational Risk Monitoring and Reporting	Explore the indicators and reporting of operational risks
Unit 9	Operational Risk Event Management	Explore the indicators and reporting of operational risks



Unit 1 - Introducing Operational Risks and Risk Management

Learning hours: 15

Assessment Guidance: Multiple choice questions

Unit Learning Aim

While studying this unit, students will be able to:

- Explore operational risk management in different contexts.

Unit in Brief

After studying this unit, students will be able to successfully identify the different types of risk that exist in cross-sector, global organisations. They will be able to define the causal factors of operational risk, as well as identify the component parts of an Operational Risk Management Framework.

Introduction to Unit

In this unit, students are introduced to the different types of risk, including operational risk. Operational risk is broken down into its four causal factors: People, Processes, Systems and External Events. Students are then introduced to the operational risk management life cycle.

The unit looks at how risks are identified, assessed, managed, reported and monitored, before delving into each of these stages in more detail.

The Unit also introduces the Risk Management Framework (“RMF”) as a tool to help manage operational risk in line with the strategic objectives of the organisation.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
1.1 Risk Types <ul style="list-style-type: none"> • Risk • Different types of risk 	1. Explore different risk types.	<ul style="list-style-type: none"> • Examine different general risk types.
1.2 Operational Risk <ul style="list-style-type: none"> • Definition • Processes • People • Systems • External events • Basel II regulatory framework definition of operational risk 	2. Investigate the causes of operational risks in a given context.	<ul style="list-style-type: none"> • Distinguish between risk and uncertainty.
1.3 The Bow-Tie Model <ul style="list-style-type: none"> • Cause, event and impact • Near misses • Categories of Operational risk events and their impacts • Emerging operational risks 	3. Understand the relationship between cause, event and impact of the Bow Tie model.	<ul style="list-style-type: none"> • Identify the causes of operational risks in a selected organisation using the Basel II regulatory framework. • Establish how the use of the bow-tie model supports the process of identifying operational risks in organisations.
1.4 Operational Risk Management Life Cycle <ul style="list-style-type: none"> • Stages of the Operational Risk management lifecycle 	4. Examine the operational risk management lifecycle.	<ul style="list-style-type: none"> • Establish the benefits of the operational risk management lifecycle in managing operational risks.
1.5 Operational Risk Perceptions <ul style="list-style-type: none"> • Objective reality • Subjective reality 	5. Investigate the benefits and limitations of different risk perceptions on the risk management of organisations.	<ul style="list-style-type: none"> • Examine the impact of different risk perceptions on a selected organisations' management of operational risks.
1.6 Operational Risk Management Framework <ul style="list-style-type: none"> • Link to strategic objectives • Owner • Regular updating • Components • Roles and responsibilities 	6. Examine the key components of the operational risk management framework.	<ul style="list-style-type: none"> • Examine the advantages of using a risk and control self-assessment (RCSA)



Unit 2 - Operational Risk Controls

Learning hours: 15

Assessment Guidance: Multiple choice questions

Unit Learning Aim

After studying this unit, students will be able to:

- Investigate operational risk controls.

Unit in Brief

After studying this unit, students will be able to:

- Differentiate between inherent and residual risks, and how they are scored in a quantitative way and understand Risk and Control Self-Assessment plans.

Introduction to Unit

In this unit, students are introduced to inherent risks and controls. They will focus on how operational risks can be identified and assessed.

Students will explore the most used techniques to quantitatively assess the overall severity of operational risks. Other methods may be used in different organisations varying by their complexity and risk management maturity, however, the method in this unit is frequently used, especially in organisations that operate in highly regulated sectors.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
2.1 Inherent Risks and Controls <ul style="list-style-type: none"> • Inherent risk • Controls • Inherent risk calculation • Likelihood • Impact 	1. Analyse the impact that inherent risks have on organisations.	<ul style="list-style-type: none"> • Establish the likelihood of an operational risk occurring, from given data. • Calculate an inherent risk score for a selected operational risk.
2.2 Control Scoring <ul style="list-style-type: none"> • Residual risk exposure • Control effectiveness 	2. Investigate the effectiveness of controls used to mitigate operational risks.	<ul style="list-style-type: none"> • Establish the impact that a selected operational risk has on a selected organisation. • Analyse the efficiency of the RCSA process for a selected organisation.
2.3 Residual Scoring <ul style="list-style-type: none"> • Calculations 	3. Examine residual risk exposure of organisations.	<ul style="list-style-type: none"> • Calculate the residual risk exposure of a selected organisation.
2.4 Risk and Control Self-Assessment (“RCSA”) <ul style="list-style-type: none"> • The RCSA cycle • Sources of information for the RCSA 	4. Investigate the risk control and self-assessment process.	<ul style="list-style-type: none"> • Assess the benefits of carrying out a residual risk assessment. • Analyse the efficiency of the RCSA process of a selected organisation.
2.5 Risk and Control Assessment Benefits		<ul style="list-style-type: none"> • Analyse the benefits of carrying out an RCSA for organisations.
2.6 RCSA Approaches <ul style="list-style-type: none"> • Different RCSA approaches 		<ul style="list-style-type: none"> • Appraise the approach/es and tools used by a selected organisation to conduct an RCSA.
2.7 Post-RCSA actions <ul style="list-style-type: none"> • Actions plans 	5. Examine operational risk action plans used by organisations after the risk and control self-assessment is completed.	<ul style="list-style-type: none"> • Analyse the operational risk action plan used by a selected organisation after the risk and control self-assessment has been completed.
2.8 Tools and Software to Support RCSA Performance <ul style="list-style-type: none"> • Tools and software 		



Unit 3 - Operational Risk Management: Monitoring and Reporting

Learning hours: 20

Assessment Guidance: Multiple choice questions

Unit Learning Aim

After studying this unit, students will be able to:

- Examine operational risk monitoring and reporting.

Unit in Brief

This unit covers treatment of operational risks including inherent risks and controls.

Introduction to Unit

Students are introduced to inherent risks and controls. This unit goes into detail on operational risk mitigation (sometimes referred to as 'treatment') by focusing on controls, including the different modes and types of controls that exist, as well as their effect on the materialisation and impact of the operational risks they mitigate.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
3.1 Operational Risk Management methods <ul style="list-style-type: none"> • Treat • Tolerate • Transfer • Terminate 	1. Explore the management of operational risks.	<ul style="list-style-type: none"> • Determine the risk management approach used for a given operational risk. • Determine risk control modes for given operational risks. • Assess the type of risk controls for given operational risks. • Assess key controls used for the mitigation of severe inherent risks. • Appraise the risk control assurance for given operational risks.
3.2 Operational Risk Control Modes <ul style="list-style-type: none"> • Control Modes and the Bow-Tie Model • Control Modes and residual risk exposure 	2. Investigate risk control modes in the mitigation of operational risks.	
3.3 Operational Risk Control Types <ul style="list-style-type: none"> • Physical controls • Procedural controls • Legal controls • Technical controls 	3. Investigate risk control types used to categorise the nature of operational risks.	
3.4 Operational Risk Key Controls <ul style="list-style-type: none"> • Key controls 	4. Investigate key controls in the mitigation of severe inherent risks.	
3.5 Operational Risk Control Assurance <ul style="list-style-type: none"> • Control testing • Control Attestation 	5. Assess the risk control assurance of organisations.	
3.6 Impact Of Ineffective Controls on Operational Risk <ul style="list-style-type: none"> • Control effectiveness • The consequences of ineffective controls • The treatment of ineffective controls 		



Unit 4 - Risk Culture

Learning hours: 30

Assessment Guidance: Multiple choice questions

Unit Learning Aim

After studying this unit, students will be able to:

- Analyse the risk culture of organisations.

Unit in Brief

In this unit students are introduced to how governance influences risk culture of organisations.

Introduction to Unit

All areas of an organisation are exposed to operational risk, no matter how small they are, remote from head office or whether they are client-facing or not. Governance thus must include all parts of an organisation, not just a small part of it as in the case of financial risks.

Operational risk is about people, both as potential sources of events as well as crucial factors in its prevention and mitigation, thus it is important to consider the behaviour of people and their culture. Hence, in addition to getting the formal structure of roles and responsibilities in place, it is of paramount importance to establish an adequate risk culture, as it determines the “way people behave when nobody is watching.”

In this unit, students are introduced to who is responsible for risk in organisations by exploring the Three Lines Model.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
4.1 Three Lines Model <ul style="list-style-type: none"> • The governance framework for managing operational risks • Background on the three lines model • Third line – risk assurance 	1. Establish what constitutes a real control in managing risks.	<ul style="list-style-type: none"> • Determine the use of the three lines model of a risk governance framework in a given context. • Distinguish between operational risks as a discipline and as a function • Appraise the role of governing body committees in managing operation risk in a given context. • Assess the importance of policies and other documentation in operational risk management. • Appraise the risk culture of an organisation in optimising risk management. • Justify the use of different risk culture and assessment methods for effective risk management. • Make recommendations to improve the risk culture of an organisation.
4.2 Committee Roles <ul style="list-style-type: none"> • Committees of the governing body 	2. Investigate the role of governing body committees in managing operational risks.	
4.3 Policies, Procedures and Other Documentation <ul style="list-style-type: none"> • The ‘use test’ • Continuous review and change 	3. Examine the significance of policies, procedures and other documentation in operational risk management.	
4.4 The Elements of a Good Risk Culture <ul style="list-style-type: none"> • Organisational culture • Risk culture 	4. Examine the elements of a good risk culture.	
4.5 Assessing and Monitoring Risk Culture <ul style="list-style-type: none"> • Surveys • Interviews • Metrics 	5. Investigate risk culture assessment and monitoring methods.	
4.6 Improving Risk Culture	6. Examines ways of improving risk culture.	



Unit 5 - Operational Risk Strategy and Risk Appetite

Learning hours: 20

Assessment Guidance: Multiple choice questions

Unit Learning Aim

After studying this unit, students will be able to:

- Explore risk strategy and risk appetite.

Unit in Brief

Students will:

- Investigate the links between risk and business strategies by exploring risk appetite and its expressions and how it is monitored and reported.

Introduction to Unit

In this unit students will consider the links between risk strategy and business strategy. Risk appetite and expressions of this are investigated both quantitatively and qualitatively. Finally, how risk appetite is monitored and reported is explored.

Organisations cannot function without taking a degree of operational risk. They must take risks to achieve their strategic objectives when exploiting opportunities to earn a profit. Operational risks are often considered 'the cost of doing business' for examples pricing of products and services at least indirectly are considered a risk type, while any changes in the organisations such as and not limited to new products, new markets, restructuring, Informational Technology systems changes, might lead to an increase or decrease in costs and will influence the operational risk profile in a negative way.

This unit covers questions such as how much operational risk should be accepted, on what basis is this decision made and risk tolerance limits.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
5.1 Interrelationship between Risk and Business Strategies <ul style="list-style-type: none"> • Principle one • Principle two • Principle three • Principle four 	1. Analyse the links between organisational strategy and risk appetite.	<ul style="list-style-type: none"> • Establish the connection between the operational risk framework and the business strategies of an organisation.
5.2 Risk Appetite and Tolerances <ul style="list-style-type: none"> • Definitions • Risk appetite framework • Operational risk appetite vs operational risk tolerance and capacity 	2. Investigate operational risk appetite, risk tolerance and capacity.	<ul style="list-style-type: none"> • Distinguish between the concepts of operational risk appetite, tolerance, and capacity.
5.3 Operational Risk Appetite Framework <ul style="list-style-type: none"> • The purpose of an operational risk appetite statement • Operational risk appetite statement • Content of an operational risk appetite statement 	3. Analyse operational risk appetite statements qualitatively and quantitatively.	<ul style="list-style-type: none"> • Interpret an operational risk appetite and tolerance of selected operational risks in an organisation.
5.4 Qualitative and Quantitative Expressions of Operational Risk Appetite <ul style="list-style-type: none"> • Qualitative expressions of operational risk appetite • Quantitative expressions of operational risk appetite 		<ul style="list-style-type: none"> • Determine the sources of information for qualitative and quantitative expressions of risk appetite of an organisation.
5.5 Setting Operational Risk Appetite <ul style="list-style-type: none"> • Risk and control indicators including limits and thresholds. • VAR models for operational risk capital • Setting operational risk appetite 	4. Examine the process of setting operational risk appetite.	<ul style="list-style-type: none"> • Assess the effectiveness of operational risk appetite setting for an organisation,
5.6 Monitoring and Reporting Risk Appetite <ul style="list-style-type: none"> • Monitoring and reporting operational risk. • Integrating operational risk appetite within the operational risk monitoring and reporting process • Aggregation to top level operational risk appetite reporting • Monitoring operational risk and decision making • Roles and responsibilities for operational risk appetite 	5. Examine the process of monitoring and reporting risk appetite.	<ul style="list-style-type: none"> • Assess the effectiveness of the monitoring and reporting of the risk appetite of an organisation.



Unit 6 - Operational Risk Categorisation and Event Data

Learning hours: 15

Assessment Guidance: Multiple choice questions

Unit Learning Aim

After studying this unit, students will be able to:

- Explore the nature and use of event data and its categorisation.

Unit in Brief

The unit introduces the data categorisation of operational risks and how these are used.

Introduction to Unit

The creation of a single, consistent data categorisation approach or taxonomy and structure for use across an organisation should be one of the first activities to be undertaken by any operational risk management function.

It is important in that it provides a common language for the rest of the operational risk framework, including policy development, programmes for risk identification and quantification, scenario assessment, risk or loss event management or the deployment of risk, control and performance metrics.

Students will be introduced to taxonomies in operational risk categorisation and how these are used to categorise data. They will explore controls, processes and tools used in data categorisation and the event data collection process. Finally, they will investigate loss data usage.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
<p>6.1 Taxonomies for Operational Risk Categorisation</p> <ul style="list-style-type: none"> • Taxonomy definition • Industry practice • Benefits of a data categorisation scheme • Features of a good data categorisation scheme 	<p>1. Examine the use of taxonomies in risk categorisation.</p>	<ul style="list-style-type: none"> • Define taxonomy. • Assess the effectiveness of an organisation's risk categorisation scheme. • Assess the importance of the risk level hierarchy to capture various risk types.
<p>6.2 Risk Categorisation for Operational Risk Management</p> <ul style="list-style-type: none"> • Boundaries, attributes and levels • Elements commonly found in an operational risk categorisation scheme • Approach to creating categorisation structures: Bow-tie model 	<p>2. Investigate risk categorisation models used in operational risk management.</p>	<ul style="list-style-type: none"> • Assess the effectiveness of the bow-tie model as a risk categorisation scheme. • Assess the effectiveness of event data used by an organisation in its operational risk management.
<p>6.3 Controls, Processes and Tools used in Data Categorisation</p> <ul style="list-style-type: none"> • Risk and control self-assessment (RCSA) • Risk and control indicators • Risk events • Scenario analysis • Operational risk quantification • Other applications 	<p>3. Analyse the effectiveness of controls processes and tools used in data categorisation for operational risks.</p>	<ul style="list-style-type: none"> • Determine how the use of the event data collection process supports its operational risk management in a selected organisation.
<p>6.4 Characteristics of Event Data</p> <ul style="list-style-type: none"> • Introduction to internal event data • Direct and indirect events • Financial and non-financial impacts • Near misses • Gains and offsets • Boundary risk events • Event description and type • Amount of loss • Date of event occurrence • Recoveries • Business entity of event • Business activity of event • Geographic location of event • Event description 	<p>4. Examine the characteristics and effectiveness of the application of internal and external event data.</p>	<ul style="list-style-type: none"> • Analyse the applications of external loss data in the operational risk management of an organisation.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
<p>6.5 Features of the Event Data Collection Process</p> <ul style="list-style-type: none"> • Aims of reporting event data • Roles and responsibilities for reporting of event data • Event data and risk and control self-assessments (RCSAs) • Event data and scenarios • Risk and control indicators • Risk modelling • Accounting treatment • Risk appetite • Other uses • Limitations 	<p>5. Analyse the use of event data collection processes.</p>	
<p>6.6 External Loss Data Usage</p> <ul style="list-style-type: none"> • Media reports, social media and public data • Competitors internal losses and consortia databases 	<p>6. Examine applications of external loss data in operational risk management.</p>	



Unit 7 - Operational Risk Assessment Methods

Learning hours: 15

Assessment Guidance: Multiple choice questions

Unit Learning Aim

After studying this unit, students will be able to:

- Explore scenario analysis in operational risk management.

Unit in Brief

This unit considers the use of scenario analysis in operational risk management in analysing future events. It explores the use of models and stress testing.

Introduction to Unit

In this unit, students are introduced to is scenario analysis which is a description of an event, an inventory of relevant risks and controls, relevant internal and external loss data, risk indicators that may describe or predict a scenario event and the use of the scenario for risk capital calculation purposes.

Internal and external loss data is a key input into this modelling as well as stress and reverse stress testing which are used to supplement loss data. These outputs can provide valuable information on the 'tail' of the probability and impact distributions they construct. Risk models are only effective if they represent the full range of outcomes for a given risk.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
7.1 Scenario Analysis Methodology <ul style="list-style-type: none"> • Scenario definition • Objectives of a scenario analysis • Types of scenarios • Number of scenarios 	1. Explore scenario analysis as an assessment methodology of operational risk management.	<ul style="list-style-type: none"> • Determine the scenario analysis process used by a selected organisation for managing potential operational risks.
7.2 Scenario Analysis Process <ul style="list-style-type: none"> • Introduction to the scenario analysis process • Purpose of scenario analysis • Participants in scenario analysis • Influence of the business environment on scenario analysis • Factors influencing a scenario analysis approach • Scenario analysis approaches • Scenario analysis challenges 	2. Examine the scenario analysis process.	<ul style="list-style-type: none"> • Differentiate between the classes of bias that could arise in scenario analysis. • Identify the key parts of the validation process of scenario analysis. • Assess the effectiveness of using different quantitative operational risk models in various contexts.
7.3 Biases in Scenario Analysis <ul style="list-style-type: none"> • Bias and gaming • Validation 	3. Examine the biases that could arise in the scenario analysis process.	<ul style="list-style-type: none"> • Assess the benefits of stress testing in operational risk management.
7.4 Quantitative Risk Modelling <ul style="list-style-type: none"> • Contextual operational risk models • Log-normal distribution of severity • Expected and unexpected losses • Value at Risk (VAR) approaches 	4. Investigate the use of quantitative modeling in operational risk management.	<ul style="list-style-type: none"> • Assess the purpose and benefits of reverse stress testing in operational risk management.
7.5 Stress Testing Approaches <ul style="list-style-type: none"> • Stress testing • Reverse stress testing 	5. Investigate the use of stress testing in establishing the hypothetical severity of operational risk exposures.	



Unit 8 - Operational Risk Monitoring and Reporting

Learning hours: 15

Assessment Guidance: Multiple choice questions

Unit Learning Aim

After studying this unit, students will be able to:

- Explore the indicators and reporting of operational risks.

Unit in Brief

This unit introduces risk, control and performance indicators and distinguishes between lagging and leading indicators.

Introduction to Unit

In this unit, students are introduced risk, control and performance indicators and the differences between lagging and leading indicators. It covers the different triggers that are set for each indicator, how these are determined and responses that any breaches of these triggers would generate.

Finally, students will examine the expectations of internal and external stakeholders in operational risk reporting.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
<p>8.1 Risk Indicators</p> <ul style="list-style-type: none"> • Introduction to risk indicators • Approaches to designing risk indicators • Value of risk indicators • Changing risk indicators • Risk indicator triggers • Defining targets, limits and thresholds • Lagging and leading indicators 	<p>1. Examine the risk indicators of operational risks.</p>	<ul style="list-style-type: none"> • Assess the triggers and effectiveness of given risk indicators. • Justify the need for monitoring the control indicators in a given context. • Analyse the links between performance indicators and operational risks in a given context.
<p>8.2 Control Indicators</p> <ul style="list-style-type: none"> • Similarities between control and risk indicators • Control indicators 	<p>2. Examine the risk control indicators of operational risks.</p>	<ul style="list-style-type: none"> • Assess the effectiveness of the risk reporting of a given organisation.
<p>8.3 Performance Indicators</p> <ul style="list-style-type: none"> • Performance indicators • Key features of performance indicators • Linkage between performance indicators and operational risk 	<p>3. Examine the performance indicators of operational risks.</p>	
<p>8.4 Risk Reporting</p> <ul style="list-style-type: none"> • Reporting and governance • Challenges around reporting • Presentation of reports 	<p>4. Investigate the operational risk reporting processes of organisations.</p>	



Unit 9 - Operational Risk Event Management

Learning hours: 15

Assessment Guidance: Multiple choice questions

Unit Learning Aim

After studying this unit, students will be able to:

- Appraise operational risk event management practices.

Unit in Brief

This unit considers operational risk event management in practice and how this leads to business continuity.

Introduction to Unit

In this unit, students are introduced to how incidents are identified and managed to maintain business continuity to ensure organisational resilience. They will also explore 'Black Swan events' which are events that have catastrophic consequences and one which was or is unknowable. A recent example of this is the Covid-19 pandemic.

Much like the management of operational risks, the operation risk event management follows similar processes.

Finally, students are briefly introduced to environmental, social and governance risks and their impact on the organisation.

Indicative Learning	Unit Learning Outcomes The student will:	Assessment Criteria
9.1 Operational Risk Event Management <ul style="list-style-type: none"> • Incident management lifecycle • Identifying an incident • Triaging an incident • Resolving an incident • Recovering from an incident • Remediating an incident • Reporting on an incident • Reviewing an incident 	1. Examine the incident management lifecycle.	<ul style="list-style-type: none"> • Recommend approaches to an organisation for managing a selected incident. • Assess the effectiveness of a post-incident practice for a selected organisation.
9.2 Post-incident Best Practice <ul style="list-style-type: none"> • Post-incident reviews • Root case analysis • The relationship between incidents, operational risks and controls 	2. Examine post-incident best practice.	<ul style="list-style-type: none"> • Analyse the relationship between incidents, operational risks and controls.
9.3 Business Continuity <ul style="list-style-type: none"> • Business continuity • Business continuity lifecycle 	3. Investigate business continuity to improve organisational resilience.	<ul style="list-style-type: none"> • Assess the effectiveness of the approach a selected organisation takes to improve its resilience.
9.4 Black Swan Events <ul style="list-style-type: none"> • Covid-19 Black Swan event example 	4. Examine Black Swan Events.	<ul style="list-style-type: none"> • Analyse the impact that a black swan event has had on a selected organisation.
9.5 Environmental, Social, Governance (ESG) Risks	5. Investigate the effectiveness of Environmental, Social and Governance risks (ESG) reviews on risk mitigation.	<ul style="list-style-type: none"> • Assess the effectiveness of ESG reviews to mitigate operational risks for a selected organisation.

16. Assessment

Formative assessments are available to students at the end of each unit to encourage learning. It provides generic feedback to students on their level of attainment. Students are encouraged to engage with the formative self-assessments in the Moodle lessons and use these tools to determine their level of attainment to move on to the next unit.

Formative assessments are where students can engage in self-assessment and feedback to assess the progression of learning and understanding.

The IRM's Level 4 International Certificate in Operational Risk Management summative assessment or assessment of learning is conducted through an online third party's software, Pearson VUE using multiple choice questions (MCQs) which are selected from a bank of questions at various degrees of difficulty. Questions may be standalone or used in conjunction with case study scenarios.

IRM assessments are designed to ensure that learning outcomes of the qualification is achieved. Students and examiners/assessors have a clear understanding of these criteria, which are published in the lessons on the VLE/Moodle.

Assessments are designed to promote effective learning. They provide opportunities for all intended learning outcomes that have been defined for the qualification and syllabus, to be assessed. The range and types of assessment measure students' achievement of qualification learning outcomes. Questions are designed to assess one or more learning outcomes of qualification. There is a clear development of, and information about, progression through the qualifications, in terms of both attainment and demonstration of skills and attributes.

16.1 Principles of External Summative Assessments

16.1.1 Validity of IRM summative assessments is assured by ensuring that the content, skills, applications, and qualities which are defined throughout the qualification, are evident in the assessment using appropriate assessment methodologies.

16.1.2 Reliability of IRM assessments is achieved by ensuring that assessments can be used with the same results over a specified period for all students in different geographies. Comparability of IRM assessments is understood by users in terms of benchmarks and historic standards as applied to the assessment, with assessment outcomes that are comparable to the standards of the qualification and the assessment itself and between similar qualifications and assessments of other awarding bodies every two years. The IRM also amends qualifications when new knowledge in the risk management field is necessitated, for the qualifications to stay current and fit for purpose.

16.1.3 Relevance of IRM assessments is achieved by evaluating both knowledge and skills of students/candidates in the field of risk management. The design of assessments reflects the skills that students are required to develop, as well as measuring the students' understanding of the learning aims and outcomes.

16.1.4 The IRM endeavours to provide sufficient balance between learning and assessment. Minimising bias of IRM assessments which is achieved by:

- Ensuring that all students have access to assessments which are highlighted in, The IRM Equality and Diversity Policy, which is considered when designing the assessment.
- Ensuring that the design of assessments reflects the needs of a wide range of students, recognising and respecting equality and diversity so that individuals or groups are not disadvantaged.

16.2 Security of summative assessments

The summative MCQ assessments are conducted on-line either at the third parties' examinations centres (currently Pearson VUE test centres) or on-line, using Pearson VUE's remote proctoring services in both cases, security is in place to prevent malpractice including Pearson VUE Candidate Rules Agreement, Securing Exams against Test Fraud and Pearson Professional Examination Rules, to prevent:

- Impersonation of students – ID and passwords are required.
- Use of mobile phones.
- Use of notes (in any format).
- Use of the internet (especially with remote proctoring).
- Use of visual aids or multiple screens in the case of remote proctoring.

During the assessment students cannot print screen or take photographs. This is to prevent 'sharing' of assessments and maintain the integrity of the assessments.

16.3 Structure of summative assessments

MCQ summative assessment for the IRM's Level 4 International Certificate in Operational Risk Management is constructed from questions in a question bank. The question bank includes questions on all areas of the syllabus hence ensuring that the learning outcomes can be assessed.

The IRM uses several question types, in designing the MCQ questions, from simple MCQs to case-study based questions. Questions may be standalone or used in conjunction with case study scenarios.

16.4 Valid assessment decisions

MCQ assessments are marked on-line by the third-party's software. A meeting is held where a statistician from the third-party provider as well as the Principal and Chief examiners and members of the examination and qualification development staff review each item performance and set the pass marks for the assessment.

16.5 Issuing Results and Certificates

The IRM aims to issue results within six weeks after the last examination sitting. The results are issued via email to students. All certificates are sent by post to students within three weeks of the notification of results.

16.6 Withholding results or certificates

Results or certificates may be withheld due to allegations of malpractice either by a student or a centre until a resolution is found but will not withhold results of certificates because of student financial difficulties.

16.7 Resits

If a student fails the MCQ examination, they can re-sit at the next available session. Students are permitted a maximum of two attempts (which includes the resit).

Re-sit application forms must be submitted with the appropriate fees by the stated deadline.

Appendix 1 Verbs used in aims and learning outcomes

Term	Definition
Analyse	Critically examine methodically breaking it down, to explain and interpret it.
Appraise	Assess the value or quality of something.
Assess	Make an informed judgement about the value, strengths, or weaknesses of an argument, claim or topic by weighing all the views on it.
Compare	Identify similarities between two or more subjects of discussion.
Critique	Provide an opinion or verdict on whether an argument or set of research findings is accurate.
Determine	Ascertain or establish the facts.
Distinguish	Identify similarities between two or more subjects of discussion.
Establish	Determining the facts.
Evaluate	Provide one's own opinion concerning the extent to which an argument or set of research findings is accurate.
Examine	Establish the key facts and important issues of a topic or argument by looking at them in close detail to analyse them.
Explain	Clarify a topic by providing as much detail as possible and giving definitions for any key terms used, showing clear understanding in a logical coherent response.
Justify	Explain the basis of an argument by presenting evidence that informed the view explaining why other arguments are unsatisfactory.
Link	Find a mutual relationship or connection in which one thing affects or depends on the other.
Monitor	To keep track of or check for a special purpose.
Recommend	Put forward something/an idea as suitable for a particular purpose or role.

Appendix 2 Glossary of terms used

Abbreviation	Meaning
Cert	Certificate
COO	Chief Operating Officer
CEO	Chief Executive Officer
CIOR	Certified Institute of Operational Risk
ESG	Environmental, Social and Governance
GLH	Guided Learning Hours
IOR	Institute for Operational Risk
IRM	Institute of Risk Management
IRMCert	Institute of Risk Management Certificate
MCQ	Multiple Choice Questions
OFQUAL	Office of Qualifications and Examinations Regulation
RCSA	Risk and Control Self-assessment
RMF	Risk Management Framework
TQT	Total Qualification Time
VAR	Value At Risk
VLE	Virtual Learning Environment (Moodle)