Institute of Risk Management

Digital Risk Management Certificate

Overview and syllabus

Developed with

WARWICK
THE UNIVERSITY OF WARWICK

irm
Developing risk professionals

Overview of the Digital Risk Management Certificate

Qualification aims

This qualification introduces the concepts of digital risk management and will equip risk practitioners with the ability to apply their skills in an increasingly fast-paced and changing digital world. It explains how new technologies and digitalisation are disrupting businesses, changing the risk environment for organisations of all types and posing new ethical challenges. It looks at how appropriate risk management tools and techniques can be applied, adapted and developed in this digital context. The qualification also provides a detailed introduction to cyber security principles and practices.

Qualification learning outcomes

By the end of the qualification, you should be able to:

- Demonstrate a broad understanding of today's most important digital technological developments
- Explain how digital technology and innovation is impacting organisations and society
- Contribute knowledgeably to identifying, assessing and controlling digital risks throughout your organisation and its wider supply chain, associated with new technologies and new ways of working
- Help your organisation apply concepts such as risk appetite, ethics and legal frameworks in the context of digital and technological innovation
- Describe the key cyber threats and the basic disciplines of cyber security
- Explain the key elements of practical cyber risk response, including the role of risk management systems, compliance and cyber defence frameworks
- Discuss governance, incident management and reporting, and apply the principles of audit and assurance to digital risks

Unit 1: The Digital Revolution

Learning outcomes

After studying this unit, you should be able to:

- Demonstrate a broad understanding of today's most important digital technological developments

Unit contents	Section learning outcomes
1.1 Digital risk, digital technology and the "4th industrial revolution"	Discuss how the world of digital technology has and is changing, including identifying the characteristics of a technical turning point Discuss the concept of the 4th industrial revolution
1.2 Increased digitisation: • Physical technology • Digital technology	Discuss a range of different digital technologies and explain how they are evolving to equal or to better the corresponding human abilities
1.3 Moore's Law	Explore exponential growth in relation to Moore's Law and its impact on innovation
1.4 Digitalisation, reproducibility and free content	Explain the concepts of non-rival goods and very cheap reproducibility to digital data and apply these ideas to a commercial case study
1.5 FinTech, RegTech and Blockchain	Understand the rapid development of FinTech and RegTech and the principal impacts these can have on an organisation Explain the concepts of Blockchain and Bitcoin

Unit 2: Digital Disruption, Ethics and Risk Management

Learning outcomes

After studying this unit, you should be able to:

- Explain how digital technology and innovation is impacting organisations and society
- Analyse the risks and opportunities associated with digital technology and innovation
- Discuss the ethical and legal frameworks within which digital technology must fit
- Discuss risk management principles and practices in relation to digital risk

Unit contents	Section learning outcomes
2.1 Digital disruption, organisational and societal change	Explain what is meant by digital disruption Discuss a range of organisational and societal changes in communication strategies
2.2 Digital disruption: Artificial intelligence	Analyse how digital disruption is affecting organisations both positively and negatively at all levels Discuss some recent digital innovations, including some involving artificial intelligence
2.3 Productivity gains from digital innovation	Discuss how digital disruption is affecting productivity, including the relationship between general purpose technology, economic growth and productivity
2.4 Ethics of digital innovation and globally-relevant European regulations	Discuss some negative effects of digital disruption and analyse the ethical issues involved in digital technology Explain the legal issues and demands involved in digital technology by reference to the European GDPR
2.5 Risk and general risk management principles and practices	Understand the main types of risk that an organisation might face from both an internal and external context Explain the use of standards such as ISO 31000 in organisations Discuss risk management principles, the risk framework and the risk process Explain risk appetite, risk tolerance and the main types of controls Understand resilience in outline

Unit 3: Digitisation Risk and Cyber Security Risk

Learning outcomes

After studying this unit, you should be able to:

- Identify some elementary business models associated with digitisation
- Describe the key cyber threats and basic disciplines of cyber security

Unit contents	Section learning outcomes
3.1 Two kinds of digital risk	Explain the difference between digitisation risks and cyber security risks Describe some risks associated with 5 models for digitising a business from scratch or adapting offline business to online transactions
3.2 Cyber threats	Describe key cyber security threats arising from internet-assisted financial and social opportunities afforded by connectivity Explain key cyber security concepts including vulnerability and defence in depth
3.3 Cyber risks from outsourced connections	Explain how cyber security weaknesses can result from outsourced connections Describe key cyber security risks including hacking, cyber attacks and malware Explain the significance of crucial case studies of data breaches
3.4 Cyber security	Analyse the classification of cyber security functions and apply these to organisations Describe the roles within these functions

Unit 4: Digital Risk Management Approaches and Security

Learning outcomes

After studying this unit, you should be able to:

- Explain the key elements of a practical, risk based cyber security framework
- Discuss ways of controlling risks and defence in depth
- Explain how security by design can identify, classify and protect valuable assets

Unit contents	Section learning outcomes
4.1 Protecting information assets	Describe how to identify and classify information assets Explain how to develop controls to reduce risk
4.2 Cyber defence points and controls	Identify appropriate cyber defence points to apply controls Select the type of control and integrate with others that are active
4.3 Defence in depth	Explain how sets of controls help develop defence in depth Analyse multiple combined attacks such as Advanced Persistent Threat (APT)
4.4 Human factors	Explain how human factors can compromise physical and cyber security Describe actions that can reduce the risk arising from human factors
4.5 Applying technical controls	Describe the life cycle of a typical complex attack Compare the effectiveness of various alternative technical controls and high-level tests

Unit 5: Attacks, Defence and Risk-Based Digital Risk Management

Learning outcomes

After studying this unit, you should be able to:

- Understand the key elements of practical cyber risk response, including the role of risk management systems, compliance and cyber defence frameworks

Unit contents	Section learning outcomes
5.1 Attack and defence	Describe the evolving nature of attack and defence
5.2 Defence methods and frameworks	Consider evolving defence methods Be able to operate and describe a 14-point framework for defence
5.3 Threat actors	Examine the motivations and capabilities of the threat actors fighting the cyber security cold war
5.4 Digital risk management	Discuss how a risk management system can help manage multiple digital risks Carry out a digital risk assessment Apply a six-step approach to digital risk management for an organisation

Unit 6: Risk-Based Cyber Security, Change Management Exposure and Response

Learning outcomes

After studying this unit, you should be able to:

- Discuss governance, incident management and reporting
- Apply the principles of audit and assurance to digital risks

Unit contents	Section learning outcomes
6.1 Governance, business objectives and digital risk	Discuss governance and digital risk Explain how the techniques discussed in this module integrate and align with business objectives
6.2 Change management	Discuss the requirements needed to manage changes effectively to protect organisational objectives
6.3 Best practice approaches	Operate a simple diagnostic audit on cyber security and describe some best practice approaches
6.4 Incident management and reporting	Describe the approach to incident management and reporting Discuss audit and assurance for digital risks
6.5 Future trends and emerging risks	Discuss possible future digital trends and risks Comment on the potential impact on digital and cyber security