Title	Cyber Incident Response
Long Title	Cyber Incident Response
Credits	**5**
NFQ Level	**8**
Module Author	**Gillian O’Carroll**

Module Description:

In this module, students will evaluate the importance of business continuity planning and incident response management in the context of an organisation’s cybersecurity risk environment. Students will analyse the critical components of effective incident response management, including appropriate advance planning, procedures and policy making. Students will learn to benchmark incident response management techniques to ISO 27035 – Information Security Incident Management and NIST guidelines. The module includes evaluation of the Cyber Incident Team skillset composition, analysis of incident response outcomes and how to conduct effective Lessons Learned post incident.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1	Examine the fundamentals of business continuity and incident response management within the context of an organisation's cybersecurity risk environment, ensuring the essential components such as policies, plans and procedures meet internationally recognised standards.
LO2	Assess the incident response lifecycle and analyse the critical steps to ensure successful management of cybersecurity incidents, including incident documentation and communications.
LO3	Examine the importance of establishing a suitable Incident Response Team, identifying the diverse skillsets and competencies required, including outsourced partnerships where appropriate.
LO4	Evaluate and test an organisation's incident response procedures using appropriate Incident Response Metrics.
LO5	Conduct a Cyber Incident Lessons Learned exercise, identifying improvements to incident response plans and procedures, ensuring continuous learning for future incidents.

Indicative Content

Business Continuity

Understanding the context of an organisation’s risk environment when conducting business continuity planning. Analysing the differences between business continuity, disaster recovery, incident management and operational resilience. Identifying relevant international standards, including NIST Special Publication 800-61 Rev 2 and ISO 27035 Parts 1 to 3: Information Security Incident Management. Considering the role of executive leadership and internal & external stakeholders as part of the incident response planning process.

Components of a Business Continuity Plan

Reviewing the key techniques underpinning business continuity planning, including risk assessments and business impact analyses. Analysing the development of strategies and solutions, such as reducing third party dependencies, to address business continuity risks. Assessing the importance of staff validation as part of the business continuity planning process.

Cyber Incident Response Governance

Evaluating the objectives of Incident Response Management and considering the Incident Response Lifecycle as a tool to underpin the incident response process. Examining Incident Response Policies, Plans and Procedures and identifying the unique role each plays in the incident response process. Investigating the prioritisation of incidents and how to appropriately tailor the organisation’s response.

Preparing for a Cyber Incident & the Incident Response Team

Identification of prevalent cyber vulnerabilities & threats and appraising the prevention tools that can be employed to minimise the occurrence of cyber incidents. Assessing an organisation’s incident detection and monitoring tools and examining common signs of a cyber incident. Evaluating the skillset required for Incident Response Team members, including Team Model options and the scope of the Incident Response Team’s responsibilities. Examination of the value of including Outsourced Partnerships to the Incident Response Team.

Cyber Incident Response

Examination of the initial incident response, including incident validation and categorisation. Analysing key technical elements of incident response – containment, eradication, recovery. Appreciation of the importance of incident communications and stakeholder involvement. Identifying critical incident documentation and evidence gathering techniques.

Learning, Testing & Evolving

Conducting a Tabletop Exercise to evaluate the robustness of an Incident Response Plan. Assessing how post-Incident ‘Lessons Learned’ reviews can improve future incident response and the organisation’s overall operational resilience. Identifying relevant Incident Response Metrics to measure the organisation’s incident management performance. Analysing the contribution of Incident Response Outsourcer partnerships and understanding their value. Relating the Business Continuity and Incident Response processes to evolving regulatory standards, including the Digital Operational Resilience Act (DORA).

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Written Report	The Learner will produce a written report to a professional standard analysing the contribution of business continuity and incident management processes in minimising cybersecurity risk.	1, 2, 3	40	Week 6
Project	This is a group project where the learners will work in groups to select a Use-Case/Real Organisation and document a case study assessing the adequacy of the incident response and business continuity measures in place at the Use-Case Organisation.	2, 3, 4, 5	60	Sem End

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework Only

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture underpinning the learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support content delivered.	1.0	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	4.0	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture underpinning the learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support content delivered.	1.0	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	4.0	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Recommended Book Resources

Dr. Erdal Ozkaya. (2021), Incident Response in the Age of Cloud: Techniques and Best Practices to Effectively Respond to Cybersecurity Incidents, Packt Publishing, [ISBN: 10:1800569211].

Supplementary Book Resources

Christopher J Hodson. (2019), Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls, 1st Ed. Kogan Page.

Supplementary Article/Paper Resources

Staves et al. (2022), A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems, International Journal of Critical Infrastructure Protection, July 2022.
Ahmad et al. (2020), How Integration of Cyber Security Management and Incident Response Enables Organizational Learning, Journal of the Association for Information Science & Technology, August 2020.
ENISA. (2010), Good Practice Guide for Incident Management, ENISA European Union Agency for Cybersecurity, December 2010, https://www.enisa.europa.eu/publications /good-practice-guide-for-incident-management

Other Resources

Website, NIST Cybersecurity Framework V1.1,
https://www.nist.gov/cyberframework
ISO, ISO/IEC 22301: 2019 Security and resilience – Business continuity management systems.
ISO, ISO/IEC 27035-1:2023 Information Security Incident Management Part 1: Principles and process.
ISO, ISO/IEC 27035-2:2023 Information Security Incident Management Part 2: Guidelines to plan and prepare for incident response.
ISO, ISO/IEC 27035-3:2020 Information Security Incident Management Part 3: Guidelines for ICT response operations.