

Module Title:	Incident Handling and Risk Analysis
Language of Instruction:	English
Credits:	10
NFQ Level:	6
Module Delivered In	No Programmes
Teaching & Learning Strategies:	This module focuses on the procedural and management side of incident handling and risk analysis. Content will be delivered to learners through lectures with class interaction, supported by practical group sessions. Practical sessions will incorporate workshop style classes for case studies, role based scenarios and evaluation of model policies/frameworks. Collaboration and peer/independent learning embedded into practical sessions, supported by reflection and critiquing of practical session outcomes.
Module Aim:	To develop learners' knowledge of information security incident handling and perform risk analysis on information systems.
Learning Outcomes	
<i>On successful completion of this module the learner should be able to:</i>	
LO1	Identify and document information security events.
LO2	Plan an appropriate incident handling policy.
LO3	Mitigate risk by evaluating risk management strategies.
LO4	Design a contingency plan which incorporates disaster recovery.
Pre-requisite learning	
Module Recommendations <i>This is prior learning (or a practical skill) that is recommended before enrolment in this module.</i>	
No recommendations listed	
Incompatible Modules <i>These are modules which have learning outcomes that are too similar to the learning outcomes of this module.</i>	
No incompatible modules listed	
Co-requisite Modules	
No Co-requisite modules listed	
Requirements <i>This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.</i>	
No requirements listed	

Module Content & Assessment

Indicative Content

Information Security Overview

Modern security threats, information security, data classification and incident handling. What is an information security event and the management of information security events.

Vulnerability, Threats and Attacks

Conducting vulnerability assessment, creating a security baseline. Security models, CIA model (Confidentiality, Integrity, Authentication), types of attacks and countermeasures.

Types of Computer Security Incident

Physical security, malicious code, network scanning/penetration, host compromise, database and web vulnerabilities, denial of service and data compromise/theft.

Incident Response

Intrusion detection and prevention systems, security policies and procedures, social engineering threats. Incident handling strategies (Proactive/Reactive) and forensic principles and policy.

Concepts of Risk Analysis

Security planning, risk management and contingency planning/disaster recovery. Policies, procedures, auditing and monitoring.

Security Planning

Risk assessment, risk mitigation - deploy controls and minimize exposure. Education - raise threat awareness and publicize event reports, procedures and reviews.

Risk Management

Physical Security Measures, Personnel Security Practices and Procedures. Administrative Security Procedural Controls. Risk assessment methodologies, strategies and cost/benefit analysis.

Contingency Planning/Disaster Recovery

Disaster classification, disaster recovery plan (detection, response and recovery). Crisis management, impact analysis, communication and follow up.

The Insider Threat

Threats from individuals. Malicious threats from disgruntled employees, former employees, contractors or business associates with insider knowledge. Non-malicious from uninformed staff.

Relevant Security Policies, Frameworks and Publications

Examples - NIST Computer Security Incident Handling Guide and CERT Computer Security Incident Response Team Publications.

Assessment Breakdown	%
Continuous Assessment	40.00%
End of Module Formal Examination	60.00%

Continuous Assessment

Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Short Answer Questions	In class, scenario based assessment.	1,2	20.00	n/a
Written Report	Generate a policy/framework document which will ensure business continuity for an organisation.	3,4	20.00	n/a

No Project

No Practical

End of Module Formal Examination

Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Formal Exam	Terminal Examination	1,2,3,4	60.00	End-of-Semester

SETU Carlow Campus reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time		
<i>Workload Type</i>	<i>Frequency</i>	<i>Average Weekly Learner Workload</i>
Lecture	30 Weeks per Stage	3.00
Estimated Learner Hours	30 Weeks per Stage	3.67
Total Hours		200.00

