SAFE: Project Incident Handling and Risk Analysis

Module Title:	Project Incident Handling and Risk Analysis
Language of Instruction:	English

Credits:	10

NFQ Level:	6

Module Delivered In	2 programme(s)

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	
On successful completion of this module the learner should be able to:	
LO1	Identify and document information security events.
LO2	Plan an appropriate incident handling policy.
LO3	Mitigate risk by evaluating risk management strategies.
LO4	Produce and justify a contigency plan which incorporates disaster recovery.

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is recommended before enrolment in this module.*
No recommendations listed
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module.*
No incompatible modules listed
Co-requisite Modules
No Co-requisite modules listed
Requirements *This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.*
No requirements listed

SAFE: Project Incident Handling and Risk Analysis

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 Framework 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	%
Project	100.00%

No Continuous Assessment

Project

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	Learners will work in teams of two or three throughout the project and can expect to receive feedback on project-related material submitted by weeks 3, 6, and 8.	1,2,3,4	100.00	Week 13

No Practical

No End of Module Formal Examination

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

SAFE: Project Incident Handling and Risk Analysis

Module Workload

Workload: Full Time		
Workload Type	*Frequency*	*Average Weekly Learner Workload*
Lecture	12 Weeks per Stage	4.00
Project	13 Weeks per Stage	5.54
Independent Learning	15 Weeks per Stage	8.67
	Total Hours	250.00

Module Delivered In

Programme Code	Programme	Semester	Delivery
CW_KCCYB_B	Bachelor of Science (Honours) in Cyber Crime and IT Security	4	Mandatory
CW_KCCYB_D	Bachelor of Science in Cybercrime and IT Security	4	Mandatory