

SAFE: Project Incident Handling and Risk Analysis

Module Title: Project Incident Handling and Risk Analysis Language of Instruction: English Credits: 10 Module Dilverol IV 2 programme(s) Tackhing & Learning 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 inter action, supported by practical group in section and peer/independent hearning embedded into procedural and management side of incident handling and risk analysis. 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 inter action, supported by practical group in section and peer/independent hearning embedded into practical group in practin grouprate in practical group in practin group in pr					
Credits: 10 NFQ Level: 6 Module Delivered In 2 programme(s) Teaching & Learning 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 mbedded 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 Identify and document information security events. L01 Identify and document information security events. L02 Plan an appropriate incident handling policy. L03 Mitigate risk by evaluating risk management strategies. L04 Produce and justify a contigency plan which incorporates disaster recovery. Pre-requisite learning Module Recommendations Module Recommendations listed Incompatible dearing outcomes that are too similar to the learning outcomes of this module. No incompatible modules listed Co-requisite modules listed Requirements Module Recommendations disted	Module Title):	Project Incident Handling and Risk Analysis		
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 To develop learners knowledge of information security incident handling and perform risk analysis on information systems. Lo1 Identify and document information security events. L01 Identify and document information security events. L02 Plan an appropriate incident handling policy. L03 Mitigate risk by evaluating risk management strategies. L04 Produce and justify a contigency plan which incorporates disaster recovery. Pre-requisite learning Module Recommendations This is prior learning outcomes that are too similar to the learning outcomes of this module. No incompatible modules listed Co-requisite Modules Iste <t< td=""><td colspan="2">Language of Instruction:</td><td colspan="3">English</td></t<>	Language of Instruction:		English		
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 To develop learners should be able to: L01 Identify and document information security events. L02 Plan an appropriate incident handling policy. L03 Mitigate risk by evaluating risk management strategies. L04 Produce and justify a contigency plan which incorporates disaster recovery. Pre-requisite learning Module Recommendations This is prior learning outcomes that are too similar to the learning outcomes of this module. No recommendations listed Incompatible Modules Incompatible Modules Into a studies which have learning outcomes that are too similar to the learning outcomes of this module. No incompatible modules listed Co-requisite modules listed Requireme	Credits:		10		
Teaching & Learning 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 session 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 To develop learners' knowledge of information security incident handling and perform risk analysis on information systems. L01 Identify and document information security events. L02 Plan an appropriate incident handling policy. L03 Mitigate risk by evaluating risk management strategies. L04 Produce and justify a contigency plan which incorporates disaster recovery. Pre-requisite learning Module Recommendations This is prior learning outcomes that are too similar to the learning outcomes of this module. No recommendations listed Incompatible Modules These are modules listed Co-requisite modules listed Requirements Requirements	NFQ Level:		6		
Strategies: Content will be delivered to learners through lectures with class interaction, supported by practical group sessions. Practical sessions will noroprore workshop style classes for case studies, role based scenarios and evaluation of model policies/frameworks. Collaboration and peer/independent learning embedded into practical session sult practical session 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 To develop learners should be able to: L01 Identify and document information security events. L02 Plan an appropriate incident handling policy. L03 Mitigate risk by evaluating risk management strategies. L04 Produce and justify a contigency plan which incorporate works. Module Recommendations Troit practical skill) that is recommended before enrolment in this module. No recommendations This is prior learning outcomes that are too similar to the learning outcomes of this module. No incompatible modules listed Co-requisite modules listed Requirements Requirements	Module Deli	vered In	2 programme(s)		
Information systems. Learning Outcomes On successful completion of this module the learner should be able to: L01 Identify and document information security events. L02 Plan an appropriate incident handling policy. L03 Mitigate risk by evaluating risk management strategies. L04 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 Requirements			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 scenario and evaluation of model policies/frameworks. Collaboration and peer/independent learning embedded into		
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	Module Aim	:			
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 listed No Co-requisite modules listed Requirements	Learning Ou	utcomes			
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	On successf	ul completior	n of this module the learner should be able to:		
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	LO1	Identify and document information security events.			
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	LO2	Plan an ap	appropriate incident handling policy.		
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	LO3	Mitigate risk by evaluating risk management strategies.			
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	LO4	Produce and justify a contigency plan which incorporates disaster recovery.			
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	Pre-requisite	e learning			
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					
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	No recomme	endations list	ted		
Co-requisite Modules No Co-requisite modules listed Requirements			h have learning outcomes that are too similar to the learning outcomes of this module.		
No Co-requisite modules listed Requirements	No incompat	ible modules	s listed		
Requirements	Co-requisite	e Modules			
	No Co-requis	site modules	s listed		
me le men realing (el a practical char) that to manaatory solete contonnont in this modulo to anomoti.			a practical skill) that is mandatory before enrolment in this module is allowed.		
No requirements listed	No requireme	ents listed			



Module Content & Assessment

SAFE: Project Incident Handling and Risk Analysis

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