Title:	Security Contingency Planning APPROVED
Long Title:	Security Contingency Planning

Module Code:	COMP9081	**Duration:**	1 Semester

Credits:	5
NFQ Level:	Expert
Field of Study:	Computer Science
Valid From:	Semester 1 - 2020/21 (September 2020)
Module Delivered in	2 programme(s)
Module Coordinator:	Sean McSweeney
Module Author:	Sean McSweeney
Module Description:	Attacks on a company can cause severe damage in terms of lost revenue, reputation damage, network disturbances impacting not only the company themselves but also its customers. Developing a proper and well defined approach to contingency planning in the face of a cyber event reduces the impact of the damage so that the company can prepare for future cyber incidents. In this module students will learn about contingency planning and its main elements in incident response, disaster recovery and business continuity.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
LO1	Develop a business continuity plan through the effective identification of threats and analysing their impact on business operations.
LO2	Perform a threat assessment and modelling with the aim of optimising network security measures.
LO3	Develop a security awareness programme for an organisation with the aim of establishing a security conscious culture.
LO4	Critique a disaster recovery plan for efficacy and adherence to regulations and legal requirements.
LO5	Plan an incident response, backup and recovery procedure for an organisation.

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is strongly recommended before enrolment in this module. You may enrol in this module if you have not acquired the recommended learning but you will have considerable difficulty in passing (i.e. achieving the learning outcomes of) the module. While the prior learning is expressed as named CIT module(s) it also allows for learning (in another module or modules) which is equivalent to the learning specified in the named module(s).*
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module. You may not earn additional credit for the same learning and therefore you may not enrol in this module if you have successfully completed any modules in the incompatible list.*
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. You may not enrol on this module if you have not acquired the learning specified in this section.*
No requirements listed

Module Content & Assessment

Indicative Content
Business Continuity Planning Business Continuity Planning vs. Disaster Recovery Planning, Project scope and planning, Business impact assessment, Identify Priorities, Business Impact Assessment (BIA), Prioritization and classification of business functions, evaluating impact and dependencies, Resource Prioritization, Continuity planning, implementation, BCP Team Selection, Legal and Regulatory Requirements, Testing and Exercises for BCP resilience, use cases of BCPs.
Assessment and Testing Categorizing Threat Actors Tools Techniques and Procedures (TTPs), MITRE ATT&CK, Strategies for Threat Modeling, Threat Analysis Practices and Tools, Categorizing Threats, Threat Models, Attack Trees, Attack Libraries, Threat Profiles, IDDIL/ATC, STRIDE/DREAD, Security Testing, Vulnerability Scanning, Penetration Testing, Log Reviews, Software Testing, Third Party Software. Managing Threat Assessment and Intelligence Operations.
Awareness, training and education User awareness and educational programmes, protecting personal privacy, elements of the digital footprint, security technologies and tools, host firewalls, VPN, proxies, access points, SSL/TLS, anti-spam, anti-virus, considerations for different device categories, computer backups (on and offline), patch application and management. Incident Reporting culture. Security Operating Procedures. Insider threats. External Attacks. Staff induction process. Maintaining user awareness.
Incident Response Defining security events and incidents, Attack and incident response lifecycles, Volatile and non-volatile data, IOCs vs IOAs, Laws relating to the capture of static and dynamic data, Pre-Incident Preparation, Scoping an Incident, Incident response team management, EU and Global legal frameworks. Best practices and uses cases. NIST 800-61 r2 and SANS PICERL. Developing and Managing Incident Response Teams and Frameworks.
Disaster Recovery Planning Categorization and assessment of disasters, System Resilience and Fault Tolerance, DR Personnel (Rescue/Recovery/Salvage teams), Trusted Recovery, Crisis Management, Emergency Communications, Recovery Time Objective, Recovery Point Objective, Layers of Defense, Fail-over Mechanisms, Plan testing and maintenance, Legal Issues, ISO 22301:2019, ISO 22313:2012, ISO 22320:2018, ASIS ORM.1.201
Backup and Availability Backup and Recovery Procedures, Storage Disk Layouts, RAID, On site and off site backups, Backup Strategies, Cloud based, Backup testing, Information storage and disposal, Server backups, Electronic Vaulting, remote journaling and mirroring, best practices, ISO/IEC 27040 and ISO 20001 requirements

Assessment Breakdown	%
Course Work	100.00%

Course Work

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	This project will evaluate the student's capacity to formulate a business continuity plan based on information presented on a use case including a threat model. The BCP is to be augmented with a awareness training strategy which the student must also detail.	1,2,3	50.0	Week 6
Written Report	This report will assess the student's understanding of the incident response process, safe and robust backup procedures and technologies and how these relate to disaster recovery. The student will formulate a disaster recovery plan and then apply this plan to a use case detailing the incident response process and mitigation with appropriate remote backups and recovery.	4,5	50.0	Sem End

No End of Module Formal Examination

Reassessment Requirement

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

The institute reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent study.	3.0	Every Week	3.00
			Total Hours	7.00
			Total Weekly Learner Workload	7.00
			Total Weekly Contact Hours	4.00

Workload: Part Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent study.	3.0	Every Week	3.00
			Total Hours	7.00
			Total Weekly Learner Workload	7.00
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

- **Michael E. Whitman, Herbert J. Mattord 2016, *Management of Information Security*, 5th Ed., Chapter 10, Cengage Learning [ISBN: 130550125X]**
- **Mike Chapple, James Michael Stewart and Darril Gibson 2018, *(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide*, 8th Ed., Sybex [ISBN: 1119475937]**

Supplementary Book Resources

- **Andrew Hiles 2010, *The Definitive Handbook of Business Continuity Management*, 3rd Ed., Wiley [ISBN: 0470670142]**

Recommended Article/Paper Resources

- **Herbane, Brahim 2010, *The evolution of business continuity management: A historical review of practices and drivers*., Business history, Vol 52, Issue 6**
- **Lee, Robert M., Michael J. Assante, and Tim Conway. 2014, *German steel mill cyber attack.*, Industrial Control Systems, Vol 30, 62**
- **Haass, Jon C., Gail-Joon Ahn, and Frank Grimmelmann 2015, *Actra: A case study for threat information sharing*., Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security.**

Other Resources

- **Website: SANS*Incident Response Reading Room* https://www.sans.org/reading-room/whitep apers/incident/**
- **Website: NIST 2012, *800-61 r2* https://nvlpubs.nist.gov/nistpubs/Specia lPublications/NIST.SP.800-61r2.pdf**

Module Delivered in

Programme Code	Programme	Semester	Delivery
CR_KCYMN_9	Master of Science in Cybersecurity Management	1	Mandatory
CR_KCYMT_9	Postgraduate Diploma in Science in Cybersecurity Management	1	Mandatory