Title:	Security Architecture APPROVED
Long Title:	Security Architecture

Module Code:	COMP9080	**Duration:**	1 Semester

Credits:	10
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:	VINCENT RYAN
Module Description:	Security Architecture is defined as a description, placement and allocation of security functions and controls with the aim of maintaining IT systems quality attributes such as confidentiality, integrity and availability. This module explores how an organisation can implement cybersecurity controls and organise its infrastructure best so that it can deter and respond to attacks when they occur. As part of this module security devices and products will also be explored in the context of their application as part of an overall security architecture implementation.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
LO1	Evaluate the applicability and use of Cybersecurity Architecture Frameworks to support and implement security features in an organisation.
LO2	Appraise the effectiveness of an organisation's Identity and Access Control (IAC) mechanisms.
LO3	Evaluate and secure a network through the appropriate design, placement and configuration of networking technologies, techniques and protocols.
LO4	Critically assess the security of a cloud based virtualised infrastructure with the aim of protecting data, application and services of cloud computing resources.
LO5	Appraise the application of cybersecurity controls and technologies used by an organisation to prevent an attack.
LO6	Appraise the application of cybersecurity controls and technologies used by an organisation to detect and respond to a successful attack.
LO7	Evaluate the security of an organisation from an Architecture viewpoint using each element of the Availability, Integrity, Confidentiality (AIC) Triad as a guide.

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 MTU 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
Frameworks for Enterprise Security Architecture SABSA - Enterprise Security Architecture. Cross Boundary Enterprise Security Framework (CB ESM). Cybersecurity Operations Centre (CSOC). The Open Group Architecture Framework (TOGAF). Critical review and comparison of different frameworks.
Cryptography Cryptography as a security control. Symmetric, Public Key, Hashing, Digital Signatures, Key Exchange, Public Key Infrastructure, TLS, Code and Update Signing.
Passwords and Authentication Authentication Controls. Password representations, Entropy, Password Cracking, Salting and Hashing, Password Spraying Attack, Passwordless Authentication, Biometrics, MFA, Authentication vs. Authorisation (e.g. SAML verses OAuth)
Access Control Role Based, Discretionary, Non-discretionary, Mandatory. Access Control Technologies : Single Sign On (SSO), Identity As A Service (IaaS), Link Discovery Access Protocol (LDAP), Kerberos, Active Directory (AD), Identity and Access Management, Privileged Access Management (PAM). Information Rights Management (IAM).
Networking LAN and WAN technologies and protocols, OSI model, TCP, IP, UDP, ICMP, Encapsulation, Wireless LANs, Routers, SNMP, Switches, Port Security, Modems, VPN Communication, Network Segmentation, VLANs, DMZ, Logging the network (PCAP, netflow, Zeek logs etc.), Application Layer Protocols (e.g. DNS, DHCP), DoH, Network based attacks such as DDoS. Lateral Movement Detection, C2 Traffic Detection, Data Exfiltration Detection, Secure configuration of network devices, BGP, OSPF, IPv6, Proxies, Load Balancers, Routing tables, Network segmentation between the OT and IT environments, Purdue Model, Dealing with Encrypted Traffic, Secure Network Design. Zero Trust Networks.
Cloud Security Security Architecture and Networking Technologies as they apply and are used in the Cloud. Policies, technologies and control to protect cloud resources. Data Centres, Virtualisation, Data Containers, Automation, Micro-segmentation.
Security Technologies and Products Firewalls, IPS/IDS, DLP, SIEM, Log Correlation and Management, UTM, User and Entity Behaviour Analytics (UEBA), Honeypots, Network Traffic Analysis, Threat Feeds, Next Generation, Anti-Virus, Patch Management, Change Management, Perimeter Management, Web Security, Email Security, Server Security, Defence in Depth, SOC, NOC, Network Monitoring Devices. Deployment of these to prevent and detect attacks.
Security Testing Mechanisms to detect vulnerabilities of a system. Vulnerability Scanning, Penetration Testing, Red and Purple Teaming, Log Reviews, Software Testing, Third Party Software, API Security
Product Security Architecture Designing software with security in mind. Where security controls fit into software design and development. Secure Software Development Lifecycle. Privacy by Design. Protecting IP in software products. Managing third party and technology partner ecosystem risks. Chip-to-Cloud Security. Secure product support, OWASP Top 10, Web App Firewalls
Case Studies Organisations and their approach to Security Architecture, AIC Triad considerations, Gap Analysis, Scoping, Budgets

Assessment Breakdown	%
Course Work	100.00%

Course Work

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Written Report	Lab report detailing and critiquing assigned tasks carried out. This assessment will focus mainly on networking and cloud technologies.	3,4	30.0	Week 5
Written Report	Lab report detailing and critiquing assigned tasks carried out. This assessment will focus mainly on Identity and Authentication, cybersecurity devices and technologies and logs.	2,5,6	30.0	Week 10

Project	Design a Security infrastructure for an organisation evaluating parameters such as reliability, cost and security.	1,2,4,5,6,7	40.0	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 underpinning learning outcomes.	4.0	Every Week	4.00
Lab	Lab supporting content delivered in class.	2.0	Every Week	2.00
Directed Learning	Independent study.	8.0	Every Week	8.00
			Total Hours	14.00
			Total Weekly Learner Workload	14.00
			Total Weekly Contact Hours	6.00

Workload: Part Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture underpinning learning outcomes.	4.0	Every Week	4.00
Lab	Lab supporting content delivered in class.	2.0	Every Week	2.00
Directed Learning	Independent study.	8.0	Every Week	8.00
			Total Hours	14.00
			Total Weekly Learner Workload	14.00
			Total Weekly Contact Hours	6.00

Module Resources

Recommended Book Resources

- **Brook S. E. Schoenfield 2019, *Secrets of a Cyber Security Architect*, Auerbach [ISBN: 9781498741996]**

Supplementary Book Resources

- **Gerard Blokdyk 2017, *Enterprise Information Security Architecture: A Complete Guide*, CreateSpace [ISBN: 9781977702067]**
- **Pass Always 2019, *ISSAP Information Systems Security Architecture Professional Study Guide: ISC CISSP-ISSAP*, Independently published [ISBN: 9781079333619]**
- **Brook S. E. Schoenfield 2017, *Securing Systems: Applied Security Architecture and Threat Models*, CRC Press [ISBN: 9781482233971]**
- **Paul Thomas 2017, *Designing Security Architecture Solutions*, CreateSpace [ISBN: 9781979805209]**

Supplementary Article/Paper Resources

- **NIST 2020, *Security and Privacy Controls for Information Systems and Organizations*, Draft NIST Special Publication 800-53 Revision 5**
- **NIST 2013, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Revision 4**
- **NIST 2013, *Cloud Computing Security Reference Architecture*, Draft NIST Special Publication 500-299**

Other Resources

- **Website: Cloudflare *Learning Centre***
  https://www.cloudflare.com/learning/
- **Website: NSA *Information Assurance Guidance***
  https://apps.nsa.gov/iaarchive/library/i a-guidance/
- **Website: Carnegie Mellon University *SEI Blog***
  https://insights.sei.cmu.edu/
- **Website: Cybersecurity Forum *What is Cybersecurity Architecture?***
  https://cybersecurityforum.com/cybersecu rity-faq/what-is-cybersecurity-architect ure.html
- **Website: *FIDO Alliance (Open Industry Association with a focused mission to help reduce the over-reliance on passwords)***
  https://fidoalliance.org/overview/

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