INFO08033
CyberSecurity Governance, Risk and Compliance

Full Title	CyberSecurity Governance, Risk and Compliance		
Status	Uploaded to Banner	**Start Term**	2020
NFQ Level	08	**ECTS Credits**	10
Module Code	INFO08033	**Duration**	26 Weeks - (26 Weeks)
Grading Mode	Numeric	**Department**	Business, Humanities and Tech
Module Author	Brian Mulhern		

Module Description

This module introduces students to concepts of Information technology governance, and the major governance frameworks which organisations use to manage their IT operations efficiently, safely and with a high degree of security: COBIT, ITIL, COSO, and CMMI. Specifically, the module explains the elements of these frameworks relating to cybersecurity risk management, cognitive risk, and the International cybersecurity standards in use: ISO 27001/2/3, NIST-CSF, and HITRUST-CSF. The module examines in detail cybersecurity Risk *categories* and quantitative and qualitative risk assessment techniques. Probabilities around attack likelihood, annual loss expectancy, and impact are calculated. Management, Technical and Operational risk mitigations are explained in terms of the MITRE ATT&CK and Lockheed Martin Kill Chain frameworks. Finally, generic industry and public service organisations: are examined: manufacturing, financial services (PCI DSS), healthcare (HL7), government; from the point of view of cybersecurity compliance/data protection regulations.

	Learning Outcomes ***On completion of this module the learner will/should be able to:***
1.	Analyse key Information Technology Governance Frameworks including COBIT, ITIL, CMMI, COSO, etc, and the rules and policies which ensure effective, controlled, and integrated operation of an organisation's IT infrastructure and data.
2.	Examine cyber security risk management frameworks, including the Mitre Cyber Prep 2.0, NIST CSF, and Cognitive Risk Frameworks.
3.	Explain international cyber security standards (ISO 27001/2/3/4, NIST CSF, and O-RT, O-RA), and explain the context in which these are used to defend against cybersecurity threats.
4.	Examine and apply qualitative and quantitative risk assessment methodologies (DREAD, CVSS, SLE, EF, ARO, and ALE) in the context of threat probabilities and vulnerabilities.
5.	Critically explore threat/cyber risk mitigation philosophies in terms of effectiveness, adaptability, and strategic integration including Lockheed Martin Cyber Kill Chain, and the Mitre ATT&CK framework.
6.	Identify the guidelines and best practices which form the compliance and regulatory frameworks in manufacturing, financial services industries, healthcare, and public service arenas: (SOX, PCI DSS, NIST, HL7, HIPAA/HITECH, SOCs, AT-101, and FedRAMP).

Indicative Syllabus

1. Information Technology Governance Frameworks - 30%

Examine the rules and policies around managing the IT infrastructure of an enterprise. Analyse the concept of an IT governance framework, and examine industry-wide frameworks: COBIT, ITIL, CMMI, COSO, etc, from the point of view of how they support the alignment of IT with organisational business strategies. Describe the aspects of standard governance frameworks relating to cybersecurity, and how these support the cyber resilience of an organisation. Investigate how governance frameworks are implemented across various organisation types.using case studies.

2. Risk Theory and Risk Evaluation in a Cybersecurity context - 15%

Review of theory around Data Distributions, Probability, and Bayesian Analysis. Examine Cyber Risk concepts: threat, vulnerability, exposure, impact and mitigation. Quantitative cyber risk assessment techniques: probability models, confidence intervals, Monte Carlo simulations. Analysis of Vulnerabilities, Assets, and Attack Profile, Risk score/metrics calculations based on Exposure Factor (EF), Annualised Loss Expectancy (ALE), Single Loss Expectancy (SLE), and Annual Rate of Occurrence (ARO). Qualitative risk assessment techniques based on the Common Vulnerability Scoring System (CVSS), and the DREAD model.

3. Risk Management - 15%

Analysis of risk categories: Hacking Risk, Insider risk, Data Loss risk, Cognitive Risk. Cyber Risk Management Frameworks (RMF), including the NIST RMF, and how they integrate with standard IT governance frameworks - specifically COBIT and ITIL. Cybersecurity posture: Adaptability, Agility, Critical Information Protection and Cyber Resilience. Technical, Managerial and Operational controls involved in mitigating cyber risk. Risk Audit. The FAIR (Factor Analysis of Information Risk) Model,

4. Risk Mitigation - 10%

Analysis and use of the Lockheed Martin Cyber Kill Chain, Mitre ATT&CK framework in risk mitigation. Criteria for risk acceptance. Risk Analysis software tools.

4. Cyber Security Standards - 10%

Cyber Security / Information security standards - definition: The need for Business, Product and Personal standards. Analysis of common cybersecurity standards: ISO\IEC 27001/2/3/4, ISO 27017/18, NIST CSF, NIST 800-171, FedRAMP, etc. Cyber Security training and qualification standards.

6. Industry specific and Generic Compliance requirements - 20%

The general laws, regulations, standards and policies around data security, mandated across all private and public service organisations - GDPR and PII. Industry specific regulatory compliance: Financial Services (PCI DSS, SOX), Banking (EBA), Healthcare (HL7, HIPAA), Service Organisations (SOC 1&2), The EU-US privacy shield framework. IT Systems compliance around food and drug manufacture. Compliance management frameworks, effects of non-compliance, Compliance management tools (Microsoft Compliance centre) Compliance Scores.

Teaching and Learning Strategy

This module can be delivered via the traditional face-to-face delivery methodology or via a blended format (employing both online and offline methodologies.) or via an online format.

Traditional face-to face delivery format.

The module can be delivered in the traditional delivery method using 2 lectures and 1 hour tutorial per week.

Blended delivery format.

The module can be delivered in the blended delivery method using a mixture of online delivery (approx. 66%) and face-to-face engagement (approx 33%) per week.

Weekly online delivery will consist of, but not exclusive to, live lectures and webinars, pre-recordings, synchronous and asynchronous discussion forums and open educational resources (OER's), exercises and reading, accounting for approx. 2 hours per week.

Online delivery format.

In the online delivery format, the module will be delivered via both synchronous and asynchronous online methods. One hour per week of live video lectures will be available in addition to 2 hours of asynchronous chats, blogs, email availability, etc. It is also intended to include live webinars from external guest lecturers (3 hours) with specific expertise in certain areas of cybersecurity GRC. As this is a part-time programme It is recognised that potential students will come from diverse industry/cybersecurity settings, and as such will bring their own unique experiences and challenges to the learning environment. In this context, online class discussions/blogs will be very much encouraged to facilitate a shared learning experience.

Information concerning the nature and timing of continuous assessment will be reviewed and agreed with learners and external examiners at the beginning of the academic year. Marking criteria, deadlines and expectations will also be provided to the learner in advance. Constructive feedback will be provided in a timely manner and in an appropriate format.

Independent Learning.

Allied to the Approved Programme Schedule hours students will be required to pursue Independent Learning as part of the module.

Assessment Strategy

The module will be assessed in line with GMIT's Code of Practice No. 3; Marks and Standards. It is intended that learning outcomes will be assessed through both continuous assessment (40%) and an end of year examination (60%). The continuous assessment elements will focus on governance and cybersecurity frameworks, risk theory and risk quantification, and will take the form of both an online time-constrained Multiple Choice Quiz (MCQ) (20%), and an individual online project submission (20%). The end of year examination, will take the form of a time-constrained (1.25 Hour) MCQ (60%), and will focus on the application of the theoretical areas of the module. This final MCQ exam is designed such that each student is presented with a unique random question set. The assessments will be moderated by an elected external examiner.

Repeat Assessment Strategies
Repeat assessments will mirror the initial module assessment, and will be staged in line with GMIT'S CoP No. 3, and in agreement with the external examiner.

Indicative Coursework and Continuous Assessment:		40 %		
Form	***Title***	***Percent***	***Week (Indicative)***	***Learning Outcomes***
Multiple Choice	Governance & Cyber Frameworks - CA	20 %	Week 8	1,2
Individual Project	Risk Quantification - CA	20 %	Week 12	3,4

End of Semester / Year Formal Exam:		60 %		
Form	***Title***	***Percent***	***Week (Indicative)***	***Learning Outcomes***
Multiple Choice	Final MCQ Exam	60 %	End of Term	2,3,5,6

Full Time Delivery Mode Average Weekly Workload:			3.00 Hours		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Lecture	In Class Lecture	Seminar Room	2	Weekly	2.00
Tutorial	In Class tutorial	Seminar Room	1	Weekly	1.00

Online Learning Delivery Mode Average Weekly Workload:			3.00 Hours		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Online Learning	Online tutorial	Online	1.0	Weekly	1.00
Online Learning	Asynchronous online student engagement: blogs, chats, emails, etc	Online	2.0	Weekly	2.00

Blended Delivery Mode Average Weekly Workload:			3.00 Hours		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Online Learning	Online Tutorial	Online	2	Weekly	2.00
Tutorial	in Class activity	Seminar Room	1	Weekly	1.00

Recommended Reading Book List
Caldwell, F., (2020). *Governance, Risk and Compliance*. Kogan Page. ISBN 1789661048 ISBN-13 9781789661040
Dr, Y., (2014). *Cyber Security Management*. Ashgate Publishing, Ltd.. ISBN 9781472432094 ISBN-13 1472432096

Online Resources
https://learnonline.gmit.ie https://thegrcbluebook.com

Programme Membership
GA_KCYBC_L08 202000 Higher Diploma in Science in Cybersecurity Risk & Compliance