UNIVERSITY OF GLOUCESTERSHIRE

School of Computing and Engineering

Park Campus, Cheltenham

www.glos.ac.uk

CT7075 Information Security Management Module Guide 2022/2023

Module Leader | Jordan Allison | jallison1@glos.ac.uk

UNIVERSITY OF GLOUCESTERSHIRE

TABLE OF CONTENTS

1) MODULE OVERVIEW

This module is concerned with the operation and improvement of information security. As such, it encompasses roles commonly defined in the security community and incorporates topics on Information Security governance and compliance, security standards and regulation, risk and threat in information security and the role of security policies. The module is taught using relatable examples of everyday risks and the relationship to the interconnected and complex digital world.

Different perspectives are also presented on cyber risk assessment with sessions that allow students discuss in groups and present their findings. Some major risk assessment methods are also presented with a justification of choices based on different scenarios.

In this module, we will go through the different aspects of information security, risk, risk management methodologies, information security methodologies and techniques, the use of policies that maintain information security as well as the management of information security in complex environments.

You will have full access to different case studies and scenarios to widen your knowledge in this area. You will also learn to develop information security-based ontologies based on different case studies. You will experiment with various ontology design strategies and will be able to evaluate and propose a design for a specific application. Attention is also paid to human factors which is a major cause of risks today. Different scenarios are used during the lessons where students are able to argue for or against the effect of human error in different cases. Different case studies are also presented to extend student's understanding of business continuity, incident response and recovery planning.

Prerequisites: Basic knowledge is required about information security, the security triad, other properties of information security, the importance of information to organisations, information security management systems, the evolving landscape of information security and the risks associated with this evolution.

Reading List: Resources, which are available through the university library are:

- Alexander et al (2020): Information Security Management Principles
- Whitman and Mattord (2018): Management of Information Security Paperback

Students are also encouraged to have a look at online resources and tutorials for different examples and current case studies.

Location: Park Campus, Cheltenham (But online for FHM students)

Scheduled learning and teaching activities: 20 hours

Module Leader: Jordan Allison – jallison1@glos.ac.uk

2) MODULE LEARNING OUTCOMES

A student passing this module should be able to:

1. Operate in complex and unpredictable contexts to select identification and authentication technologies appropriate for an organisation.

2. Reformulate and use practical, conceptual, and technological understanding to create security roles, procedures, and management structures appropriate for an organisation.

3. Provide original and creative critical responses to the task of developing an appropriate business continuity and disaster recovery plan for an organisation.

4. Undertake analysis of complex, incomplete or contradictory evidence/data and argue for a scheme of risk management appropriate for an organisation.

5. Operate in complex and unpredictable contexts to select physical and environmental security measures appropriate for an organisation.

3) MODULE EVALUATION

3.1) Evaluation for 2021/2022

The module involved a one-week intensive course delivery with homework on a daily basis. There was a diverse set of topics related to Information Security Management. On a daily basis, the students were asked to complete a learning journal which showed areas that they were deficient in and which needed further development. This form of delivery was followed by in-class activities to help students develop their understanding. Homework was set each day with all homework being marked to provide students with feedback on their progress.

The feedback from the students was positive and the students indicated that they liked this module as they felt it was quite challenging and had the right content to stimulate and support their learning. Generally, students found the module very interesting and they could relate their better developed critical skills to the module content.

The assessment required students to write a report on the challenges involved in employing contract cyber security professionals. It involved their developing and showing off their critical reasoning skills and providing links to the gig economy as well. The report was in detail rather than general discussion about the chosen topic. The module marks reflect that the average student provided sufficient evidence that linked the report to the case study provided in the assignment brief. Most students provided sufficient information for the paper.

3.2) Evaluation for Current Year

In this current academic year **2022/23**, you will be given the opportunity to undertake a mid-module evaluation. This will contribute to the course board of studies meeting and will inform the module design for the following year. In addition, there will be an independent end of year level evaluation distributed by the University known as the Annual Course Evaluation (ACE).

Additionally, you will be given the opportunity to give continual feedback anonymously via Padlet: https://padlet.com/jrallison1/vo8dtjv3v1okboeo

4) SCHEME OF WORK

Detailed in the table below is the scheme of work for CT7075. *This is an **indicative** scheme of work and subject to change.*

Day	Topic	Cybok Areas

1	• Module Overview and Introduction to Information Security Management
	  ○ Managing information security in organizations.
	  ○ Human factors of managing information security.
	  ○ Evolving cyber-crime environments
	  ○ Physical security of information
	• Organisations and Information Security Responsibilities
	• Emerging Technologies for ISM
		2.2, 2.4, 4.1, 4.2, 4.3, 4.6

2	• Examining Key and Emerging Technologies
	• Security Standards and Security Breaches
	  ○ Data Protection Act & GDPR
	  ○ ISO27000 series
	  ○ Cyber Essentials
	  ○ IASME
	  ○ Cloud control matrix
		2.4, 2.6

3	• Risk and Threat landscape
	  ○ Risk Management – strategic options
	  ○ Risk Assessment methodologies and controls
	  ○ Risk Frameworks
	• Enterprise Risk Management
	• Future of Cyber Security
		2.2, 2.3, 2.4, 2.6

4	• Threats to and Vulnerabilities of Information Systems
	  ○ Threat and vulnerability identification
	  ○ Threat categorization and impact assessment
	• Security Policies, Culture and Awareness
	  ○ The human factor and risk communication
	  ○ Types of security policies
	  ○ Security policy contents
	  ○ Enacting Security policy
		2.5, 4.1, 4.2, 4.3, 4.4, 4.6

5	• Disaster recovery, business continuity, incident management
	  ○ Policies for disaster recovery & business continuity.
	  ○ Threat and vulnerability identification
	  ○ Threat categorization and impact assessment
	• Assignment Workshop
		2.5, 2.6, 2.7, 8.4, 8.5, 8.7

Cybok Knowledge Areas Covered (https://www.cybok.org/knowledgebase/):

- 2.2 – What is Risk
- 2.3 - Why is risk assessment and management important?

- 2.4 - What is cyber risk assessment and Management?
- 2.5 - Risk Governance
- 2.6 - Risk assessment and management principles
- 2.7 - Business continuity: incident response and recovery planning
- 4.1 - Understanding human behaviour in security
- 4.2 - Usable security – the basics
- 4.3 – Human Error
- 4.4 – Cyber Security Awareness and Education
- 4.6 – Stakeholder Engagement
- 8.4 - Plan: Security information and event management
- 8.5 - Execute: Mitigation and countermeasures
- 8.7 - Human Factors: Incident management

5) ASSESSMENT 1

1. Module Code and Title:	**CT7075 Information Security Management**
2. Module Tutor:	Jordan Allison – jallison1@glos.ac.uk
3. Tutor with Responsibility for this Assessment:	Jordan Allison. This is your first point of contact.
4. Assignment:	**001: 100% Coursework:** 001: 100% Coursework: Individual, standard written: 4000 words or equivalent: Individual based on the written assignment.
5. Submission Deadline:	**20th January 2023 at 3pm -** Report submission Your attention is drawn to the penalties for late submission; *see Academic Regulations for Taught Provision.*
6. Arrangements for Submission:	MOODLE
7. Date and Location for Return of Work:	Written feedback and a provisional mark should be within 20 working days.
8. Students with Disabilities:	Alternative assessment arrangements may be made, where appropriate, for disabled students. However, these will only be implemented upon the advice of the disability advisor. Disabled students wishing to be considered for alternative assessment arrangements must give notification of the disability (with evidence) to the Disability Advisor by the published deadlines.
9. University Regulations for Assessment:	All assessments are subject to the **Academic Regulations for Taught Provision**. These include regulations relating to errors of attribution and assessment Offences. In exercising their judgement, examiners may penalise any work if the standard of English, numeracy or presentation adversely affects the quality of the work, or where the work submitted exceeds the published size or time limits, or where the work fails to follow normal academic conventions for acknowledging sources.

10. The Requirements for the Assessment:	You have been employed as an information security management consultant and have been tasked in analysing a small company (of your choice) with regard to the company's' security posture. Specifically, you need to prepare a report (of 4000 words) which includes the following components: 1. An introduction to the company which highlights what the company does, and considers the main security threats faced by the sector the company is in. 2. An analysis of the company's security roles, procedures, and management structures. 3. A network diagram which depicts the key locations, departments, and devices within the organisation (use software such as Cisco Packet Tracer to help with this). Label and provide insights into current security measures within this network diagram (you do not need to configure the network). 4. A risk analysis framework or methodology which is used to evaluate the company's key security risks. 5. Based on the analysis and findings of parts 1, 2, 3 and 4 above, provide recommendations about what should be changed and why. This should consider technical, human, and physical security measures, and any identification and authentication technologies that would be appropriate for the organisation to improve their information security. Justification must be provided for each recommendation. 6. A (brief) business continuity and disaster recovery plan for the organisation. This should also be fully justified and relate to the previous analysis and findings. 7. References. 8. Appendix documentation (if applicable). It is recommended that you choose a small organisation where it may be possible to conduct interviews with employees of the company to help aid your analysis and make your report as real as possible (although this is not compulsory). Where information is not available in the public domain or through contacting the company, you may make some assumptions (but assumptions should be stated in your report in the appendix). The report should be in detail rather than a general discussion about information security management.
11. Special Instructions:	None

13. Associated Learning Outcomes:	1 Operate in complex and unpredictable contexts to select identification and authentication technologies appropriate for an organisation. 2 Reformulate and use practical, conceptual, and technological understanding to create security roles, procedures, and management structures appropriate for an organisation. 3 Provide original and creative critical responses to the task of developing an appropriate business continuity and disaster recovery plan for an organisation. 4 Undertake analysis of complex, incomplete or contradictory evidence/data and argue for a scheme of risk management appropriate for an organisation. 5 Operate in complex and unpredictable contexts to select physical and environmental security measures appropriate for an organisation.