WM267-15 Cyber Risks in Organisations

24/25

Department
WMG
Level
Undergraduate Level 2
Module leader
Hany Atlam
Credit value
15
Module duration
12 weeks
Assessment
100% coursework
Study locations
University of Warwick main campus, Coventry Primary
Distance or Online Delivery

Description

Introductory description

This module covers Information Security Management Principles and a wide area of Information security fundamentals. The course provides an in-depth understanding of principles for managing security operations and legal and regulatory compliance impact on information security management systems. The delegates will also be exposed to secure asset management and effective information security governance with specific applications and references in organisational contexts.

Module web page

Module aims

This module provides students with the theoretical frameworks, foundations, and practical skills underpinning operational information security management and related areas. The module introduces students to the requirements and techniques for risk identification and assessment, and the elements of security management from a business operational and technological perspectives. It also provides students with the fundamentals of governance and compliance, threats, threat

modelling, threat mitigations, the development of secure and resilient systems, and cybersecurity operations and management.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Information security principles
Managing Information risk
Information security frameworks
Procedural and people security controls
Technical security controls
Software development life cycles
Physical and environmental security
Disaster recovery and business continuity management
Other technical security aspects
Corporate Governance
Business continuity and disaster recovery
Applied Cryptography
Security and Privacy models
Systems & Network security Principles
Ethics code of conduct in cyber security

Learning outcomes

By the end of the module, students should be able to:

- Understand how to design, implement, and test information security processes in information security management systems to increase their resilience and conformance with legal and regulatory functions.
- Demonstrate awareness and knowledge of information and systems and network security management processes.
- Assess and analyse tools, techniques, and approaches to quantify threat landscapes and provide mitigation plans in a variety of organisational contexts.
- Design and implement information security policy programs fully aligned with legal and regulatory compliance frameworks.

Indicative reading list

Alexander, D., Finch, A., Sutton, D., & Taylor, A. (2013). Information security management principles. Swindon, U.K: BCS Learning & Development Ltd.
Douglas Landoll. 2011. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, Second Edition (2nd. ed.). CRC Press, Inc., USA.
William Stallings. 2016. Cryptography and Network Security: Principles and Practice (7th. ed.). Prentice Hall Press, USA.

Subject specific skills

You will develop skills and actively be engaged in enquiry during the learning process in information security management frameworks, technologies and tools to real-world scenarios, evaluating and comparing their performance, and analysing the results

You will look at ethics, risk, governance, compliance, the law, and regulations in relation to business operations in terms of real-world cybersecurity scenarios, to gain an understanding of the underpinning concepts of information security management, and the techniques and systems used to operate them

You will further develop collaborative abilities through practical sessions and seminars as part of the task to cross-fertilise and discuss ideas about the technologies, challenges and opportunities in the domain of enquiry. Information sharing is highly recommended and promoted so as to present news ways of tackling with these security challenges and issues in our modern cyberspace

You will work creatively with new ideas and approaches. It will challenge your ability to intellectually, pragmatically and systematically determine the needs in terms of producing appropriate solutions to address aspects of operational information security management based on existing knowledge in the target discipline suitably balanced with your workplace duties and activities

Transferable skills

Team working
Leadership
Decision making
Communication skills

Study

Study time

Type	Required
Lectures	18 sessions of 1 hour (12%)
Seminars	5 sessions of 1 hour (3%)
Tutorials	2 sessions of 1 hour (1%)
Practical classes	5 sessions of 1 hour (3%)
Work-based learning	22 sessions of 1 hour (15%)
Online learning (independent)	30 sessions of 1 hour (20%)
Other activity	8 hours (5%)
Total	150 hours

Type	Required
Assessment	60 hours (40%)
Total	150 hours

Private study description

No private study requirements defined for this module.

Other activity description

Other activity (8 hrs): 3hrs live and asynchronous support sessions to answer questions related to the module and its assessment and 5 hrs of self-directed learning during teaching days.

Online learning independent (30): Apprentices to use their working hours to revise the contents taught during the module.
WBL (22 hrs): Apprentices to discuss with their employers their current practices in managing cyber risks.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time	Eligible for self-certification
Coursework	100%	60 hours	Yes (extension)

Apprentices will undertake a risk assessment and threat modelling on a specific scenario or company.

Feedback on assessment

Feedback given as appropriate to the assessment type:

- verbal feedback given during seminar/tutorial sessions,
- written individual formative feedback on the assignment report and on the presentation,
- written cohort-level summative feedback on the exam.

Availability

Courses

This module is Core for:

- Year 2 of DWMS-H655 Undergraduate Digital and Technology Solutions (Cyber) (Degree Apprenticeship)
- Year 2 of DWMS-H652 Undergraduate Digital and Technology Solutions (Data Analytics) (Degree Apprenticeship)
- Year 2 of DWMS-H653 Undergraduate Digital and Technology Solutions (Network Engineering) (Degree Apprenticeship)
- Year 2 of DWMS-H654 Undergraduate Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)