WM9C4-15 Managing Cyber Risk, Audit and Compliance

24/25

Department
WMG
Level
Taught Postgraduate Level
Module leader
Hany Atlam
Credit value
15
Module duration
4 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Cyber security consultants are often tasked with:

- Providing advice regarding establishing and maintaining an information risk assessment and management framework.
- Aiding clients in determining which risk assessment approach is the most appropriate for the business outcomes they wish to achieve.
- Providing guidance on how identified risks can be strategically managed.
  This module exposes participants to various approaches to information risk assessment and management. There is an emphasis on the practical nature of this process, the issues that face managers in the real world, and the importance of assessing information risk management within the corporate context to ensure that information security and assurance strategies are aligned with business objectives and consistent with legal and regulatory obligations.
  This module equips participants with a detailed applied knowledge of how to establish and maintain a risk management framework. A strong focus will be placed on cost-effectiveness and value to the objectives of the business or enterprise. The module also covers business continuity and resilience.

Participants will gain a detailed understanding of relevant cyber law, ethics, principles and rules of cyber security, data protection, consent and privacy. There is an emphasis on domestic legislation and cross-boundary issues and international efforts as well as an examination of legal issues relating to the authorised conduct of cyber operations such as ethical (as opposed to unethical) hacking.

Module aims

This module equips students to understand various approaches to information risk assessment and management. There is an emphasis on the practical nature of this process, the issues that face managers in the real world, and the importance of assessing information risk management within the corporate context to ensure that information security and assurance strategies are aligned with business objectives and consistent with legal and regulatory obligations.
This module equips students with a detailed applied knowledge of how to establish and maintain a risk management framework. A strong focus will be placed on cost effectiveness and value to the objectives of the business or enterprise. The module also covers business continuity and resilience.
Students will gain a detailed understanding of relevant cyber law, ethics, principles and rules of cyber security, data protection, consent and privacy. There is an emphasis on domestic legislation and cross-boundary issues and international efforts as well as an examination of legal issues relating to the authorised conduct of cyber operations such as ethical (as opposed to unethical) hacking.

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.

- Risk assessment and management approaches and frameworks. International Standards - ISO27001 & ISO3100; certification; the risk assessment and accreditation process; organisational life¬cycle methodologies and processes; interpreting and implementing a security policy as an organisational Information Security Management System (ISMS) Programme.
- Information Governance. Strategic planning and best practices; policy development; business consideration and legal functions; E-discovery; standardisation and accepted practices; auditing and enforcement; monitoring; records management and inventorying; information governance in the Cloud; social media and mobile devices; maintaining an Information governance programme; capability maturity models.
- Business continuity planning. Relating risks to mitigating safeguards and procedures; developing, reviewing and enacting business continuity plans.
- Compliance and auditing. Regulation and compliance including: GDPR, The Data Protection Act, PCI DSS; Understanding auditing standards such as: the International Standards on Auditing (UK) (ISAs (UK)) and International Standard on Quality Control (UK) (ISQC (UK)); security certifications; understanding auditability; the internal audit process.
- Culture and Communication. Techniques and controls; culture and awareness; communicating risk and developing uptake.

Learning outcomes

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

- Demonstrate a critical awareness of the key attributes of an information governance and compliance framework and of legal, regulatory, and good practice guidelines and regulations which govern information/data compliance for delivery in a range of organisational settings.
- Apply an appropriate risk management approach to a given scenario to identify risk, determine risk probability, and identify mitigation strategies.
- Collaboratively generate and present a business continuity and disaster recovery plan to a given case study.
- Demonstrate a critical awareness of the process of auditing information systems.

Indicative reading list

Tipton, H.F. and Nozaki, M.K., 2007. Information security management handbook. CRC press.

Fitzgerald, T., 2016. Information security governance simplified: from the boardroom to the keyboard. CRC Press.

Brotby, K., 2009. Information security governance: a practical development and implementation approach (Vol. 53). John Wiley & Sons.

View reading list on Talis Aspire

Research element

There is a strong emphasis on the development, growth and enhancement of individual research skills so as to provide participants with the high level research knowledge, skills and competencies needed to undertake an independent, original piece of research. The module content draws upon and highlights research within the domain and the module assessment requires participants to perform further research before preparing a response to the assessment task.

Interdisciplinary

Although the module is largely dedicated towards the development of discipline-specific technical, professional and analytical skills, there is an inherent emphasis on the interdisciplinary nature of the subject. Risk assessment and management is a skill that is applicable across a multitude of disciplines, so much so that this module could be made available to participants from other degree programmes.

Subject specific skills

Participants will develop an advanced applied understanding of risk assessment and management approaches and frameworks, issues and challenges relating to information governance, business continuity planning, and the process of compliance and auditing planning and implementation.

Transferable skills

Critical thinking, communication, information literacy, digital literacy, intercultural awareness, professionalism.

Study

Study time

Type	Required
Supervised practical classes	30 sessions of 1 hour (20%)
Private study	60 hours (40%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Independent work between workshops

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A3

	Weighting	Study time
Risk Management Report	80%	50 hours
Students will prepare a risk management report to include a comprehensive mitigation and response plan and strategy.		
Risk, Audit, Compliance presentation	20%	10 hours
Students will be given a task and divided into groups. Then, each group will prepares response, plan and present it on the final day		

Assessment group R1

	Weighting	Study time
Risk Management Report	100%	

Students will prepare a risk management report to include a comprehensive mitigation and response plan and strategy

Feedback on assessment

Feedback will be provided as annotated commentary within the submitted work. High level feedback will be provided on a standard WMG feedback sheet. Students will have an opportunity to get further feedback and support directly from the module tutor.

Availability

Courses

This module is Core for:

- Year 1 of TWMS-H1S1 Postgraduate Taught Cyber Security Engineering (Full-time)
- Year 1 of TWMS-H1SH Postgraduate Taught Cyber Security Management (Full-time)