WM279-18 Information Risk and Security Management

24/25

Department
WMG
Level
Undergraduate Level 2
Module leader
Paul Stephens
Credit value
18
Module duration
18 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

All organisations have information that they value and that value needs protecting. Within an organisation, some individuals carry formal responsibility for protecting the value of information. Ensuring that the responsible persons within an organisation have appropriate confidence in the security measures, which are protecting the organisation's valuable information, is the realm of information security management.

Why the organisation might value the information will vary from organisation to organisation and from information point to information point. The properties of the information that give it value similarly will vary by organisation and by information point. Some information will be special secret knowledge that gives the organisation competitive advantage; if that information leaks to a competitor, then its value is reduced. Some information may control the organisation's processes; if this controlling information is changed, then its value may be reduced since it causes the organisation to behave less well. Some information may relate to external perception of the organisation's ability to function; if external parties perceive this publicity information is not under the control of the organisation, then future opportunities for the organisation may be degraded through loss of trust.

Determining the relationship between the properties of information that give it value, the

vulnerability of those properties to degradation, threats that might take advantage of the vulnerability to degradation, and the resultant impact to the organisation when bad things happen, is the realm of information risk management. Things can be done to reduce the vulnerability, the threat, or the severity of the impact. These things enhance information security.

Module aims

The module aims to provide the students with the skills that will allow them to have the confidence to recognise and assess information security risks and identify appropriate ways to manage information security within an organisational context. It is about designing and evaluating the solutions that have the strategy, policy, processes, behaviours, and technology, in place and coherently supporting each other.

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 Standards
- Legal and Regulatory frameworks
- Audit and Compliance
- Information Security Governance and Planning
- Information Assurance
- Planning for Risk Assessment
- Managing Risks and Threats
- Information Security Policy Principles
- Information Security Policy Implementation
- Physical and environmental security
- Technical security controls
- Disaster recovery and business continuity
- Incident Response and digital investigations
- Information sharing

Learning outcomes

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

- Develop an understanding on adopting a responsible attitude to the social, ethical, legal and regulatory consequences that flow from professional engagement in security management.
- Apply a relevant risk management approach to a given organisation or scenario.
- Analyse the organisational consequences that result from inadequate information risk management.
- Evaluate the overall coherence of an organisation's management of cyber security, recommending remediation where needed.

Indicative reading list

The existing list will be updated with books such as: Information Risk Management: A

practitioner's guide, David Sutton, 2021.

View reading list on Talis Aspire

Subject specific skills

Participants will demonstrate the ability to:

- apply the principles of information risk and security management at the strategic, tactical and operational levels of an organisation;
- design, conduct and manage an assessment of risks relating to information systems and assets;
- articulate methods that support the overall evaluation of an organisation's management of information security;
- design and deliver an information security management system.

Transferable skills

- Organisational awareness
- Communication
- Teamwork
- Decision making

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 2 hours 30 minutes (25%)
Private study	65 hours (36%)
Assessment	70 hours (39%)
Total	180 hours

Private study description

Independent activities between workshops, following up on activities initiated in previous activities or preparing for upcoming activities.

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 A

	Weighting	Study time
Report on managing risks	50%	35 hours
Conduct a risk assessment on a given scenario and discuss remediation approaches.		
Information Security Framework of Policies	50%	35 hours
Design and apply a framework of policies that adheres to specific requirements.		

Feedback on assessment

Written feedback for each assignment
Verbal feedback during seminars
Summative feedback on assignments

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security