WM055-15 Information Risk Management and Governance

22/23

Department
WMG
Level
Taught Postgraduate Level
Module leader
Elzbieta Titis
Credit value
15
Module duration
1 week
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Various approaches are available concerning the identification, quantification, treatment and monitoring of information risk. There are substantial formal consequences in numerous regulated sectors for failure to deal appropriately with risk. There are substantial informal consequences in all sectors for failure to deal appropriately with risk.

This module develops an understanding, both of the risks that digital information and network assets are exposed to, and of how to the manage those risks to the benefit the enterprise; this includes home users, e-commerce, and all organisations using digital networks for infrastructure, both closed and open. Therefore, this module is relevant for the majority of organisations in existence today or likely to exist in the future.

The module equips students to establish and maintain a risk management framework to provide assurance that information security and assurance strategies are aligned with business objectives and consistent with legal and regulatory obligations. A strong focus will be put on cost effectiveness and value to the objectives of the business or enterprise.

Various approaches to information risk management and the governance are compared and contrasted. The module also covers business continuity and resilience. There is an emphasis on

the practical nature of this process and issues that face managers in the real world.

Module aims

To equip students to undertake information risk management and information risk governance.

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.

International Standards, certification, 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.

Security:
Techniques and Controls ,
Culture & Awareness
System Management
in contracts .

Operational Management

Overview of Incident Management

Information risk:
in context,
core concepts ,
assessments
mitigations ,
standards and methodologies

Implementing a risk management strategy

Working with other organisations

Communicating risk and developing uptake

Information security governance

Learning outcomes

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

- Critically analyse various approaches to information risk management.
- Critically analyse various approaches to information risk governance
- Critically evaluate the most suitable approach to information risk management for a given scenario.

- Critically evaluate the most suitable approach to information risk governance and select the most appropriate for a given scenario.

Indicative reading list

Information Security Governance - Wiley, Krag Brotby (2009), ISBN 978-0-470-13118-3
Information Security Governance Simplified – from the boardroom to the keyboard – CRC press Taylor and Francis Group, Todd Fitzgerald (2011), ISBN 978-1-439-81183-4

Subject specific skills

Undertake information risk management. Undertake information risk governance .

Transferable skills

critical thinking, organisational awareness, ethical values

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Seminars	10 sessions of 1 hour (7%)
Tutorials	10 sessions of 1 hour (7%)
Online learning (independent)	50 sessions of 1 hour (33%)
Assessment	70 hours (47%)
Total	150 hours

Private study description

No private study requirements defined for this module.

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 A1

	Weighting	Study time	Eligible for self-certification
Coursework	80%	60 hours	Yes (extension)
Report, typically addressing a specific scenario.			
Risk, Audit, Compliance presentation	20%	10 hours	No
Task presented to group in week, students placed into groups, presentation made to panel on final day of module.			

Assessment group R

	Weighting	Study time	Eligible for self-certification
Assessed work as specified by department	100%		Yes (extension)
100% Assignment			

Feedback on assessment

Written feedback provided with the mark via tabula.

Availability

Anti-requisite modules

If you take this module, you cannot also take:

- WM055-10 Information Risk Management and Governance

Courses

This module is Core optional for:

- Year 1 of TWMA-H6C7 Postgraduate Taught Cyber Security Engineering