WM9QQ-15 Cyber Security Audit

26/27

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

Description

Introductory description

This module aims to provide a comprehensive and critical understanding of Cyber Security Auditing, primarily using ISO 27001(Information Security standard) and ISO 19011 (Management systems auditing standard). Students will learn how to set up full programmes to effectively and comprehensively assess information security management systems over a set period in compliance with the requirements of ISO27001. They will further learn how to justify and continually improve the audit programmes they produce.
We will examine the roles of external auditors and explore the importance of external audit for the stakeholders of an organisation.
A variety of techniques will be utilised to teach students how to set up and prepare audits, how to conduct them, how to deal with problems that may arise, how to conduct themselves in a variety of real-life audit situations and how to apply critical thinking to audit scenarios in order to produce useful, effective and accurate audit reports.
Students will learn a number of auditing techniques and approaches and the pros and cons thereof. In particular we will focus on using the auditees own risk assessments and security policies and objectives to educate and facilitate our auditing.
This module will include practical exercises based on real world case studies in managing and consulting on cyber security systems, and auditing organisations for compliance to international standards.
Students will gain an appreciation of the regulatory framework in which auditors operate, apply this

knowledge to case study situations and evaluate the procedures used by auditors. As well as considering the processes of both internal and external audit, the module explores the profession of auditing, looking at how the professional firms operate, and profession-wide issues such as audit quality, ethical behaviour, as well as economic and political pressures.

Module aims

The aim of the module is to enable students to understand the nature and objectives of the audit function. They will also appreciate the issues and complexities of the audit process and the principles of audit practice.
Students will gain a detailed understanding of relevant ethics, principles and rules of cyber security, data protection, consent and privacy. There is an emphasis on auditing against the organisation's own Information security management system and the requirements of ISO27001.

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.

The module will include some of the following topics:

- The role of the external auditor: An introduction to, and evaluation of, the ethical and regulatory framework in which audit operates. ISO19011
- The process of an external audit: initial client and engagement acceptance, the method of planning an audit and performing key audit techniques, risk assessment, obtaining audit evidence and reporting audit findings, addressing a range of practical and theoretical issues.
- The application of critical thinking to audit scenarios. The ability to identify the clear evidence of non-conformity and present it such that the finding is unarguable.
- The completion stage of the audit: presentation and agreement on findings, the auditor’s report and types of audit reports.
- Current issues in audit risk and audit quality.
- The relationship between external and internal functions and the role of audit in corporate governance.
- Auditor behaviour and attributes

Learning outcomes

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

- Demonstrate critical appreciation of the need for external and internal audit, and evaluate different approaches to auditing.
- Evaluate the main processes of internal and external audit, and assess whether an engagement has been appropriately accepted, planned and performed.
- Carry out all aspects of a cyber security audit within a specific scope and in compliance with the relevant standards.
- Analyse on areas of difficulty in auditing and consider how the profession can or should react to developments in business practice and economic situations.

Indicative reading list

Reading lists can be found in Talis

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.

Subject specific skills

- The relationship between external and internal functions and the role of audit in corporate governance.
- Apply audit regulations to practical business scenarios.
- Recognise factors which impact on audit quality.
- Develop professional scepticism and question information provided when appropriate.
- The audit process including planning an external audit, risk assessment, obtaining audit evidence and reporting audit findings, addressing a range of practical and theoretical issues.

Transferable skills

Critical and analytical thinking, problem solving, communication, professionalism as well as:

- Themes which underpin audit quality, including the application of professional ethics.
- Auditor behaviour and attributes, including the use of professional scepticism and professional judgement.
- Current issues in audit, for example auditor liability and the expectation gap.
- Apply logical reasoning to justify actions to be taken by auditors in a given situation.

Study

Study time

Type	Required
Supervised practical classes	30 sessions of 1 hour (20%)
Online learning (independent)	10 sessions of 1 hour (7%)
Private study	50 hours (33%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Research on and analysis on additional learning resources.

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
Cyber Security Audit Test	20%	12 hours	No
In-class test assessing the students' critical understanding of the relevant standards, frameworks and the audit process.			
Cyber Security Audit	80%	48 hours	Yes (extension)
A non-conformity report presenting the results of a cyber security audit carried out on a given case study. The assessment will include an interview carried out as part of the cyber security audit. (The students will be the auditors, i.e. interviewers, and the module tutor will be representing the audited organisation).			

Assessment group R1

	Weighting	Study time	Eligible for self-certification
Cyber Security Audit Test	20%		No
Cyber Security Audit	80%		No

Feedback on assessment

Feedback will be provided on a standard WMG feedback form.

Availability

Courses

This module is Core optional 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)