

WM9B9-15 Cyber Security Consultancy

26/27

Department

WMG

Level

Taught Postgraduate Level

Module leader

Sarah Aktaa

Credit value

15

Module duration

4 weeks

Assessment

100% coursework

Study location

University of Warwick main campus, Coventry

Description

Introductory description

Cyber security consultants are required to apply analytical, decision-making, and communication skills to provide reliable advice to clients. Quite often they report progress and outcomes to stakeholders, which include those who are able to understand technical terms, descriptions, and explanations, and those who are not always able to understand these. Consultants must possess strong leadership skills, enhanced project management skills, organisation and management skills and possess the knowledge and confidence to make effective leadership interventions within a cyber security context.

Module aims

The module will expose participants to realistic experiences of the work that a cyber security consultant is involved with. The module will develop a thorough understanding of the cyber security consultancy lifecycle, which typically involves presales, execution, and closure. Students will work on an industry-supplied consultancy project. Participants will work in their respective project teams to deliver the project and, in so doing, will undertake tasks such as:

- Elucidating, organising and categorising client requirements.
- Undertaking role and work allocation.

- Organising and managing the scheduling of the project to ensure successful and timely delivery.
 - Organising and managing finances related to the project, both in terms of cost to client and internal costs.
 - Undertaking and delivering the project.
 - Reporting on the project at specified points.
- Participants will be expected to keep a shared portfolio of work and conduct professional 'minuted' meetings with their teams, and utilise appropriate technology (for example, Microsoft Teams) to support project progress and communication.

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 role of a consultant. The strategic context setting of Cyber Security; the culture of cyber security; roles in an enterprise; human factors in cyber security; roles and responsibilities within a cyber team; security professionalism; security culture and raising cyber awareness;
- Managing consultancy projects. The consultancy life cycle; elucidating requirements; planning, developing, controlling, and delivering consultancy projects; developing consultancy proposals; consultancy tools, skills, and techniques; dealing with uncertainty such as vague specifications and rapidly changing environments.
- Managing cyber security projects from a system, application, and physical security viewpoint. Identity management: authentication, access control and privilege management; securing compute environments and applications; Email, web and database security; social networks; DRM; database security; big data security; physical and environmental controls; physical protection of IT assets.
- Responsible and secure implementation of AI for different platforms and organisations.
- Explore the role of security consultants in designing and implementing emerging technologies such as Web3, quantum computing, and block chain.

Learning outcomes

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

- Adapt and innovate to solve problems and manage unpredictable situations, making sound judgements in the absence of complete data.
- Demonstrate the ability to work collaboratively using self-direction and initiative, applying planning, organisational and budgeting skills appropriately.
- Demonstrate effective professional relationship skills, including negotiation, facilitation and communication.
- Formulate and deliver logical and precise arguments for organisational decision makers.

Indicative reading list

[Reading lists can be found in Talis](#)

[Specific reading list for the module](#)

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 a small emphasis on the interdisciplinary nature of the subject. The key transferable skills acquired in this module, namely project management, budget management, time management, and resource management, are key skills that are applicable across a range of disciplines.

Subject specific skills

Participants will develop a detailed applied knowledge of the day-to-day work of a cyber security consultant and the process of managing consultancy projects.

Transferable skills

Self-awareness, communication, teamwork, sustainability, intercultural awareness, professionalism, organisational awareness.

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (11%)
Tutorials	20 sessions of 1 hour (22%)
Online learning (independent)	5 sessions of 1 hour (6%)
Private study	55 hours (61%)
Total	90 hours

Private study description

The students are required to work on their coursework.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A2

	Weighting	Study time	Eligible for self-certification
Assessment component			
Group Report	80%	48 hours	No
Working in small groups, students will research and analyse a complex cyber security management problem. The project requires a comprehensive group report, assessing the group's collective understanding and ability to apply theory to practice. Peer adjustment will be applied to individual marks within the group to reflect individual contribution.			

Reassessment component

Individual Report	No
-------------------	----

This is an individual reassessment for students who have failed the group project component. It requires a single student to independently research, analyse, and write a report on a complex cyber security management problem with a different scenario to the original group project.

Assessment component

	Weighting	Study time	Eligible for self-certification
Individual reflection	20%	12 hours	Yes (extension)
Each student will submit a reflective piece evaluating their personal learning journey, their contribution to the group project, and the module's relevance to professional practice. This assessment fosters individual accountability and deep, reflective learning.			

Reassessment component

Individual reflection	No
Each student will submit a reflective piece evaluating their personal learning journey and the module's relevance to professional practice. This assessment fosters individual accountability and deep, reflective learning.	

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-H1SH Postgraduate Taught Cyber Security Management (Full-time)