WM3E1-15 Information Assurance

26/27

Department
WMG
Level
Undergraduate Level 3
Module leader
Maria Papadaki
Credit value
15
Module duration
12 weeks
Assessment
100% coursework
Study locations
University of Warwick main campus, Coventry Primary
Distance or Online Delivery

Description

Introductory description

Information assurance is defined by NIST as " Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." This module is grounded within the Authentication, Authorisation & Accountability Knowledge Area CYBOK (cyber security body of knowledge). The module aligns closely with the CYBOK KA and readers are referred to the CYBOK for more information on technical content covered within the module. The CYBOK KA is also the main reading list item.

In certain scenarios, IT systems are engineered to prevent undesirable behaviour completely. Conversely, some IT systems are designed with a high degree of flexibility, necessitating additional measures to control undesirable behaviour based on specific circumstances. As highlighted by Lessig, this control can be achieved either by coding within the system to prohibit rule-violating behaviour or by establishing codes of conduct for users to follow. In the latter case, disciplinary or legal actions address those who breach the rules, framing the context for authentication, authorization, and accountability.
While readers familiar with academic conventions might anticipate precise definitions and current methodologies regarding authentication, authorization, and accountability, this conventional

approach faces an immediate challenge. These terms suffer from overloading, leading to potential confusion and debate. For instance, authorization encompasses both rule establishment and compliance verification. Therefore, readers should approach literature on this Knowledge Area with caution.
Moreover, the evolving landscape of IT usage poses its own challenges to taxonomies. How closely should terms be anchored to their original contexts? There's a tendency in trade and research literature to associate terms solely with traditional conceptualizations while inventing new terminology for emerging environments, even if the underlying concepts remain unchanged.

Module web page

Module aims

The module focuses on the discipline of Information Assurance and compliance, encompassing its associated theories, practices, and principles governing modern information systems within multi-disciplinary structures, processes, and procedures. Special attention is given to frameworks, standards, and strategies for managing an organization's information assets, ensuring compliance with legal and regulatory requirements.

The objective of this module is to enable students to systematically address threats, vulnerabilities, and their potential negative consequences in an organization's daily cyber activities. Students will learn to establish and maintain a risk management framework, providing assurance that information security and assurance strategies align with business objectives and meet legal and regulatory obligations. Various approaches to information risk management and resolution will be examined for a simplified system, with an emphasis on practical application and addressing real-world managerial challenges.

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.

Understanding authentication, authorisation & accountability, and the role they play in information assurance.
Access Control
Biometrics and other access control systems
SAML
OAUTH2
DRM
Auditing

Encryption

- terminology: hash, digest, Message Authentication Code, function
- properties: irreversible, deterministic, collision resistance, length
- applications in the cybe domain- authentication, known good/ bad files, file integrity,
- attacks- brute force, rainbow tables, password salting/ stretching, collisions
- specific hashes- MD5 (and collisions), SHA1, SHA2** series

- practical application of specific algorithms to specific tasks

Encryption theory:

- terminology: plaintext, ciphertext, key, algorithm, protocol,
- concepts: entropy, one time pad, complexity, modular arithmetic, initialisation vectors

Symmetric encryption:

- encryption over distance or time- the key exchange problem
- example algorithms- DES, Triple DES, AES,

Asymmetric encryption:

- properties- encrypting for known recipient, signing by authentic sender,
- establishing trust- hierarchy (X509) and web (OpenPGP), certificates,
- consequences of loss of key control- revocation certificates.

Hybrid encryption:

- Using asymmetric encryption to share symmetric key,
- SSL/TLS

Other specific protocols:

- Kerberos.
- IPSEC.

Learning outcomes

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

- Apply cryptosystem based solutions to information assurance problems. [CITP:2.1.7]
- Develop processes designed to assess the reliability of technologies and processes. [CITP:2.1.11]
- Develop robust information assurance strategies. [CITP:2.1.5] [AHEP:4-C9]
- Using different methods to communicate information assurance concepts and technologies to lay people. [CITP:2.1.13] [AHEP4:-C10, C17]

Indicative reading list

Reading lists can be found in Talis

Subject specific skills

This module covers the following Knowledge and Skills based on the latest published DTS DA standard:
-- S2: Identify risks, and determine mitigation strategies and opportunities for improvement in a

digital and technology solutions project.
-- S41: Undertake security risk assessments for complex systems without direct supervision and propose a remediation strategy relevant to the context of the organisation.
-- S42: Recommend improvements to the cyber security approaches of an organisation based on research into future potential cyber threats and considering threat trends.
-- S44: Use appropriate cyber security technology, tools and techniques in relation to the risks identified.

In addition, the module covers these skills:

- Rationalise the selection of information assurance strategies for economical deployment, by industry standards.
- Participate actively in the investigation throughout the educational journey, exploring information assurance management frameworks, technologies, and tools within authentic scenarios, assessing and contrasting their efficacy, and dissecting outcomes.
- Acquire proficiency in developing information assurance strategies pertinent to business activities within practical cyber security contexts, to grasp the fundamental principles of information assurance management, and the methodologies and infrastructures employed for their execution.

Transferable skills

team working
leadership
communication skills
decision making

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (12%)
Practical classes	20 sessions of 1 hour (24%)
Work-based learning	15 sessions of 1 hour (18%)
Online learning (independent)	10 sessions of 1 hour (12%)
Other activity	5 hours (6%)
Private study	25 hours (29%)
Total	85 hours

Private study description

The private study can include revision of module contents, solution of additional seminar-type questions, video tutorials and supplementary materials.

Other activity description

- Pre-module reading list given on Moodle to encourage flipped learning approach.
- Preparation for the practical activities.

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			
Coursework	60%	36 hours	Yes (extension)
Implementation of a crypto based solution to an information assurance problem with report submitted on completion.			
Reassessment component			
Coursework			No
Implementation of a crypto based solution to an information assurance problem with report submitted on completion.			
Assessment component			
Coursework	40%	24 hours	Yes (extension)
Development of a strategic solution to an information assurance problem. The report is aimed at senior exec in an organisation.			
Reassessment component			
Coursework			No
Development of a strategic solution to an information assurance problem. The report is aimed at			

	Weighting	Study time	Eligible for self-certification
senior exec in an organisation.			

Feedback on assessment

Feedback will be given as appropriate to the assessment type:

- formative feedback for the assignment,
- verbal feedback during tutorial & lab sessions,
- Solutions provided to tutorial questions,
- summative feedback on post module assessment & exam.

Availability

Courses

This module is Core for:

- Year 3 of DWMS-H652 Undergraduate Digital and Technology Solutions (Data Analytics) (Degree Apprenticeship)
- Year 3 of DWMS-H654 Undergraduate Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)