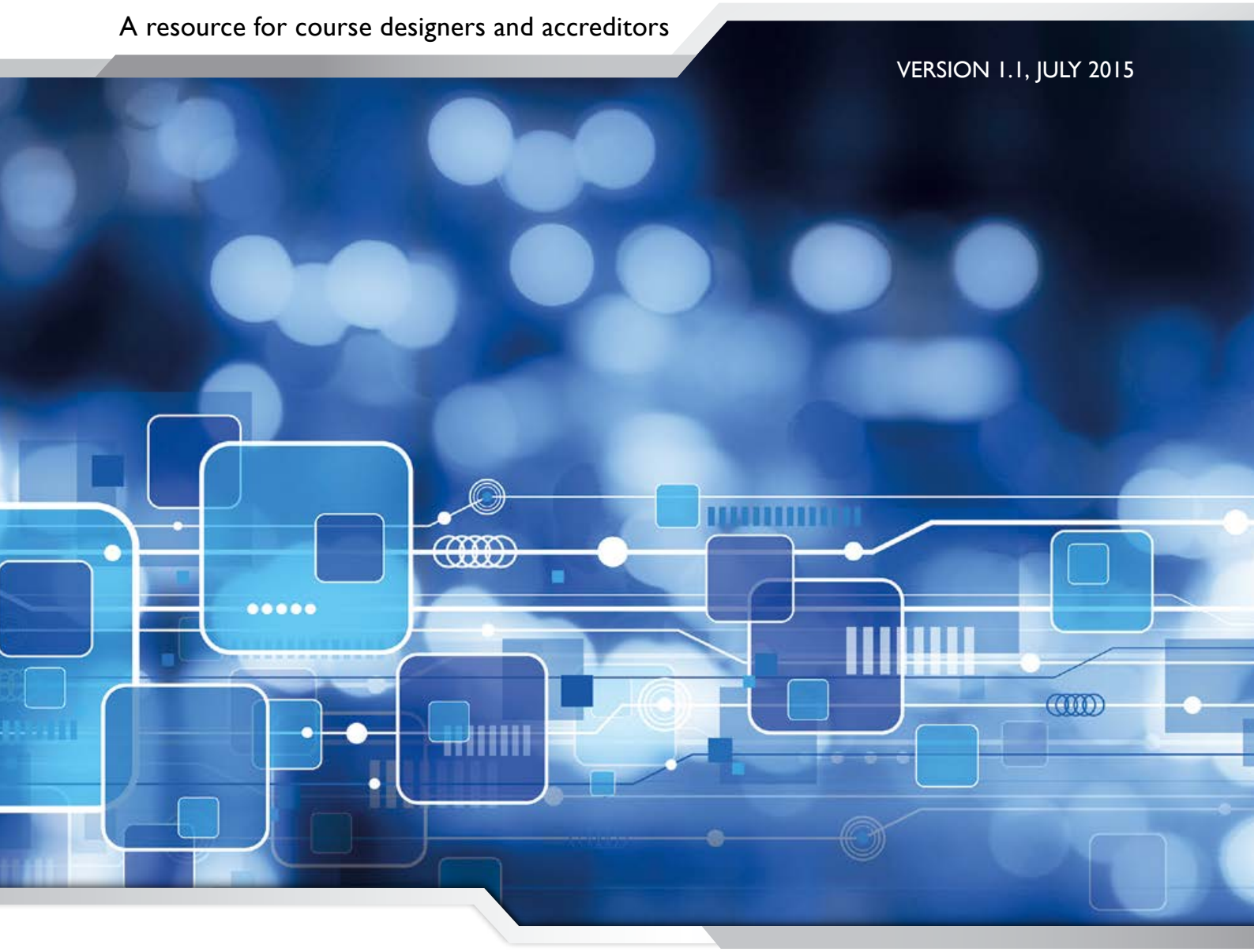
CYBERSECURITY PRINCIPLES AND LEARNING OUTCOMES
FOR COMPUTER SCIENCE AND IT-RELATED DEGREES

A resource for course designers and accreditors

VERSION 1.1, JULY 2015



(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

CPHC
The Council of Professors and Heads of Computing

CONTENTS

INTRODUCTION

Information has never been so ubiquitous, valuable, or available. However, with the significant growth in information created, stored, processed and transmitted across Information Technology (IT) systems and networks – often of a sensitive or personal nature – comes the need to protect that information from a range of threats. Similarly the infrastructure that we come to rely on in business, government and society – whether it be for communications, utility, public or business service – must be protected from these threats as it is typically controlled by information that is processed and transmitted across IT systems, IT-enabled control systems and networks. The threats can range from professional criminals making their living from stealing information to well-intentioned employees or individuals making mistakes in the way they use applications or IT, or acts of social protest and terrorism.

Protecting information along with the IT systems, control systems, networks and devices processing that information is now recognised as an industry, a profession and an academic discipline in its own right. However, IT systems, control systems, networks, websites and applications are typically designed or built by people who do not give adequate consideration for this need. As a result, IT systems, control systems, networks, websites and applications typically: contain well-known errors; are deployed with well-known default settings that leave the systems open to exploit; and leave the information and organisations they support vulnerable to compromise. This situation has given rise to an acknowledged and growing prevalence of attack, compromise and loss, fuelling recognition for the need to develop cybersecurity knowledge and skill within the disciplines responsible for networks and IT systems, including within the academic courses that lead or prepare students to pursue a career in these areas.

$(ISC)^2$, the largest not-for-profit membership body of certified information and software security professionals worldwide, with over 100,000 members and The Council of Professors and Heads of Computing (CPHC), brought together a wide-ranging group of industry and academic experts to identify the key concepts related to cybersecurity that can be embedded across undergraduate computing science and IT-related (e.g. business information systems and IT management for business) degree courses. This guide is the result of this effort, designed to help enrich those computing courses by providing the key cybersecurity principles and suggested learning outcomes.

The concepts covered here are outlined for five themes: information and risk; threats and attacks; cybersecurity architecture and operations; secure systems and products; and cybersecurity management, to satisfy Level 4 requirements as stated in The framework for higher education qualifications in England, Wales and Northern Ireland August 2008. Advanced concepts and further learning outcomes are also provided for each theme, so that academic institutions can develop or enhance their courses to meet Level 5 and 6 requirements of the framework. The descriptors for all three levels (4 – 6) are presented in Annex A. They are developed to support accreditation guidelines used by BCS, The Chartered Institute for IT (BCS) and Institution of Engineering and Technology (IET).

ACCREDITATION GUIDELINES

Working with BCS, the Chartered Institute for IT, explicit advice addressing core systems and information security concepts have been added to enhance the guidance that accreditors use in their assessment of computing and computing science degrees. This document has been developed to provide detailed support for this advice.

For BCS, The Chartered Institute for IT accreditation guidelines[1] state that courses should address:

- *The ability to recognise the legal, social, ethical and professional issues involved in the exploitation of computer technology and be guided by the adoption of appropriate professional, ethical and legal practices*
- *Knowledge and understanding of information security issues in relation to the design, development and use of information systems*

This resource provides new information to complement the above guidelines, which is summarised below:

For a given computer technology development or information system – such as an individual service, application, server, network device, laptop, smartphone or network or combinations thereof – students will be expected to show knowledge and understanding of the core concepts and principles within the following themes where this is relevant to the Programme Learning Outcomes under consideration:

1. **Information and risk:** models including confidentiality, integrity and availability (CIA); concepts such as probability, consequence, harm, risk identification, assessment and mitigation; and the relationship between information and system risk
2. **Threats and attacks:** threats, how they materialise, typical attacks and how those attacks exploit vulnerabilities
3. **Cybersecurity architecture and operations:** physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify and mitigate vulnerability, and ensure organisational compliance
4. **Secure systems and products:** the concepts of design, defensive programming and testing and their application to build robust, resilient systems that are fit for purpose
5. **Cybersecurity management:** understanding the personal, organisational and legal/regulatory context in which information systems could be used, the risks of such use and the constraints (such as time, finance and people) that may affect how cybersecurity is implemented.

It is commonly recognised that information security concerns are most appropriately addressed as integral rather than as an add-on to the design of information systems. As a consequence, the teaching of security issues is ideally embedded across computing and IT-related subject areas.

Approaches using specific application, for example the specifying of requirements for CIA of personally identifiable information being stored and/or processed by a system or the use and analysis of threat data in the selection of security arrangements, are recommended.

Annex B presents the applicability of the five themes to meet current BCS accreditation guidelines.

[1] BCS, The Chartered Institute for IT, *Guidelines on course accreditation, Information for universities and colleges.*

USING THIS RESOURCE

This document is designed to provide course designers with a manual to help them embed cybersecurity into degree modules and associated syllabi. Here five cybersecurity themes are described for inclusion into Computing Science and IT-related degrees, along with their associated core concepts, principles and learning outcomes. We recognise that computing and IT-related degrees vary in their focus and content and that not all the material presented here may be suitable or required across all degrees.

We suggest that course designers can use this resource in five ways:

1. To validate that the cybersecurity content currently embedded in degree courses covers the material presented here
2. To identify areas where their cybersecurity teaching can be further embedded, enhanced or strengthened
3. To add the themes into non-cybersecurity modules (e.g. database or software engineering) offered as part of undergraduate degrees
4. To add core concepts into non-cybersecurity modules offered as part of undergraduate degrees
5. To create a cybersecurity module to complement embedded content that can be offered as part of an undergraduate degree.

For accreditors, this resource is designed to provide them with concepts, examples and outcomes that can be investigated and assessed during the accreditation process.

Embedding into current degree curricula/syllabi

This booklet does not include guidance on the manner (such as lecture, self-study, tutorial or lab) and duration of any teaching on the themes. Instead, there are stated learning outcomes that the contributors believe should be attained. How these outcomes are achieved are left to the discretion of the staff at each academic institution. For each theme, the outcomes are stated for Level 4. If an institution wishes to teach its students more demanding concepts and principles, advanced concepts and further learning outcomes are also stated. Whether the additional outcomes should be attained at Level 5 or 6 is deliberately not indicated, leaving this decision to the discretion of the staff at each academic institution as well.

We provide examples of how to apply the themes to computing science degree modules in Annex C and in table 1.

Table 1: Example application of the themes to course modules by Year

Year 1 – example modules	*Applicable themes*	Year 2 – example modules	*Applicable themes*	Year 3 – example modules	*Applicable themes*
Fundamentals of Comp Sci.	*Information and risk*	Operating Systems	*Information and risk* *Threats and attacks* *Secure systems and products* *Cybersecurity architecture and operations*	Project	*As appropriate*
Digital Systems	*Information and risk*	Database Systems	*Information and risk* *Threats and attacks* *Secure systems and products* *Cybersecurity architecture and operations*	Electives	
Programming	*Information and risk* *Threats and attacks*	Software Design/ Engineering	*Information and risk* *Threats and attacks* *Secure systems and products* *Cybersecurity architecture and operations*	Security	*All apply*
Software Development	*Information and risk* *Threats and attacks* *Secure systems and products*	Computer networks	*Threats and attacks* *Cybersecurity architecture and operations*		

For each of the modules presented here, the course designer can select the core concepts, principles and learning outcomes to match the level of the course and the topics covered.

Use of themes and their structure

Each theme contains core concepts, example techniques and technologies and learning outcomes. Advanced concepts and further learning outcomes are also presented. The diagram below explains each of these components in detail:

Figure 1: Theme components

Core concepts	The fundamental concepts and principles of the theme
Example terms, techniques and technologies	Published terms, definitions, methodologies, tools and technology that can be used to illustrate the application and implementation of the concepts, aid student understanding and address the risks listed
Learning outcomes	The understanding and knowledge of the core concepts expected of a student at Level 4
Advanced concepts	Building on the core concepts, these present a richer, wider view of the theme
Further learning outcomes	More advanced understanding and knowledge expected of a student (Level 5 and/or Level 6)

Where possible, each theme is designed to stand alone from the others. The core concepts and outcomes from one theme can be combined with those from another theme if that approach is better suited to their style of teaching and the current course structure, or the concepts from the themes can be taught in existing modules.

THEME: INFORMATION AND RISK

Information – in all its forms – is a vital component of the digital environment in which we live and work. The protection of information in its physical form is well understood but the protection of digital information within systems and devices – and what needs to be protected – is less so. Information risk is concerned with the importance of information to the organisation and the harm that can be caused from the failure to manage, use or protect information in all its forms. Risk management allows an organisation to prioritise risks, deploy resources efficiently and to treat risks using a consistent and documented approach taking into account threats, vulnerabilities, assets and harm. System risk needs to be understood and actively foreseen and managed within this context.

Core concepts

Utility and value of information and data	Risk and hazard
Classification of information	Impact, harm and consequence
Information/data life cycle	Information risk process
Attributes of information, data and systems	Risk taking, human error, naïveté, malicious drivers
Information systems	

Example terms, techniques and technologies

The confidentiality, integrity and availability triad (CIA)	Core steps in the information risk management process: ■ Identification ■ Organisation Impact Assessment ■ Threat and vulnerability analysis ■ Treatment options ■ Control selection ■ Measurement/monitoring ■ Review
Parkerian Hexad	
Access management	
Authentication, authorisation, auditing and non-repudiation	
Simple classification schemes	
Risk and associated terminology, such as likelihood, probability, harm and impact	

Learning outcomes

Students should understand that information: ■ is an organisational asset that has utility, and a value – which may be relative depending on the perspective taken, and therefore can be classified to reflect its importance to an organisation or individual ■ is vulnerable to threats in systems ■ has the attributes relating to confidentiality, possession or control, integrity, authenticity, availability, and utility, any of which can make it vulnerable to attack	■ may need to be protected – and some of the reasons why that protection must occur (for example, legal and regulatory drivers, customer rights or organisation objectives) ■ has a lifecycle – from creation through to deletion – and protection may be required and may change throughout that lifecycle ■ that information risk management is a term referring to the process of documenting what information is at risk, type and level of risk realised; and the impact of realisation

Theme: Information and risk continued...

Advanced concepts	
Information risk management as part of an organisation's overall risk management Risk landscape and threat categories System risk, Residual risk	Risk management standards, such as: NIST SP800-30; Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE); CCTA Risk Analysis and Management Method (CRAMM); ISO 31000; ISO/IEC 27005 Quantitative and qualitative approaches to risk management
Further learning outcomes	
The student should understand: ■ the concept of a risk landscape, its dynamic nature and how to create a landscape for an organisation ■ how to classify threats – and example categories system risk – its components and interactions with information risk ■ the concept of residual risk and what it means for an organisation	■ that criteria can be used to assess the suitability of risk management approaches for an organisation, including quantitative approaches such as Annualised Rate of Occurrence (ARO), Single Loss Expectancy (SLE) & Annualised Loss Expectancy (ALE) and qualitative expressions of risk such as heat maps and Likert scales

THEME: THREATS AND ATTACKS

Information, services and systems can be attacked in various ways. Understanding the technical and social perspectives, how attacks work, the technologies and approaches used are key to being able to protect against attacks.

Core concepts	
Threats	Typical targets
Vulnerabilities	Social engineering; mind-sets of hackers
Attack vectors (routes of attack) on information and the systems that process, store and transmit information	Targeted attacks
Example terms, techniques and technologies	
Characterisation/classification of threats (for example by using the PLEST – political, legal, economic, socio-cultural and technical – framework)	Typical attacks (e.g. Distributed Denial of Service (DDOS), phishing, buffer overflow and social engineering) and targets (e.g. people, databases, credentials)
Vulnerabilities, defects and bugs	Sources of information: Verizon Data Breach Incident report, SANS Top 20 Critical Security Controls / Defence Signals Directorate (DSD) Top 35 Strategies to Mitigate Targeted Cyber Intrusions/ Open Web Application Security Project (OWASP) top 10/ BugTraq
Attack process and methodology (reconnaissance, scanning, creation, test, attack/gain access, exfiltration & exiting)/kill chain	User behaviour and awareness
Learning outcomes	
Students should be able to understand: ■ the difference between threat, risk, attack and vulnerability ■ how threats materialise into attacks ■ where to find information about threats, vulnerabilities and attacks ■ typical threats, attacks and exploits and the motivations behind them	■ high-level understanding of how example attacks work (e.g. DDOS, phishing and buffer overflow) ■ how users are targeted in an attack and why this must be considered in defending against such attacks
Advanced concepts	
Threat landscape	Combined attacks
Attack patterns and methodologies	Attacks on infrastructure, Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA), cyber-physical systems
Malware types and their detailed mechanism of operation	
Further learning outcomes	
The student should understand: ■ the concept of a threat landscape, its dynamic nature and how to create a landscape for an organisation ■ how to classify threats – and example categories ■ that there are different attacks, which have different patterns and different steps – for example be able to compare a DDOS to an attack designed to copy information	■ that there are different types of malware – for example viruses, Trojans and spyware – their distribution mechanism and a detailed understanding of how they compromise information and systems ■ that attacks can be combined for greater effect (e.g. phishing email, followed by social engineering phone call)

THEME: CYBERSECURITY ARCHITECTURE AND OPERATIONS

The protection of information, services and systems relies on a range of technical and procedural activities, often grouped in a framework. The framework will contain technical and logical, physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify and mitigate vulnerability, and satisfy compliance obligations.

<table>
<tr><th colspan="2">Core concepts</th></tr>
<tr><td>Service continuity and reliability</td><td>Defence in depth</td></tr>
<tr><td>Security architecture</td><td>Operational fundamentals of technical controls</td></tr>
<tr><td>People, Process and Technology</td><td>Testing and monitoring</td></tr>
<tr><td>Control</td><td>Usability, awareness and behaviour</td></tr>
<tr><th colspan="2">Example terms, techniques and technologies</th></tr>
<tr><td>Controls are developed and managed across four areas:
1. Physical controls (such as fences, barriers and building design)
2. Process/operational controls (such as separation of duties, least privilege, due care, due diligence and access management)
3. Logical controls (such as access management, firewalls, anti-virus software and patch management)
4. Technical controls operation (e.g. authentication, authorisation, basics of cryptography, firewall operation and IPSec)</td><td>Monitoring and analytics
Testing Systems Controls and overall Penetration testing
Systems updates
Vulnerability scanning
Usability, error and awareness
Management frameworks, e.g. ISO/IEC 27001; Architectural frameworks, e.g. Sherwood Applied Business Security Architecture (SABSA), The Open Group Architecture Framework (TOGAF)</td></tr>
<tr><th colspan="2">Learning outcomes</th></tr>
<tr><td>Students should be able to:
■ highlight the need for security architecture and its relevance to systems, service continuity and reliability
■ discuss the application of techniques such as defence in depth to demonstrate how controls can be selected, deployed and tested to minimise risk and impact</td><td>■ differentiate between controls to protect systems availability and reliability; controls to protect information; and controls to manage human behaviour
■ understand the trade-offs for functionality, usability and security
■ understand the role of operations in monitoring, maintaining and evolving controls</td></tr>
<tr><th colspan="2">Advanced concepts</th></tr>
<tr><td>Types of control – preventative, detective, reactive, corrective compensating controls
More on technical controls, such as cryptography, access management and network security devices, and how they work</td><td>Incident handling, response and recovery
Principles of business/service continuity and disaster recovery as they relate to architecture and operations
Forensics and investigations</td></tr>
</table>

Theme: Cybersecurity architecture and operations continued...

Further learning outcomes	
The student should understand: ■ that controls can be categorised and selected on the basis of that categorisation ■ where technical controls cannot be used, other controls can be selected ■ how technical controls (examples include cryptography, access management, firewalls, anti-virus software and intrusion prevention systems) work in detail/at an advanced level of understanding ■ how the technical controls can be deployed in practice – and associated strengths and weaknesses	■ the role of forensics and investigations in revealing how an attack was carried out and understand how to support investigations ■ the key steps in managing incidents ■ the components and steps of a Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) (e.g. ISO/IEC 27031) and understand how to support BCP/DRP measurement of recovery – Recovery Time Objective (RTO) /Recovery Point Objective (RPO)/ Maximum Tolerable Downtime (MTD)

THEME: SECURE SYSTEMS AND PRODUCTS

This theme examines the process of building security into a system (such as an individual service, application, server, network device, laptop, smartphone or network or combinations thereof) from the concept stage to decommissioning and disposal. It looks at the concepts of design, defensive programming and testing and their application to build robust, resilient systems that are fit for purpose.

Core concepts	
Systems and software design, build and testing	Systems hardening
Software and systems Development Lifecycle	Usability; security requirements for functional design
Vulnerability and misuse	Communications, remote access/control and connectivity
Security within quality assurance	
Example terms, techniques and technologies	
Secure Software, systems and product lifecycles Requirements analysis for: 1. Information, service and systems attributes 2. Security controls – physical operational, logical and technical 3. Usability, user error and behaviour 4. Availability/risk appetite – fault tolerance, load balancing, attack vectors	Secure implementation of systems and services Component libraries/input testing Use and misuse testing; penetration testing Defensive programming
Outcomes	
The student should be able to: ■ understand the concepts that must be considered in requirements analysis and explain the importance of "building security in" ■ highlight the key steps in a design process and where security considerations should be worked in	■ explain how security controls can be implemented to protect systems and information ■ describe defensive programming and cite examples such as input checking ■ identify common trade-offs and compromises that are made in the design and development process
Advanced concepts	
Designing for Resilience – definition Designing for damage limitation; fault tolerance, etc.	Standards for secure and trustworthy software design (e.g. Capability Maturity Model (CMM), BS PAS 754, Building Security In Maturity Model Software Security Framework (BSSIM SSF), Open Web Application Security Project (OWASP), ISO/IEC 27034 series)
Additional outcomes	
The student should be able to: ■ provide examples of resilient information systems ■ highlight techniques available to provide resilience	■ illustrate the use of standards to enhance security in the development process

THEME: CYBERSECURITY MANAGEMENT

The protection of information does not occur in a vacuum: it is intimately tied to the organisation and its requirements, the legal and regulatory environments in which the organisation trades and to the efforts and abilities of individuals in handling information correctly.

Core concepts	
Managing information protection in organisations	Assessment, analysis and management of risk
Organisational culture, accountability and employee expectations	Security as an ethical issue within IT practice
Compliance	Balance of opportunity and security – and the trade-offs required
Policy and strategy	
Example terms, techniques and technologies	
Use of standards to create a management framework (e.g. ISO/IEC 27001 Information Security Management System, ISO/IEC 27005 risk management)	Tools for managing security: policies, standards/ baselines, procedures and guidelines
Cybersecurity strategies, programmes	User behaviour and awareness
Learning outcomes	
The student should demonstrate: ■ knowledge of a management framework and identify commonly used standards and areas of best practice ■ ability to place security in an organisational context ■ respect for organisational needs, other individuals and confidential (often personal) information ■ understanding of the need to provide a positive security influence	■ ability to describe the various tools that can be used in cybersecurity management ■ an understanding of compliance and its importance ■ awareness of ethical concerns ■ the key factors to consider when creating an awareness or user education programme
Advanced concepts	
Security and information assurance within IT governance	Information security in the supply chain
Privacy	Resilience
Disaster recovery Business continuity management and plans – e.g ISO 22301 and ISO/IEC 27031	Advanced analytics – types and value of systems and security information
Further learning outcomes	
The student should understand: ■ key elements of governance and its role ■ standards such as ISO/IEC 27014 cybersecurity governance, ITGI Information Security Governance, the ISO/IEC 27036 series ■ privacy as a special form of information protection, and that privacy and cybersecurity are linked	■ privacy has a legal and regulatory aspect – with obligations and requirements on individuals and organisations ■ what resilience means, and how to take a structured approach to managing security risks, business continuity, and information technology operations within the context of an organisation's objectives.

ANNEX A: FHEQ DESCRIPTORS FOR LEVELS 4, 5 AND 6[1]

Descriptor for a higher education qualification at level 4: Certificate of Higher Education

The descriptor provided for this level of the FHEQ is for any Certificate of Higher Education which should meet the descriptor in full. This qualification descriptor can also be used as a reference point for other level 4 qualifications.

Certificates of Higher Education are awarded to students who have demonstrated:

- knowledge of the underlying concepts and principles associated with their area(s) of study, and an ability to evaluate and interpret these within the context of that area of study
- an ability to present, evaluate and interpret qualitative and quantitative data, in order to develop lines of argument and make sound judgements in accordance with basic theories and concepts of their subject(s) of study.

Typically, holders of the qualification will be able to:

- evaluate the appropriateness of different approaches to solving problems related to their area(s) of study and/or work
- communicate the results of their study/work accurately and reliably, and with structured and coherent arguments
- undertake further training and develop new skills within a structured and managed environment.

And holders will have:

- the qualities and transferable skills necessary for employment requiring the exercise of some personal responsibility.

Holders of a Certificate of Higher Education will have a sound knowledge of the basic concepts of a subject, and will have learned how to take different approaches to solving problems. They will be able to communicate accurately and will have the qualities needed for employment requiring the exercise of some personal responsibility. The Certificate of Higher Education may be a first step towards obtaining higher level qualifications.

Descriptor for a higher education qualification at level 5: Foundation Degree

The descriptor provided for this level of the FHEQ is for any Foundation Degree which should meet the descriptor in full. This qualification descriptor can also be used as a reference point for other level 5 qualifications, including Diplomas of Higher Education, Higher National Diplomas, etc.

[1] Excerpted from QAA, *The framework for higher education qualifications in England, Wales and Northern Ireland August 2008*, August 2008

Foundation Degrees are awarded to students who have demonstrated:

- knowledge and critical understanding of the well-established principles of their area(s) of study, and of the way in which those principles have developed
- ability to apply underlying concepts and principles outside the context in which they were first studied, including, where appropriate, the application of those principles in an employment context
- knowledge of the main methods of enquiry in the subject(s) relevant to the named award, and ability to evaluate critically the appropriateness of different approaches to solving problems in the field of study
- an understanding of the limits of their knowledge, and how this influences analyses and interpretations based on that knowledge.

Typically, holders of the qualification will be able to:

- use a range of established techniques to initiate and undertake critical analysis of information, and to propose solutions to problems arising from that analysis
- effectively communicate information, arguments and analysis in a variety of forms to specialist and non-specialist audiences, and deploy key techniques of the discipline effectively
- undertake further training, develop existing skills and acquire new competencies that will enable them to assume significant responsibility within organisations.

And holders will have:

- the qualities and transferable skills necessary for employment requiring the exercise of personal responsibility and decision-making.

Descriptor for a higher education qualification at level 6: Bachelor's degree with honours

The descriptor provided for this level of the FHEQ is for any bachelor's degree with honours which should meet the descriptor in full. This qualification descriptor can also be used as a reference point for other level 6 qualifications, including bachelor's degrees, graduate diplomas etc.

Bachelor's degrees with honours are awarded to students who have demonstrated:

- a systematic understanding of key aspects of their field of study, including acquisition of coherent and detailed knowledge, at least some of which is at, or informed by, the forefront of defined aspects of a discipline
- an ability to deploy accurately established techniques of analysis and enquiry within a discipline
- conceptual understanding that enables the student:
  - » to devise and sustain arguments, and/or to solve problems, using ideas and techniques, some of which are at the forefront of a discipline
  - » to describe and comment upon particular aspects of current research, or equivalent advanced scholarship, in the discipline
  - » an appreciation of the uncertainty, ambiguity and limits of knowledge
  - » the ability to manage their own learning, and to make use of scholarly reviews and primary sources (for example, refereed research articles and/or original materials appropriate to the discipline).

Typically, holders of the qualification will be able to:

- apply the methods and techniques that they have learned to review, consolidate, extend and apply their knowledge and understanding, and to initiate and carry out projects
- critically evaluate arguments, assumptions, abstract concepts and data (that may be incomplete), to make judgements, and to frame appropriate questions to achieve a solution – or identify a range of solutions – to a problem
- communicate information, ideas, problems and solutions to both specialist and non-specialist audiences.

And holders will have:

- the qualities and transferable skills necessary for employment requiring:
  - the exercise of initiative and personal responsibility
  - decision-making in complex and unpredictable contexts
  - the learning ability needed to undertake appropriate further
  - training of a professional or equivalent nature.

Holders of a bachelor's degree with honours will have developed an understanding of a complex body of knowledge, some of it at the current boundaries of an academic discipline. Through this, the holder will have developed analytical techniques and problem-solving skills that can be applied in many types of employment. The holder of such a qualification will be able to evaluate evidence, arguments and assumptions, to reach sound judgements and to communicate them effectively.

Holders of a bachelor's degree with honours should have the qualities needed for employment in situations requiring the exercise of personal responsibility, and decision-making in complex and unpredictable circumstances.

ANNEX B: BCS ACCREDITATION GUIDELINES AND APPLICABILITY OF THE THEMES

The table below highlights where the subject areas and associated concepts can be used to enhance an institution's academic teaching against the BCS accreditation guidelines[1].

		Information and risk	Threats and attacks	Cybersecurity architecture and operations	Secure systems and products	Cybersecurity management
Computing-related cognitive abilities	■ Knowledge and understanding of essential facts, concepts, principles and theories relating to computing and computer applications as appropriate to the programme of study	✓	✓	✓	✓	✓
	■ The use of such knowledge and understanding in the modelling and design of computer-based systems for the purposes of comprehension, communication, prediction and the understanding of trade-offs				✓	
	■ The ability to recognise and analyse criteria and specifications appropriate to specific problems, and plan strategies for their solution	✓			✓	✓
	■ The ability to analyse the extent to which a computer-based system meets the criteria defined for its current use and future development				✓	
	■ The ability to deploy appropriate theory, practices and tools for the specification, design, implementation and evaluation of computer-based systems			✓	✓	✓
	■ The ability to recognise the legal, social, ethical and professional issues involved in the exploitation of computer technology and be guided by the adoption of appropriate professional, ethical and legal practices	✓				✓
	■ Knowledge and understanding of the commercial and economic context of the development, use and maintenance of information systems	✓				✓
	■ Knowledge and understanding of the management techniques which may be used to achieve objectives within a computing context	✓				✓

[1] BCS, The Chartered Institute for IT, *Guidelines on course accreditation, Information for universities and colleges.*

Annex B: BCS accreditation guidelines and applicability of the themes continued...

		Information and risk	Threats and attacks	Cybersecurity architecture and operations	Secure systems and products	Cybersecurity management
Computing-related practical abilities	■ Knowledge and understanding of cybersecurity issues in relation to the design, development and use of information systems	✓	✓	✓	✓	✓
	■ The ability to specify, design or construct computer-based systems	✓		✓	✓	
	■ The ability to evaluate systems in terms of general quality attributes and possible trade-offs presented within the given problem	✓		✓	✓	
	■ The ability to recognise any risks or safety aspects that may be involved in the operation of computing equipment within a given context	✓	✓		✓	✓
	■ The ability to deploy effectively the tools used for the construction and documentation of computer applications, with particular emphasis on understanding the whole process involved in the effective deployment of computers to solve practical problems	✓		✓	✓	
Transferable skills	■ An ability to work as a member of a development team recognising the different roles within a team and different ways of organising teams	✓			✓	
	■ The development of transferable skills that will be of value in a wide range of situations. These include problem solving, working with others, effective information management and information retrieval skills, numeracy in both understanding and presenting cases involving a quantitative dimension, communication skills in electronic as well as written and oral form to a range of audiences and planning self-learning and improving performance as the foundation for on-going professional development	✓				✓

ANNEX C: EXAMPLE APPLICATIONS OF THE THEMES TO COMPUTING SCIENCE SYLLABI

References to the various themes are given thus: *(Theme title)*

Database Systems Syllabus

Within the database systems syllabus, the core concepts of the information lifecycle , attributes of information and classification *(Information and risk)* can be incorporated into lectures on architecture, data modelling and database design. These cybersecurity concepts can be further supplemented by the concepts of secure design, requirements analysis for security *(Secure systems and products)* and the functioning of security controls *(Cybersecurity architecture and operations)*.

Understanding the type(s) of information to be stored in a database and their classification can be used to identify and express database requirements, such as integrity, and then build secure designs to meet those requirements.

Finally, the concepts of threats and attacks and cybersecurity architecture and operations can be used to highlight possible attacks on databases – and how they may be carried out in practice – and the potential cybersecurity controls that can be implemented to mitigate such attacks *(Threats & attacks, Cybersecurity architecture and operations)*. The core concepts of cybersecurity management can also be discussed, such as using standards or guidelines to ensure consistent development approaches are taken *(Cybersecurity management)*.

Networks Syllabus

Within the networks syllabus, the core concepts of confidentiality, integrity and availability *(Information and risk)* can be incorporated into lectures on network architecture, data encoding and data encryption. These cybersecurity concepts can be further supplemented by the concepts of secure protocol design, requirements analysis for security and the functioning of security controls *(Cybersecurity architecture and operations)*.

Understanding the type(s) of information to be carried by communication networks and their classification can be used to identify and express communication network requirements, such as confidentiality, integrity and availability and then build secure designs to meet those requirements.

Finally, the concepts of threats and attacks and cybersecurity architecture and operations can be used to highlight possible attacks on networks and the information that they carry; how these attacks may be carried out in practice; and the potential cybersecurity controls that can be implemented to mitigate such attacks should also be covered *(Threats & attacks, Cybersecurity architecture and operations)*. The core concepts of cybersecurity management can also be discussed, such as using standards or guidelines to ensure consistent development approaches are taken *(Cybersecurity management)*.

Operating Systems Syllabus

Within the operating systems syllabus, the core concepts of the information lifecycle, authorisation and authentication can be incorporated into lectures on OS/Kernel design, process management and memory management. These cybersecurity concepts can be further supplemented by the concepts of secure design, requirements analysis for security and the functioning of security controls *(Secure systems and products)*.

Understanding the type(s) of information to be stored and how that is used by the OS can be used to identify and express requirements, such as authorisation, and then build secure designs to meet those requirements.

Finally, the concepts of threats and attacks and cybersecurity architecture and operations can be used to highlight possible attacks on operating systems; how they may be carried out in practice; and the potential cybersecurity controls that can be implemented to mitigate such attacks *(Threats & attacks)*.

Software Engineering Syllabus

Within the software engineering syllabus, the core concepts of the software development lifecycle, and software design, build and testing can be incorporated into lectures. These concepts can be further supplemented by the Cybersecurity concepts of secure design, requirements analysis for security and the functioning of security controls *(Secure systems and products, cybersecurity architecture and operations)*.

Understanding the type(s) of information to be used by software and their classification can be used to identify and express requirements, such as those associated with input validation, and then build and test secure designs to meet those requirements *(Secure systems and products)*.

Finally, the concepts of threats and attacks and cybersecurity architecture and operations can be used to highlight possible attacks on software applications; how they may be carried out in practice and the potential cybersecurity controls that can be implemented to mitigate such attacks. The core concepts of cybersecurity management can also be discussed, such as using standards or guidelines to ensure consistent development approaches are taken *(Cybersecurity management)*.

ANNEX D: SOURCES CONSULTED

Association for Computing Machinery, *Computer Science Curricula 2013*, December 2013 https://www.acm.org/education/CS2013-final-report.pdf (accessed 23/04/15)

BCS, The Chartered Institute for IT, *Guidelines on course accreditation, Information for universities and colleges*, September 2010, updated for use from Autumn 2012, www.bcs.org/content/ConMediaFile/20312 (accessed 23/04/15)

Contributions from attendees of three workshops held 2013-2015 to create this resource

Gordon, A. (editor), *Official (ISC)² Guide to the CISSP CBK (Fourth edition)*, CRC Press, Boca Raton, Florida, 2015

Hernandez, S. (editor), *Official (ISC)² Guide to the CISSP CBK (Third edition)*, CRC Press, Boca Raton, Florida, 2013

Kim, D. and Solomon, M.G., *Fundamentals of Information Systems Security (Second edition)*, Jones & Bartlett Learning, Burlington, 2014

QAA, *The framework for higher education qualifications in England, Wales and Northern Ireland August 2008*, August 2008, http://www.qaa.ac.uk/publications/information-and-guidance/publication?PubID=2718#.VTjur5M3vVI (accessed 23/04/15)

UK university Computing Science websites (including, but not limited to: Durham, Greenwich, Kent, Lancaster, Imperial, Middlesex, Open, QMW, Royal Holloway, Warwick and UCL)

ANNEX E: REFERENCE DOCUMENTS

British Standard PAS 754 Software Trustworthiness. Governance and management. Specification

Building Security In Maturity Model Software Security Framework (BSSIM SSF) https://www.bsimm.com/online/ (accessed July 7 2015)

Capability Maturity Model (CMM) http://cmmiinstitute.com/ (accessed 7 July 2015)

CRAMM (CCTA Risk Analysis and Management Method) [no site found]

Defence Signals Directorate (DSD) Top 35 Strategies to Mitigate Targeted Cyber Intrusions http://www.asd.gov.au/infosec/mitigationstrategies.htm (accessed 7 July 2015)

ISO 22301 Societal security -- Business continuity management systems -- Requirements

ISO 31000 Risk management -- Principles and guidelines

ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements

ISO/IEC 27005 Information technology -- Security techniques -- Information security risk management

ISO/IEC 27014 Information technology -- Security techniques -- Governance of information security

ISO/IEC 27031 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity

ISO/IEC 27034-1 Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts

ISO/IEC 27034-2 Information technology -- Security techniques -- Application security -- Part 2: Organization normative framework (under development)

ISO/IEC 27034-3 Information technology -- Security techniques -- Application security -- Part 3: Application security management process (under development)

ISO/IEC 27034-4 Information technology -- Security techniques -- Application security -- Part 4: Application security validation

ISO/IEC 27034-5 Information technology -- Security techniques -- Application security -- Part 5: Protocols and application security controls data structure (under development)

ISO/IEC 27034-6 Information technology -- Security techniques -- Application security -- Part 6: Security guidance for specific applications (under development)

ISO/IEC 27034-7 Information technology -- Application security -- Part 7: Application security assurance prediction (under development)

ISO/IEC 27036-1 Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts (under development)

ISO/IEC 27036-2 Information technology -- Security techniques -- Information security for supplier relationships -- Part 2: Requirements

ISO/IEC 27036-3 Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for information and communication technology supply chain security

ISO/IEC 27036-4 Information technology -- Information security for supplier relationships -- Part 4: Guidelines for security of Cloud services (under development)

ITGI Information Security Governance Guidance for Boards of Directors and executive Management 2nd Edition

NIST SP800-30 Guide for Conducting Risk Assessments Revision 1

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) http://www.cert.org/resilience/products-services/octave/ (accessed July 7 2015)

Open Web Application Security Project (OWASP) https://www.owasp.org/index.php/Main_Page (accessed July 7 2015)

Open Web Application Security Project (OWASP) top 10 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (accessed July 7 2015)

SANS Top 20 Critical Security Controls https://www.sans.org/critical-security-controls/ (accessed July 7 2015)

Sherwood Applied Business Security Architecture (SABSA) http://www.sabsa.org/ (accessed July 7 2015)

The Open Group Architecture Framework (TOGAF) http://www.opengroup.org/subjectareas/enterprise/togaf (accessed July 7 2015)

Verizon Data Breach Incident Report http://www.verizonenterprise.com/DBIR/ (accessed July 7 2015)

ENDNOTES

[I] The experts consulted include representatives from: BCS, The Chartered Institute for IT, The Tech Partnership, the IET, Department of Business, Innovation and Skills, GCHQ, Office of Cyber Security and Information Assurance of the Cabinet Office, Trustworthy Software Initiative, ISACA, IISP and CompTIA. We extend our thanks to all of them for their input and support.