National Cyber Security Centre
a part of GCHQ

NCSC Cyber Security Training Courses

Supporting Assessment Criteria for the NCSC Certified Training Scheme

Document History

Issue	Date	Comment
1.0	30 September 2014	First Issue
2.0	08 January 2016	Second Issue
3.0	3 June 2020	Third Issue
4.0	December 2020	Fourth Issue

Introduction

Reflecting the aims of the National Cyber Security Programme, UK Government and its delivery partners are working to increase the UK's educational capability in all fields of cyber security. Together the Department for Business, Energy and Industrial Strategy, the Engineering and Physical Sciences Research Council, the Department for Digital, Culture, Media and Sport, NCSC and Cabinet Office have developed a joint approach and strategy for reaching this goal. As part of that strategy, through the NCSC Certified Training scheme, NCSC intends to certify cyber security training courses, which are available to anyone and not just the public sector. The scheme is designed to provide confidence in cyber security training providers and the courses that they offer.

Overview

Cyber Security: the National Cyber Security Strategy 2016-2021[1] describes cyber security as 'the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.' This document's use of the term 'cyber security' is consistent with this definition. However, it should be recognised that there are many definitions of cyber security and a succinct definition will always be rather abstract. The NCSC is using the Cyber Security Body of Knowledge (CyBOK[2]) to define the discipline of cyber security, including its boundaries, dependencies and relationships with other disciplines.

The CyBOK Knowledge Areas (KAs) should be used as the basis for assessing and defining the cyber security *knowledge* content of a training course. Applicants claiming to map training to CyBOK KA topics must provide supporting evidence. This self-assessment will be used as a basis for assessment by the Certification Body (APMG). Mapping the knowledge content of cyber security topics in training courses to CyBOK KAs is in line with the approach used for mapping cyber security degree knowledge content to CyBOK for NCSC certification of degrees. This is intentional as it provides a common baseline for cyber security capability from awareness and training through to that used at the highest levels of academic pursuit. The anticipated key benefits include providing clear guidance to prospective students and employers about the content and quality of such courses.

The requirement is for training providers to tell a coherent story which lays out what will be taught, why that makes a coherent module of training and to demonstrate that the content is correct and relevant to the audience/community. To meet the scope to apply for recognition, eighty per cent or more of the training must be related to cyber security. As CyBOK is the agreed community scope for established cyber security knowledge, it is anticipated that the majority of *knowledge* provided in cyber security training will map to CyBOK topics. Other elements in cyber security practice, for example the application of skills, may also be included.

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[2] www.cybok.org

Course Content and Structure

Training providers will be able to submit two types of courses for assessment: those which provide fundamental or introductory topic coverage and courses which provide coverage which is beyond introductory. Training providers will be asked to designate which type of course they are submitting.

At least eighty per cent of the training course must cover cyber security (which can include knowledge and skills), as nominated by the training provider in their self-assessment. Applicants need to show how the training provides a coherent body of work for students and ensures that they will gain knowledge about key areas of cyber security. Course content must be consistent with NCSC guidance on the same subject matter.

It is *expected* that an introductory training course will:

- Provide an introduction, awareness and overview of topics in one or more of the nominated CyBOK KAs
- Be applicable for those who are taking up a new cyber security role or wishing to enter the cyber security profession
- Not require any training, professional or academic prerequisites
- Not have to include any self-study
- Not have to provide any practical/'hands-on' learning
- Not have to include a formal examination or assessment, although this can be offered if required

It is *expected* that training courses which provide more than an introduction to cyber security will:

- Provide a detailed insight and understanding of a breadth of topics in one or more of the nominated CyBOK KAs
- Be applicable for those who are already performing a cyber-security role and wish to further their professional capability
- Require training, professional or academic prerequisites
- Typically run for two or more days
- Include self-study
- Provide practical/'hands-on' learning
- Include formal examination or assessment, which could form part of a professional certification.

The Assessment Process

APMG, the Certification Body, assesses three distinct areas of course delivery.

1) The quality management systems of the training provider will be checked to ensure that the management of applicants, their personal details, the processes for developing courses and the delivery of training and maintaining oversight of those delivering the training are consistent, efficient and effective.

2) The trainers will be assessed for their teaching ability and delivery, their technical knowledge of the cyber security topics covered by the course being assessed and the ways in which they maintain their cyber security knowledge. This will include observation of their training and an interview with each trainer delivering a course. The platform performance for online training will also be assessed.

3) The training content will be assessed to ensure that it provides the best opportunity for delegates to feel that they have received a high quality training course.

- At least eighty per cent of a training course must address cyber security.
- Course content must be consistent with NCSC guidance on the same subject matter.
- Applicants need to justify how the distribution of topics provides a coherent body of work for students and ensures that they are gaining knowledge about key areas of cyber security.
- The CyBOK[3] is the community consensus for the scope of cyber security knowledge. It is therefore anticipated that most cyber security *knowledge* in cyber security training will map to CyBOK topics. Cyber security topics not included in CyBOK may also be included, in particular skills, including cross-cutting skills.
- In order to claim to map to a CyBOK Knowledge Area (KA), course topics should, for example, map to approximately half of the topics in the nominated KA.
- The depth of coverage of cyber security topics should also be indicated (e.g., introductory or above introductory). This can be evidenced, for example, by how much of the course is devoted to the topic and how the topic is treated. By way of example only for topic treatment - the level of detailed information provided about the topic and the degree to which a student must demonstrate understanding of it, including whether the topic is tested, and if so, the rigour of that testing method and whether there is more than one way in which topic knowledge acquisition is assessed. In addition, if indicative material for the topic can be mapped to a 3rd of 4th set of sub-nodes in a KA Knowledge Tree, this might indicate that the topic is being treated at a depth that is above introductory.
- The overall course description and syllabus should:
    - explain which cyber security topics are covered
    - explain what the training should enable students to do as a result of attending the course

[3] www.cybok.org

- justify the description of the type of training offered (introductory or above introductory)
- include a bar chart and/or radar chart based on CyBOK mapping to show the relative emphasis of the course (see Appendix A).

See Appendix A for guidance on how to map to the CyBOK KAs, using mapping resources from the CyBOK website[4]. Applicants are encouraged to refer to all of the mapping resources.

See Appendix B for some examples of indicative material for cyber security topics. Training programmes are not required to cover all indicative material explicitly, however in order to demonstrate that a KA topic is satisfactorily addressed, there must be evidence of a good breadth of indicative material or similar examples.

The above should provide prospective applicants with a full understanding of what to expect from the training. Marketing material for the training will also be assessed to ensure that it does not mislead potential applicants.

Certification of training courses by APMG will be subject to a set of terms and conditions (T&Cs) which all applicants will have to agree to as part of the application process.

[4] See a set of resources at https://www.cybok.org/usecases/

Appendix A

Methodology for mapping topics to one or more CyBOK Knowledge Areas

The following mapping resources are taken from the Cyber Security Body of Knowledge ('CyBOK'), which is published under an Open Government Licence. See www.cybok.org for further information. All are free to download.

1. Highlight and list key terms and topics in training material and use the following resources to establish if they can be mapped to CyBOK topics:

- CyBOK Knowledge Trees (see https://www.cybok.org/knowledgebase/)
- CyBOK Mapping Reference v 1.1. (see https://www.cybok.org/usecases/
- An A-Z of CyBOK Knowledge Areas Indicative Material (see https://www.cybok.org/usecases/
- CyBOK Tabular Representation of the Broad Categories and Knowledge Areas (see https://www.cybok.org/usecases/

The following 4 tables are an example of how to record mapping to CyBOK.

MAPPING TO CyBOK USING KNOWLEDGE TREES				
Training Module/Section	**Topic**	**CyBOK Topic**	**CyBOK Knowledge Area**	**CyBOK Broad Category**

<table>
<tr><th colspan="5">MAPPING TO CyBOK USING AN A-Z of CyBOK KNOWLEDGE AREAS INDICATIVE MATERIAL</th></tr>
<tr><th>Training Module/Section</th><th>Topic</th><th>CyBOK Topic</th><th>CyBOK Knowledge Area</th><th>CyBOK Broad Category</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

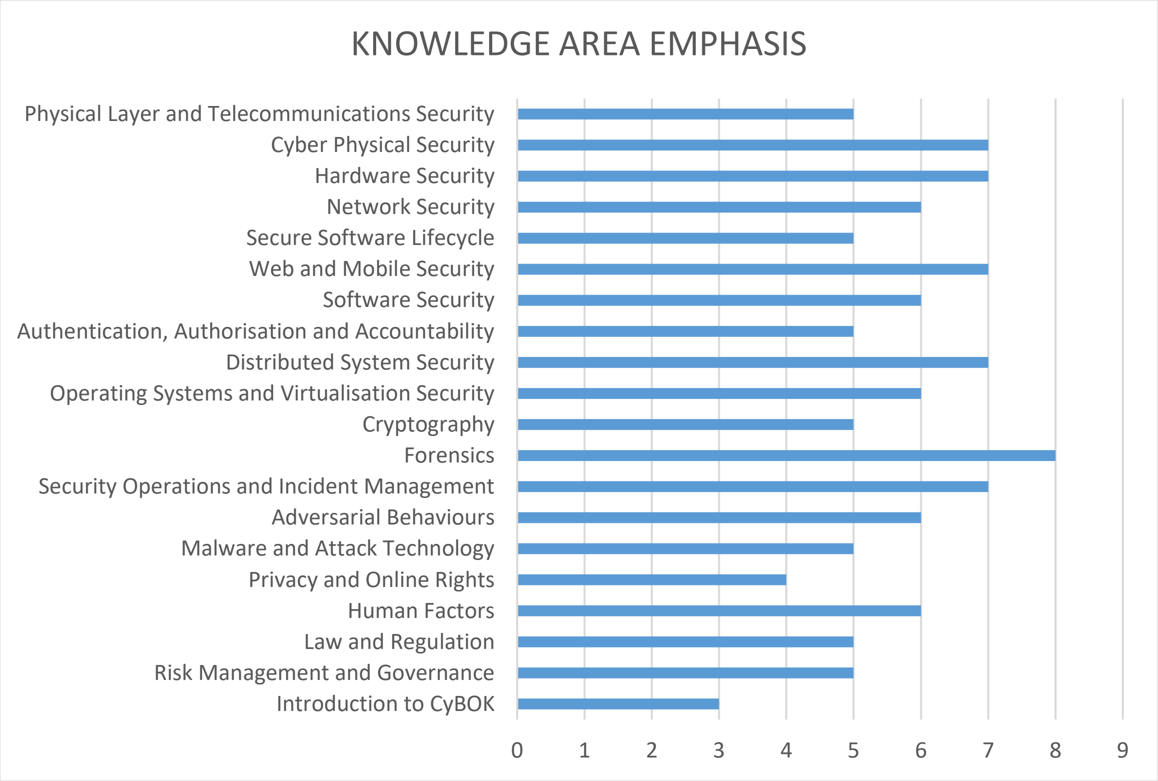
<table>
<tr><th colspan="5">MAPPING TO CyBOK USING THE CyBOK MAPPING REFERENCE V1.1</th></tr>
<tr><th>Training Module/Section</th><th>Topic</th><th>CyBOK Topic</th><th>CyBOK Knowledge Area</th><th>CyBOK Broad Category</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="5">MAPPING TO CyBOK USING A TABULAR REPRESENTATION OF BROAD CATEGORIES AND KAs</th></tr>
<tr><th>Training Module/Section</th><th>Topic</th><th>CyBOK Topic</th><th>CyBOK Knowledge Area</th><th>CyBOK Broad Category</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

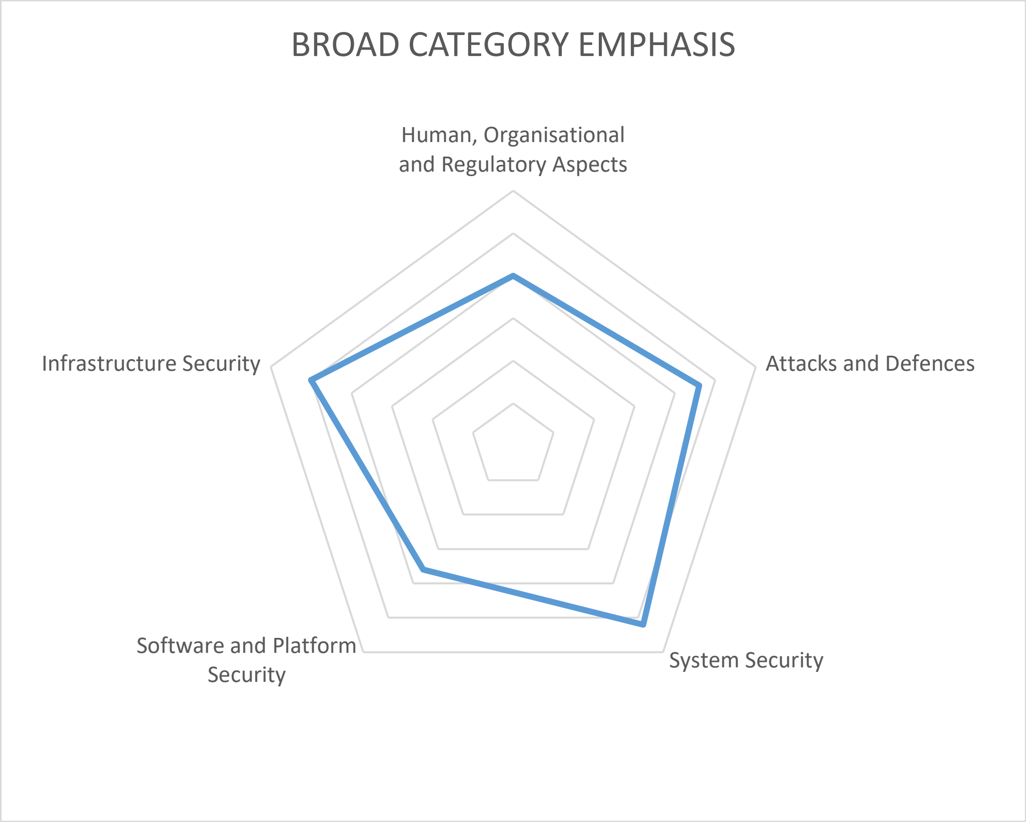
2. Use the largest list produced for each Knowledge Area (KA) to produce a bar chart to show the relative emphasis of the CyBOK KAs in the training course. Produce a radar chart or similar to show the relative emphasis of the CyBOK broad categories.

3. The following is an example of how to produce these charts.

EXAMPLE OF A CHART TO SHOW KNOWLEDGE AREA EMPHASIS	
Introduction to CyBOK	3
Risk Management and Governance	5
Law and Regulation	5
Human Factors	6
Privacy and Online Rights	4
Malware and Attack Technology	5
Adversarial Behaviours	6
Security Operations and Incident Management	7
Forensics	8
Cryptography	5
Operating Systems and Virtualisation Security	6
Distributed System Security	7
Authentication, Authorisation and Accountability	5
Software Security	6
Web and Mobile Security	7
Secure Software Lifecycle	5
Network Security	6
Hardware Security	7
Cyber Physical Security	7
Physical Layer and Telecommunications Security	5


KNOWLEDGE AREA EMPHASIS
Physical Layer and Telecommunications Security
Cyber Physical Security
Hardware Security
Network Security
Secure Software Lifecycle
Web and Mobile Security
Software Security
Authentication, Authorisation and Accountability
Distributed System Security
Operating Systems and Virtualisation Security
Cryptography
Forensics
Security Operations and Incident Management
Adversarial Behaviours
Malware and Attack Technology
Privacy and Online Rights
Human Factors
Law and Regulation
Risk Management and Governance
Introduction to CyBOK
0
1
2
3
4
5
6
7
8
9

EXAMPLE OF A CHART TO SHOW BROAD CATEGORY EMPHASIS	
Human, Organisational and Regulatory Aspects	20
Attacks and Defences	23
System Security	26
Software and Platform Security	18
Infrastructure Security	25



4. List the main cyber security topics in the training material in the following table and provide evidence against the headings to support claims for introductory or above introductory topic coverage. This information should form the basis for the overall description and marketing of the course. It is expected that the overwhelming majority of topics in a course would be at an above introductory depth in order to justify a claim that the course as a whole can be described as above introductory.

DEPTH OF TOPIC COVERAGE				
Cyber Security Topic	**Training Module/Section**	**Topic Coverage that is above Introductory (e.g., is there a very full degree of detail, is the topic assessed, are there a number of different ways that the topic is treated or understanding is assessed, etc.?)**	**Coverage at introductory level**	**Mapped to CyBOK - Y/N** (*this information should be available from the previous mapping tables*)

Appendix B

The following tables (one for each CyBOK Knowledge Area) show some *examples* of the type of indicative material which would demonstrate some coverage of knowledge relating to the nominated cyber security topic. Other examples may also be applicable.

KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLE OF INDICATIVE MATERIAL
1. CyBOK Introduction	Foundational Concepts	Objectives of cyber security
		Definition of cyber security
		Failures and incidents
		Risk management
	Principles	Saltzer and Schroeder principles
		NIST principles
		Latent design conditions
		Precautionary Principle
	Cross-cutting Themes	Security economics
		Security architecture and lifecycle
		Verification and formal methods

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLE OF INDICATIVE MATERIAL
Human, Organisational and Regulatory Aspects	2. Risk Management and Governance	Risk Definitions	Risk assessment
			Risk management
			Levels of perceived risk
		Risk Governance	Governance models
			Risk perception factors
			Human factors and risk communication
			Security culture
			Enacting security policy
		Risk Assessment & Management Principles	Component versus systems perspectives
			Elements of risk
			Risk assessment and management methods
			Risk assessment and management in cyber-physical systems
			Security metrics
		Business Continuity: Incident Response and Recovery Planning	ISO/IED 27035
			NCSC Guidance

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLE OF INDICATIVE MATERIAL
Human, Organisational and Regulatory Aspects	3. Law and Regulation	Introductory Principles of Legal Research	Nature of law and legal analysis
			Applying law to cyberspace and information technologies
			Criminal law
			Civil law
			Liability and courts
			Evidence and proof
			Holistic approaches to legal risk analysis
		Jurisdiction	Prescriptive jurisdiction
			Enforcement jurisdiction
			Data sovereignty
		Privacy Laws in General and Electronic Interception	International norms
			Interception by a state
			Interception by persons other than state
			Enforcement of privacy laws
		Data protection	Subject matter and regulatory focus
			Core regulatory principles
			Investigation and prevention of crime
			Personal data breach notification
			Enforcement and penalties
		Computer crime	Crimes against information systems
			De minimis exceptions to crimes against information systems
			The enforcement of, and penalties for, crimes against information systems
			Warranted state activity
			Research and development activities conducted by non-state persons
			Self-help disfavoured: software locks and hack-back
		Contract law	On-line contracts
			Encouraging security standards via contract
			Warranties and their exclusion
			Limitations of liability and exclusions of liability
			Breach of contract and remedies
			Effects of contract on non-contracting parties

			Conflict of law - contracts
Human, Organisational and Regulatory Aspects	3. Law and Regulation	Intellectual Property	Understanding intellectual property
			Catalogue of intellectual property rights
			Enforcement – remedies
			Reverse engineering
			International treatment and conflict of law
		Internet Intermediaries	Shields from liability
			Take-down protection
		Dematerialisation of Documents and Electronic Trust Services	Admission into evidence of electronic documents
			Requirements of form and the threat of unenforceability
			Electronic signatures and identity trust services
			Conflict of law – electronic signatures and trust services
		Other Regulatory Matters	Industry-specific regulations
			Restrictions on exporting security technologies
			Matters classified as secret by a state
		Public International Law	Attributing action to a state under international law
			State cyber operations in general
			Cyber espionage in peacetime
			Cross-border criminal investigation
			The law of armed conflict
		Ethics	Obligations owed to a client
			Codes of conduct
			Vulnerability testing

BROAD CATEGORY	CyBOK KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLE OF INDICATIVE MATERIAL
Human, Organisational and Regulatory Aspects	4. Human Factors	Usable Security	Assessment criteria
			Mental models of security
		Fitting the task to the Human	Human capabilities and limitations
			Short-term memory
			Long-term memory
			Human biases
			Needs of specific groups
			Goals and tasks
			Interaction context
			Device capabilities and limitations
		Human Error	Latent usability failures in systems-of-systems
			Thinking fast and slow
			Shadow security
			Security hygiene
		Awareness and Education	Terms
			New approaches
			Mental models of cyber risks and defences
		Positive Security	Fear uncertainty and doubt
			People are not the weakest link
		Stakeholder Engagement	Employees
			Software developers

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLE OF INDICATIVE MATERIAL
Human, Organisational and Regulatory Aspects	5. Privacy and Online Rights	Confidentiality	Data confidentiality
			Metadata confidentiality
		Control	Privacy settings configuration
			Privacy policy negotiation
			Privacy policy interpretability
		Transparency	Feedback-based transparency
			Audit-based transparency
		Privacy Technologies and Democratic Rights	Privacy technologies as support to democratic political systems
			Censorship resistance and freedom of speech
		Privacy Engineering	Goals
			Strategies
			Privacy evaluation

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLE OF INDICATIVE MATERIAL
Attacks and Defences	6. Malware and Attack Technologies	Malware Taxonomy	Dimensions
			Kinds
			Potentially unwanted programs
		Malicious Activities by Malware	Attack on confidentiality, integrity, availability
			Cyber kill chain
			Underground eco-system
		Malware Analysis	Analysis techniques
			Analysis environments
			Anti-analysis and evasion techniques
			Identifying the analysis environment
		Malware Detection	Identifying the presence of malware
			Evasion and countermeasures
			Attack detection
		Malware Response	Disrupting malware operations
			Attribution

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPICS	EXAMPLE OF INDICATIVE MATERIAL
Attacks and Defences	7. Adversarial Behaviours	Characterisation of Adversaries	Cyber-enabled crime vs cyber-dependent crime
			Interpersonal crimes
			Cyber-enabled organised crime
			Cyber-dependent organised crime
			Hacktivists
			State actors
		Elements of a Malicious Operation	Affiliate programmes
			Infection vectors
			Infrastructure
			Specialised services
			Human services
			Payment methods
		Models	Attack trees
			Kill chains
			Environmental criminology
			Flow of capital
			Attribution

BROAD CATEGORY	**KNOWLEDGE AREA**	**CyBOK TOPICS**	**EXAMPLE OF INDICATIVE MATERIAL**
Attacks and Defences	8. Secure Operations and Incident Management	Fundamental Concepts	Workflows and vocabulary
			Architectural principles
		Monitor: Data Sources	Network traffic
			Network aggregates: netflow
			Network infrastructure information
			Application logs: web server logs and files
			System and kernel logs
			Syslog
		Analyse: Analysis Methods	Misuse detection
			Anomaly detection
			Machine learning
			Testing and validating intrusion detection systems
			The base-rate fallacy
			Contribution of SIEM to analysis and detection
		Plan: Security Information and Event Management	Data collection
			Alert correlation
			Security operations and benchmarking
		Execute: Mitigation and Countermeasures	Intrusion prevention systems
			SIEM platforms and countermeasures
			SOAR: impact and risk assessment
			Site reliability engineering
		Knowledge: Intelligence and Analysis	Cyber security knowledge management
			Honeypots and honeynets
			Cyber-threat intelligence
			Situational awareness
		Human Factors: Incident Management	Prepare: incident management planning
			Handle: actual incident response
			Follow up: post incident activities

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPICS	EXAMPLES OF INDICATIVE MATERIAL
Attacks and Defences	9. Forensics	Definitions and Conceptual Models	Forensic science
			Cyber domain
			Digital (forensic) trace
			Legal concerns and the Daubert Standard
			Definitions
			Conceptual models
		Operating System Analysis	Storage forensics
			Data acquisition
			Filesystem analysis
			Block device analysis
			Data recovery and file content carving
		Main Memory Forensics	Process information
			File information
			Network connections
			Artifacts and fragments
			Challenges of live forensics
		Application Forensics	Case study: e.g., web browsers
		Cloud Forensics	Services
			Forensics challenges
			SaaS forensics
		Artifact Analysis	Cryptographic hashing
			Block-level analysis
			Approximate analysis
			Cloud-native artifacts

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPICS	EXAMPLES OF INDICATIVE MATERIAL
Systems Security	10. Cryptography	Schemes	AES
			RSA
			DES
			PKCS
			DSA
			Kerberos
			TLS
		Symmetric Cryptography	Symmetric primitives
			Symmetric encryption and authentication
		Public Key Cryptography	Public-key encryption
			Public-key signatures
		Cryptographic Security Models	Basic security definitions
			Hard problems
			Setup assumptions
			Simulation of cryptographic operations
			Universal composability
		Information-Theoretically Secure Constructions	One-time pad
			Secret sharing
		Standard Protocols	Authentication protocols
			Key agreement protocols
		Advanced Protocols	Oblivious transfer
			Zero knowledge
			Sigma protocols
			Secure multi-party computation
		Public-Key Schemes with Special Properties	Group signatures
			Ring signatures
			Blind signatures
			Identity-based encryption
			Linearly homomorphic encryption
			Fully homomorphic encryption

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPICS	EXAMPLES OF INDICATIVE MATERIAL
Systems Security	11. Operating Systems and Virtualisation Security	Attacker Model	Attack surface
			Threats to security for modern OSs
		Role of Operating Systems	Mediation
			Design choices
			Virtual machines
			IOT
			Security domains
			Isolation
		OS Security Principles	Security models
			Newer principles
			Saltzer and Schroeder's principles
		Primitives for Isolation and Mediation	Protection rings
			Low-end devices and IOT
			Multics
			Trusted computer system evaluation criteria
			Memory protection and address spaces
			Capabilities
			Physical access and secure deletion
			Authentication and identification
			Modern hardware extensions for memory protection
		OS Hardening	Information hardening
			Control-flow restrictions
			Partitioning
			Code and data integrity checks
			Anomaly detection
			Formal verification
		Related Areas	Databases
		Embracing Security	PaX Team
			GRSecurity

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPICS	EXAMPLES OF INDICATIVE MATERIAL
Systems Security	12. Distributed Systems Security	Classes of Distributed Systems	Decentralised point-to-point interactions across distributed entities without a centralised coordination service
			Coordinated clustering across distributed resources and services
		Classes of Vulnerabilities and Threats	Access/admission control and ID management
			Data transportation
			Resource management and coordination services
			Data security
		Decentralised P2P Models	Principles
			Unstructured P2P protocols
			Structured P2P protocols
			Hybrid P2P protocols
			Hierarchical P2P protocols
		Attacking P2P Models	Functional elements
			Attack types
			Attacks and their mitigation
		Coordinated Resource Clustering	Systems coordination styles
			Reliable and secure group communications
			Coordination principles
			Replication management and coordination schema
		Coordination Classes and Attackability	Classes of disruptions
			Resource coordination class
			Services coordination class

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPICS	EXAMPLES OF INDICATIVE MATERIAL
Systems Security	13. Authentication, Authorisation and Accountability	Authorisation	Access control
			Enforcing access control
			Theory
		Access Control in Distributed Systems	Core concepts
			Origin-based policies
			Federated access control
			Cryptography and access control
		Authentication	Identity management
			User authentication
			Authentication in distributed systems
			Facets of authentication
		Accountability	Technical aspects
			Privacy and accountability
			Distributed logs

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLES OF INDICATIVE MATERIAL
Software and Platform Security	14. Software Security	Categories of Vulnerabilities	CVEs and CWEs
			Memory management vulnerabilities
			Structured output generation vulnerabilities
			Race condition vulnerabilities
			API vulnerabilities
			Side channel vulnerabilities
		Prevention of Vulnerabilities	API design
			Coding practices
			Erroneous execution
			Language design and type systems
			Structured output generations mitigations
			Race condition mitigations
			Information flow
		Mitigating Exploitation	Runtime detection of attacks
			Automated software diversity
			Limiting privileges
		Detection of Vulnerabilities	Static detection
			Dynamic detection
			Soundness
			Completeness

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLES OF INDICATIVE MATERIAL
Software and Platform Security	15. Web and Mobile Security	Fundamental Concepts and Approaches	Appification
			Webification
			Application stores
			Sandboxing
			Permission dialogue based access control
			Web PKI and HTTPS
			Authentication
			Cookies
			Passwords and alternatives
			Frequent software updates
		Client-Side Vulnerabilities and Mitigations	Phishing
			Clickjacking
			Client-side storage
			Physical attacks
		Server-Side Vulnerabilities and Mitigations	Injection vulnerabilities
			Server-side misconfiguration and vulnerable components

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLES OF INDICATIVE MATERIAL
Software and Platform Security	16. Secure Software Lifecycle	Motivations for Secure Software Lifecycle	Breaches are costly
			Vulnerabilities can be exploited without being noticed
			Patching can introduce vulnerabilities
			Customers don't apply patches
			Trusted computing
		Prescriptive Processes	SAFECode
			Microsoft SDL
			Touchpoints
		Adaptations of Secure Software Lifecycle	Agile and DevOps
			Mobile
			Cloud computing
			IOT
			Road vehicles
			Ecommerce
		Assess the Secure Software Lifecycle	SAMM
			BSIMM
			Common criteria

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLES OF INDICATIVE MATERIAL
Infrastructure Security	17. Network Security	Internet Architecture	Application layer security
			Transport layer security
			Network layer security
			Link layer security
		Network Defence Tools	Packet filters
			Intrusion detection systems
			Intrusion prevention systems
			Network architecture design
			Application gateway
			Circuit level gateway
		Wireless LAN security	WPA
			WPA2
			WEP
			WPA3
			RSN
		Advanced Network Security Topics	Software defined networking
			Internet of Things security
		Network Protocols and Vulnerability	Dolev-Yao adversarial model
			Common network attacks

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLES OF INDICATIVE MATERIAL
Infrastructure Security	18. Hardware Security	Hardware Design Cycle	Hardware design process
			Root of trust
			Threat model
		Measuring Hardware Security	FIPS 140-2
			Common criteria and EMVCo
			SESIP
		Secure Platforms	Hardware security module (HSM)
			Secure element and smartcard
			Trusted platform module (TPM)
		Hardware Support for Software Security	IBM 4578 secure coprocessor
			ARM Trustzone
			Protected module architectures
			Lightweight solutions
			Objectives
			Virtual machines
			Trusted execution environment
		Hardware Design for Cryptographic Algorithms	Cryptographic algorithms at RTL level
			Design process
		Side Channel Attacks and Fault Attacks	Attacks
			Countermeasures
		Entropy generating Building Blocks	Physically unclonable functions (PUFs)
			Random number generation
		Hardware Design Process	Time
			Design and fabrication of silicon integrated circuits
			Trojan circuits
			Circuit level techniques
			Board level security

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPICS	EXAMPLES OF INDICATIVE MATERIAL
Infrastructure Security	19. Cyber Physical Systems Security	Cyber Physical Systems Security	Characteristics
			Protection against natural events and accidents
			Security and privacy concerns
		Cross Cutting	Preventing attacks
			Detecting attacks
			Mitigating attacks
		Cyber Physical Systems Domains	Industrial control systems
			Electric power grids
			Transportation systems and autonomous vehicles
			Robotics and advanced manufacturing
			Medical devices
			IOT
		Policy and Political Aspects	Incentives and regulation
			Cyber conflict
			Industry practices and standards

BROAD CATEGORY	KNOWLEDGE AREA	CyBOK TOPIC	EXAMPLES OF INDICATIVE MATERIAL
Infrastructure Security	20. Physical Layer and Telecommunications Security	Schemes for Confidentiality, Integrity and Access Control	Key establishment based on channel reciprocity
			MIMO-supported approaches
			Secrecy capacity
			Friendly jamming
			Protecting data integrity
			LPI and covert communication
		Jamming and Jamming-Resilient Communications	Classification of jammers
			Countermeasures
			Coordinated spread spectrum techniques
			Uncoordinated spread spectrum techniques
			Signal annihilation and overshadowing
		Identification	Device under identification
			Identification signals
			Device fingerprints
			Attacks on physical layer identification
		Distance Bounding and Secure Positioning	Distance bounding protocols
			Distance measurement techniques
			Physical layer attacks on secure distance measurement
			Secure positioning
		Compromising Emanations and Sensor Spoofing	Compromising emanations
			Sensor compromise
		Physical Layer Security of Selected Communications Technologies	NFC
			Air traffic communications networks
			Cellular networks
			GNSS security and spoofing attacks