CyBOK Mapping Framework for NCSC Certified Degrees
Guidance Document for UK Higher Education

Lata Nautiyal | University of Bristol

Awais Rashid | University of Bristol

1 STEP BY STEP IMPLEMENTATION OF MAPPING PROCESS BY TAKING EXAMPLE OF ONE MODULE DESCRIPTION FROM MIT UNIVERSITY, USA

Applied Cyber Security (MIT-USA)

Introduction to Information Security Fundamentals and Best Practices

- Protecting Your Computer and its Contents
- Securing Computer Networks–Basics of Networking
- Compromised Computers
- Secure Communications and Information Security Best Practices
- Privacy Guidelines
- Safe Internet Usage

Ethics in Cybersecurity & Cyber Law

- Privacy
- Intellectual Property
- Professional Ethics
- Freedom of Speech
- Fair User and Ethical Hacking
- Trademarks
- Internet Fraud
- Electronic Evidence
- Cybercrimes

Forensics

- Forensic Technologies
- Digital Evidence Collection
- Evidentiary Reporting

Network Assurance

- Layered Defense
- Surveillance and Reconnaissance
- Outsider Threat Protection

Secure Software & Browser Security

- Software Construction
- Software Design and Architecture

- Software Testing
- Methodologies
- The New Universal Client
- The Web Model
- Cookies and Browser Storage
- HTML5 Security

Business Information Continuity

- Managing a Business Information Continuity Plan
- Vulnerabilities and Controls
- The Law and Business Information Continuity Plan

Information Risk Management

- Asset Evaluation and Business Impact Analysis
- Risk Identification
- Risk Quantification
- Risk Response Development and Control
- Security Policy, Compliance, and Business Continuity

Cyber Incident Analysis and Response

- Incident Preparation
- Incident Detection and Analysis
- Containment, Eradication, and Recovery
- Proactive and Post-Incident Cyber Services

1.1 Formation Phase:

Applied Cyber Security (MIT-USA)

Introduction to Information Security Fundamentals and Best Practices

- Protecting Your Computer and its Contents
- Securing Computer Networks–Basics of Networking
- Compromised Computers
- Secure Communications and Information Security Best Practices
- Privacy Guidelines
- Safe Internet Usage

Ethics in Cybersecurity & Cyber Law

- Privacy

- Intellectual Property
- Professional Ethics
- Freedom of Speech
- Fair User and Ethical Hacking
- Trademarks
- Internet Fraud
- Electronic Evidence
- Cybercrimes

Forensics

- Forensic Technologies
- Digital Evidence Collection
- Evidentiary Reporting

Network Assurance

- Layered Defense
- Surveillance and Reconnaissance
- Outsider Threat Protection

Secure Software & Browser Security

- Software Construction
- Software Design and Architecture
- Software Testing
- Methodologies
- The New Universal Client
- The Web Model
- Cookies and Browser Storage
- HTML5 Security

Business Information Continuity

- Managing a Business Information Continuity Plan
- Vulnerabilities and Controls
- The Law and Business Information Continuity Plan

Information Risk Management

- Asset Evaluation and Business Impact Analysis

- Risk Identification
- Risk Quantification
- Risk Response Development and Control
- Security Policy, Compliance, and Business Continuity

Cyber Incident Analysis and Response

- Incident Preparation
- Incident Detection and Analysis
- Containment, Eradication, and Recovery
- Proactive and Post-Incident Cyber Services

1.2 Connecting Phase:

Searching for those highlighted ***keywords*** or a ***set of keywords*** using the resources in the ***"CyBOK Mapping Structure Guide"***. This phase is comprised of 5 steps (**Steps A** to **E**).

Step A: – Mapping with an alphabetical version of the CyBOK's knowledge areas indicative material from NCSC's certification document: –

Start your search with this document. If your Highlighted/Underlined ***keywords*** or a ***set of keywords*** are found in this part, then record these in the table and move on to the next ***keywords*** or a ***set of keywords***. Repeat the process until the last ***keywords*** or a ***set of keywords***. **(Move to step B)**

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword or a Set of Keywords	Mapping with an alphabetical version of the CyBOK knowledge areas indicative material
1					Protecting Your Computer and its Contents	Not Found
2					Securing computer networks - Basics of networking	Not Found
3					Compromised Computers	Not Found
4					Secure Communications and Information Security Best Practices	Not Found
5					Privacy Guidelines	Not Found
6					Privacy	Not Found
7					Intellectual Property	Not Found
8					Professional Ethics	Not Found

9					Freedom of Speech	Not Found
10					Ethical Hacking	Not Found
11					Trademarks	Not Found
12					Internet Fraud	Not Found
13					Electronic Evidence	Not Found
14					Cybercrimes	Not Found
15	Attacks and defences	F	Definition and conceptual models	Forensic science	Forensic Technologies (Forensic science)	Found and Recorded
16					Digital Evidence Collection	Not Found
17					Evidentiary Reporting	Not Found
18					Layered Defense	Not Found
19					Reconnaissance	Not Found
20					Outsider Threat Protection	Not Found
21					Software Construction	Not Found
22					Software Design and Architecture	Not Found
23					Software Testing	Not Found
24					Methodologies	Not Found
25					The Web Model	Not Found
26	Software and Platform Security	WAM	Fundamental concepts and approaches	Cookies	Cookies	Found and Recorded
27					HTML5 Security	Not Found
28					Managing a Business Information Continuity Plan	Not Found
29					Vulnerabilities and control	Not Found
30					Continuity Plan	Not Found
31					Asset Evaluation and Business Impact Analysis	Not Found
32					Risk Identification	Not Found
33					Risk Quantification	Not Found
34					Risk Response development and control	Not Found
35					Security Policy	Not Found
36					Compliance, and Business Continuity	Not Found
37	Attacks and Defences	SOIM	Human Factors: Incident Management	Prepare: Incident management planning	Incident preparation (incident management planning)	Found and Recorded
38	Attacks and Defences	SOIM	Human Factors: Incident Management	Prepare: incident management planning	Incident Detection and Analysis (Incident management planning)	Found and Recorded

39					Containment, Eradication, and Recovery	Not Found
40	Attacks and Defences	SOIM	Human Factors: Incident Management	Follow up - Post-incident activities	Post-incident cyber services (Follow up :post-incident activities)	Found and Recorded

Step B: – Mapping with CyBOK Mapping Reference 1.1: –

Continue your search with this document. If your remaining **(Not Found)** ***keywords*** or a ***set of keywords*** are found in this part, then record these in the table and move on to the next ***keywords*** or a ***set of keywords***. Repeat the process until the last ***keywords*** or a ***set of keywords***. **(Move to step C)**

S.No.	Broad Category	KA	Keyword or a Set of Keywords	Mapping with CyBOK Mapping Reference 1.1
1			Protecting Your Computer and its Contents	Not Found
2	Infrastructure Security	NS	Securing Computer Networks - Basics of networking	Found and Recorded
3	Software and Platform Security	SS, NS	Compromised Computers (CVEs, CWEs), Or (Common network attacks)	Found and Recorded, (Selected SS as relevant)
4	Systems Security	C	Secure Communications and Information Security Best Practices (Secure Communication Channel)	Found and Recorded
5			Privacy Guidelines	Not Found
6	Human, Organisational and Regulatory Aspects	POR	Privacy	Found and Recorded
7	Human, Organisational and Regulatory Aspects	LR	Intellectual Property	Found and Recorded
8	Human, Organisational and Regulatory Aspects	LR	Professional Ethics (Ethics)	Found and Recorded
9	Human, Organisational and Regulatory Aspects	POR	Freedom of Speech	Found and Recorded
10	Infrastructure Security	NS, SOIM, SSL	Ethical Hacking, (Penetration testing) or (Penetration testing - DNS) Or (Penetration testing – active penetration) Or (Penetration testing – software tool)	Found and Recorded, (Selected NS as relevant) (But Multiple mappings are possible)
11	Human, Organisational and Regulatory Aspects	LR	Trademarks	Found and Recorded
12			Internet Fraud	Not Found
13	Attacks and Defences	F	Electronic Evidence (Forensic evidence)	Found and Recorded
14	Human, Organisational and Regulatory Aspects	LR, F	Cybercrimes	Found and Recorded (Selected LR as relevant)
16	Attacks and Defences	F	Digital Evidence Collection	Found and Recorded
17			Evidentiary Reporting	Not Found
18	Systems Security	AAA, RMG, SSL	Layered Defense, (Security Policies) Or (Defence in depth)	Found and Recorded, (Selected AAA as relevant)
19			Reconnaissance	Found (Not recorded, not relevant as per the context)
20	Attacks and Defences	SOIM, AB, RMG	Outsiders Threat Protection (Threats External)	Found and Recorded, (Selected SOIM as relevant)
21	Software and Platform Security	SSL	Software Construction, (Software Development)	Found and Recorded
22			Software Design and Architecture	Not Found

23			Software Testing	Not Found
24	Software and Platform Security	SSL	Methodologies (Software Development methods)	Found and Recorded
25			The Web Model	Not Found
27			HTML5 Security	Not Found
28	Attacks and Defences	RMG, SOIM	Managing a Business Information Continuity Plan, (Business continuity management/planning)	Found and Recorded, (Selected RMG as relevant)
29	Software and Platform Security	SS, CPS	Vulnerabilities and control	Found and Recorded, (Selected SS as relevant)
30	Human, Organisational and Regulatory Aspects	RMG	Continuity plan (Continuity management)	Found and Recorded
31	Human, Organisational and Regulatory Aspects	RMG	Asset Evaluation and Business Impact Analysis (Business impact analysis - in information asset classification)	Found and Recorded
32	Human, Organisational and Regulatory Aspects	RMG	Risk Identification Analysis	Found and Recorded
33	Human, Organisational and Regulatory Aspects	RMG	Risk Quantification (Risk – measuring)	Found and Recorded
34	Human, Organisational and Regulatory Aspects	RMG	Risk Response development and control	Found and Recorded
35	Human, Organisational and Regulatory Aspects	RMG	Security Policy	Found and Recorded
36	Human, Organisational and Regulatory Aspects	RMG	Compliance and Business Continuity	Found and Recorded
39	Attacks and Defences	SOIM	Containment, Eradication and Recovery (Containment in Incident response plan)	Found and Recorded

Step C: – Complete the missing Topics and Indicative Material from CyBOK Knowledge Trees for all the recorded keywords or a set of keywords found through CyBOK Mapping reference 1.1: –

Searching topics and indicative materials from CyBOK Knowledge Trees for all the recorded ***keywords*** or a ***set of keywords*** found through CyBOK Mapping reference 1.1 as CyBOK Mapping reference 1.1 provides relevant CyBOK knowledge areas but not the topic and indicative material, therefore CyBOK Knowledge Trees are used. **(Move to step D)**

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword or a set of Keywords	Mapping missing Topics and Indicative Material from CyBOK Knowledge Trees
2	Infrastructure Security	NS	Network Defence Tools	***	Securing Computer Networks - Basics of networking	Found and Recorded (Multiple mappings are possible) Mapping to NS is just an interpretation as per our viewpoint
3	Software and Platform Security	SS, NS	Categories of vulnerability	CVEs and CWEs	Compromised Computers (CVEs, CWEs), Or (Common network attacks)	Found and Recorded, (Selected SS as relevant)

4	Systems Security	C	Public key cryptography	***	Secure Communications and Information Security Best Practices (Secure Communication Channel)	Found and Recorded
6	Human, Organisational and Regulatory Aspects	POR	Control	***	Privacy	Found and Recorded
7	Human, Organisational and Regulatory Aspects	LR	Intellectual Property	Understanding intellectual property OR Catalogue of intellectual property rights	Intellectual Property	Found and Recorded
8	Human, Organisational and Regulatory Aspects	LR	Ethics	Codes of conduct	Professional Ethics (Ethics)	Found and Recorded
9	Human, Organisational and Regulatory Aspects	POR	Privacy technologies and democratic values	Censorship resistance and freedom of speech	Freedom of Speech	Found and Recorded
10	Infrastructure Security	NS, SOIM, SSL	Network protocols and vulnerability	Common network attacks	Ethical Hacking (Penetration testing) or (Penetration testing - DNS) Or (Penetration testing – active penetration) Or (Penetration testing – software tool)	Found and Recorded, (Selected NS as relevant)(But Multiple mappings are possible)
11	Human, Organisational and Regulatory Aspects	LR	Intellectual Property	Catalogue of intellectual property rights	Trademarks	Found and Recorded
13	Attacks and Defences	F	Definition and conceptual model	Digital (forensic) trace	Electronic Evidence (Forensic evidence)	Found and Recorded
14	Human, Organisational and Regulatory Aspects	LR, F	Computer Crime	Crimes against information systems	Cybercrimes	Found and Recorded (Selected LR as relevant)
16	Attacks and Defences	F	Main Memory Forensics OR Operating System Analysis OR Cloud Forensics OR Artifact Analysis It could be any of these depending on the context.	***	Digital Evidence Collection	Found and Recorded
18	Systems Security	AAA, RMG, SSL	Authorisation	Access Control	Layered Defense (Security Policies) Or (Defence in depth)	Found and Recorded, (Selected AAA as relevant)

20	Attacks and Defences	SOIM, AB, RMG	Knowledge: intelligence and analytics	Cyber-threat intelligence	Outsiders Threat Protection (Threats External)	Found and Recorded, (Selected SOIM as relevant)
21	Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Software Construction, (Software Development)	Found and Recorded
24	Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Methodologies (Software Development methods)	Found and Recorded
28	Attacks and Defences	RMG, SOIM	Business Continuity: Incident Response and Recovery Planning	***	Managing a Business Information Continuity Plan (Business continuity management/planning)	Found and Recorded, (Selected RMG as relevant)
29	Software and Platform Security	SS, CPS	Categories of Vulnerabilities (SS) OR Prevention of Vulnerabilities	***	Vulnerabilities and control	Found and Recorded (Selected SS as relevant)
30	Human, Organisational and Regulatory Aspects	RMG	Business continuity: incident response and recovery planning	***	Continuity plan (Continuity management)	Found and Recorded
31	Human, Organisational and Regulatory Aspects	RMG	Risk Assessment and Management Principles	Risk assessment and management methods	Asset Evaluation and Business Impact Analysis (Business impact analysis - in information asset classification)	Found and Recorded
32	Human, Organisational and Regulatory Aspects	RMG	Risk Definition	Risk assessment	Risk Identification Analysis	Found and Recorded
33	Human, Organisational and Regulatory Aspects	RMG	Risk Assessment and Management Principles	Security metrics	Risk Quantification (Risk – measuring)	Found and Recorded
34	Human, Organisational and Regulatory Aspects	RMG	Business continuity: incident response and recovery planning	***	Risk Response development and control	Found and Recorded
35	Human, Organisational and Regulatory Aspects	RMG	Risk Governance	Enacting security policy	Security Policy	Found and Recorded
36	Human, Organisational and Regulatory Aspects	RMG	Business continuity: incident response and recovery planning	***	Compliance and Business Continuity	Found and Recorded

39	Attacks and Defences	SOIM	Human factors: incident management	Handle: actual incident response	Containment, Eradication and Recovery (Containment in Incident response plan)	Found and Recorded

Step D:– Mapping with CyBOK Knowledge Trees: –

Continue your search with this document. If your remaining **(Not Found)** ***keywords*** or a ***set of keywords*** are found in this part, then record these in the table and move on to the next ***keywords*** or a ***set of keywords***. Repeat the process until the last ***keywords*** or a ***set of keywords***. **(Move to step E)**

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword or a set of Keywords	Mapping with CyBOK Knowledge Trees
1	CyBOK Introduction	CI	Foundational Concepts	Definition of cyber security	Protecting Your Computer and its Contents	Found and Recorded
5	Human, Organisational and Regulatory Aspects	POR	Control	***	Privacy Guidelines (privacy policy interpretability)	Found and Recorded
12	Attacks and Defences	AB, LR	Characterisation of Adversaries	cyber-enabled crime vs cyber-dependent crime OR interpersonal crimes OR cyber-enabled organised crime OR cyber-dependent organised crime	Internet Fraud	Found and Recorded (Selected AB as relevant)
17	Attacks and Defences	F	Definitions and conceptual models	Legal Concerns and the Daubert Standard	Evidentiary Reporting	Found and Recorded
19	Attacks and Defences	SOIM	Knowledge: Intelligence and analytics	***	Reconnaissance	Found and Recorded
22	Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Software Design and Architecture	Found and Recorded
23	Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Software Testing	Found and Recorded
25	Software and Platform Security	WAM	Fundamental concepts and approaches	Webification	The Web Model	Found and Recorded
27	Software and Platform Security	WAM	Fundamental concepts and approaches	Webification	HTML5 Security	Found and Recorded

Step E:– Complete final missing keywords using the Tabular representation of CyBOK broad categories, knowledge areas and their description: –

If the ***keywords*** or a ***set of keywords*** are not found in any of the materials provided to support the mapping process then identify the most relevant knowledge area using this document and then record the relevant KA.

Not Applicable - All the keywords have been mapped by using Step A to D

1.3 Finalising Phase:

This phase is a result of the mapping process; the results are transferred from the various tables to the **Final table**. It will be helpful to fill **Table (3.3)** in the application for NCSC certification. **Table (3.3)** is required as a part of the application for NCSC certification.

Broad Category	KA	Topic	Indicative Material	Keyword/ Set of Keywords/Course keywords
CyBOK Introduction	CI	Foundational Concepts	Definition of cyber security	Protecting Your Computer and its Contents
Infrastructure Security	NS	Network Defence Tools	***	Securing computer networks - Basics of networking
Software and Platform Security	SS	Categories of vulnerability	CVEs and CWEs	Compromised Computers
System Security	C	Public key cryptography	***	Secure Communications and Information Security Best Practices
Human, Organisational and Regulatory Aspects	POR	Control	***	Privacy Guidelines
Human, Organisational and Regulatory Aspects	POR	Control	***	Privacy
Human, Organisational and Regulatory Aspects	LR	Intellectual Property	Understanding intellectual property OR Catalogue of intellectual property rights	Intellectual Property
Human, Organisational and Regulatory Aspects	LR	Ethics	Codes of conduct	Professional Ethics
Human, Organisational and Regulatory Aspects	POR	Privacy technologies and democratic values	Censorship resistance and freedom of speech	Freedom of Speech
Infrastructure Security	NS	Network protocols and vulnerability	Common network attacks	Ethical Hacking
Human, Organisational and Regulatory Aspects	LR	Intellectual Property	Catalogue of intellectual property rights	Trademarks
Attackafe and Defences	AB	Characterisation of Adversaries	cyber-enabled crime vs cyber-dependent crime OR interpersonal crimes OR cyber-enabled organised crime OR cyber-dependent organised crime	Internet Fraud
Attacks and Defences	F	Definition and conceptual model	Digital (forensic) trace	Electronic Evidence
Human, Organisational and Regulatory Aspects	LR	Computer Crime	Crimes against information systems	Cybercrimes
Attacks and Defences	F	Definition and conceptual model	Forensic science	Forensic Technologies
Attacks and Defences	F	Main Memory Forensics OR Operating System Analysis OR Cloud Forensics	***	Digital Evidence Collection
Attacks and Defences	F	Definitions and conceptual models	Legal Concerns and the Daubert Standard	Evidentiary Reporting
Systems Security	AAA	Authorisation	Access Control	Layered Defense
Attacks and Defences	SOIM	Knowledge: Intelligence and analytics	***	Reconnaissance
Attacks and Defences	SOIM	Knowledge: Intelligence and analytics	Cyber-threat intelligence	Outsider Threat Protection
Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Software Construction

Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Software Design and Architecture
Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Software Testing
Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Methodologies
Software and Platform Security	WAM	Fundamental concepts and approaches	Webification	The Web Model
Software and Platform Security	WAM	Fundamental concepts and approaches	Cookies	Cookies
Software and Platform Security	WAM	Fundamental concepts and approaches	Webification	HTML5 Security
Attacks and Defences	RMG	Business Continuity: Incident Response and Recovery Planning	***	Managing a Business Information Continuity Plan
Software and Platform Security	SS	Categories of Vulnerabilities (SS) OR Prevention of Vulnerabilities,	***	Vulnerabilities and control
Human, Organisational and Regulatory Aspects	RMG	Business continuity: incident response and recovery planning	***	Continuity Plan
Human, Organisational and Regulatory Aspects	RMG	Risk Assessment and Management Principles	Risk assessment and management methods	Asset Evaluation and Business Impact Analysis
Human, Organisational and Regulatory Aspects	RMG	Risk Definition	Risk assessment	Risk Identification
Human, Organisational and Regulatory Aspects	RMG	Risk Assessment and Management Principles	Security metrics	Risk Quantification
Human, Organisational and Regulatory Aspects	RMG	Business continuity: incident response and recovery planning	***	Risk Response development and control
Human, Organisational and Regulatory Aspects	RMG	Risk Governance	Enacting security policy	Security Policy
Human, Organisational and Regulatory Aspects	RMG	Business continuity: incident response and recovery planning	***	Compliance and Business Continuity
Attacks and Defences	SOIM	Human Factors: Incident Management	Prepare: incident management planning	Incident preparation
Attacks and Defences	SOIM	Human Factors: Incident Management	Prepare: incident management planning	Incident Detection and Analysis
Attacks and Defences	SOIM	Human factors: incident management	Handle: actual incident response	Containment, Eradication, and Recovery
Attacks and Defences	SOIM	Human Factors: Incident Management	Follow up - Post-incident activities	Post-incident cyber services

Note :- Some topics are too broad to be covered in a single KA, therefore if terms are so broad, they can't be mapped without more context. It is better to consider the context and then record the appropriate Indicate Material, Topic, Knowledge Areas and Broad Category.

*** Indicated that there is no direct mapping of keyword with Indicative material but with Topic coverage.

2 SOURCE OF MODULE CONTENTS

https://professional.mit.edu/course-catalog/applied-cybersecurity