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 UNIVERSITY OF SURREY, UK

Information Security Management (COMM037)

Introduction to Information Security

- The business need for security:
- Confidentiality, availability, integrity et al
- Components of an information system: Software, hardware, data, people, procedures
- System and security development lifecycles

Risk Management

- Risk Management terminology: Agents, threats, vulnerabilities, etc
- Risk Identification assessment (quantitative and qualitative)
- Risk appetite and residual risk
- Selecting a risk control strategy

Planning for Security

- Methodologies for Information Security Evaluation and Assurance
- ISO 27000, Common Criteria
- Security education and training
- Continuity strategies

The role of cryptography in security

- Cryptographic algorithms and their application
- Cryptographic tools, PKI, digital signatures
- Examples of secure protocols

Practical Information Security Management

- Formal security modelling and analysis
- Penetration testing approaches and tools

Security technologies

- Firewalls and VPNs
- Intrusion detection, scanning and analysis tools
- Physical security controls

Implementing Information Security

- Information security project management

- Technical aspects
- Non-technical aspects

1.1 Formation Phase:

Information Security Management (COMM037)

Introduction to Information Security

- The business need for security
- Confidentiality, availability, integrity et al
- Components of an information system: Software, hardware, data, people, procedures
- System and security development lifecycles

Risk Management

- Risk Management terminology: Agents, threats, vulnerabilities, etc
- Risk Identification assessment (quantitative and qualitative)
- Risk appetite and residual risk
- Selecting a risk control strategy

Planning for Security

- Methodologies for Information Security Evaluation and Assurance
- ISO 27000, Common Criteria
- Security education and training
- Continuity strategies

The role of cryptography in security

- Cryptographic algorithms and their application
- Cryptographic tools, PKI, digital signatures
- Examples of secure protocols

Practical Information Security Management

- Formal security modelling and analysis
- Penetration testing approaches and tools

Security technologies

- Firewalls and VPNs
- Intrusion detection, scanning and analysis tools
- Physical security controls

Implementing Information Security

- Information security project management
- Technical aspects
- Non-technical aspects

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					The business need for security	Not Found
2					Confidentiality, availability, integrity	Found but not recorded (Not relevant as per the context
3					Components of an information system: Software, hardware, data, people, procedures	Not Found
4					System and security development lifecycles	Not Found
5	Human, Organisational and Regulatory Aspects	RMG	Risk Definition	Risk Management	Risk Management terminology	Found and Recorded
6					Agents, threats, vulnerabilities	Not Found
7	Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	. Risk assessment and management methods	Risk Identification, assessment (quantitative and qualitative)	Found and Recorded
8					Risk appetite and residual risk	Not Found
9	Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	Risk assessment and management methods	Selecting a risk control strategy	Found and Recorded

10					Methodologies for Information Security Evaluation and Assurance	Not Found
11					ISO 27000, Common Criteria	Not Found
12					Security education and training	Not Found
13					Continuity Strategies	Not Found
14					Cryptographic algorithms and their application	Not Found
15					Cryptographic tools, PKI, digital signatures	Not Found
16					Examples of secure protocols	Not Found
17					Formal security modelling and analysis	Not Found
18					Penetration testing approaches and tools	Not Found
19					Firewalls	Not Found
20	Infrastructure Security	NS	Network defence tools	Intrusion detection system	Intrusion detection, scanning and analysis tools	Found and Recorded
21					Physical security controls	Not Found
22					Information security project management, Technical aspects, Non-technical aspects	Not Found
23					VPN	Not Found

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	Human, Organisational and Regulatory Aspects	RMG	The business need for security (Business Model for Information Security)	Found and Recorded
2			Confidentiality, availability, integrity	Found but not recorded (Not relevant as per the context
3			Components of an information system: Software, hardware, data, people, procedures	Not Found
4	Software and Platform Security	SSL	System and security development lifecycles	Found and Recorded

6	Attacks and Defences	AB	Agents, threats, vulnerabilities	Found and Recorded
8	Human, Organisational and Regulatory Aspects	RMG	Risk appetite and residual risk	Found and Recorded
10	Human, Organisational and Regulatory Aspects	RMG	Methodologies for Information Security Evaluation and Assurance (Effective information security governance assurance process)	Found and Recorded
11	Human, Organisational and Regulatory Aspects	RMG	ISO 27000, Common Criteria	Found and Recorded
12	Human, Organisational and Regulatory Aspects	HF	Security education and training (Awareness and education)	Found and Recorded
13	Human, Organisational and Regulatory Aspects	RMG, SOIM	Continuity Strategies (Business Continuity Management/Planning)	Found and Recorded (Selected RMG as relevant)
14	Systems Security	C	Cryptographic algorithms and their application	Found and Recorded
15	Systems Security	C	Cryptographic tools, PKI, digital signatures	Found and Recorded
16			Examples of secure protocols	Not Found
17			Formal security modelling and analysis	Not Found
18	Software and Platform Security	SSL, SOIM	Penetration testing approaches and tools	Found and Recorded (Selected SSL as relevant)
19	Infrastructure Security	NS	Firewalls and VPNs	Found and Recorded
21			Physical security controls	Not Found
22			Information security project management, Technical aspects, Non-technical aspects	Not Found
23	Infrastructure Security	NS	VPN	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
1	Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	***	The business need for security (Business Model for Information Security)	Found and Recorded
4	Software and Platform Security	SSL	Motivations for secure software lifecycle	***	System and security development lifecycles	Found and Recorded
6	Attacks and Defences	AB	Characterisation of Adversaries	***	Agents, threats, vulnerabilities	Found and Recorded
8	Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	Elements of risk	Risk appetite and residual risk	Found and Recorded

10	Human, Organisational and Regulatory Aspects	RMG	Risk Assessment and Management Principles	Risk assessment and management methods	Methodologies for Information Security Evaluation and Assurance (Effective information security governance assurance process)	Found and Recorded
11	Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management Principles	Risk assessment and management methods	ISO 27000, Common Criteria	Found and Recorded
12	Human, Organisational and Regulatory Aspects	HF	Awareness and education	Terms	Security education and training (Awareness and education)	Found and Recorded
13	Human, Organisational and Regulatory Aspects	RMG, SOIM	Business continuity: incident response and recovery planning	ISO/IEC 27034 or NCSC guidance	Continuity Strategies (Business Continuity Manage-ment/Planning)	Found and Recorded (Selected RMG as relevant)
14	Systems Security	C	Schemes	AES or RSA or DES or PKCS or DSA or Kerberos or TLS	Cryptographic algorithms and their application	Found and Recorded
15	Systems Security	C	Public key cryptography	Public- key encryption or public key signature	Cryptographic tools, PKI, digital signatures	Found and Recorded
18	Software and Platform Security	SSL, SOIM	Prescriptive Processes	SAFECode	Penetration testing approaches and tools	Found and Recorded (Selected SSL as relevant)
19	Infrastructure Security	NS	Network defence tools	Packet filters	Firewalls	Found and Recorded
23	Infrastructure Security	NS	Network defence tools	Link Layer Security	VPN	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
2					Confidentiality, availability, integrity	Found but not recorded (Not relevant as per the context
3	CyBOK Introduction	CI	Foundational Concepts	Definition of cyber security	Components of an information system: Software, hardware, data, people, procedures	Found and Recorded
16	Formal Methods for Security	FMS	Modelling and Abstraction	Security models or Security properties	Examples of secure protocols	Found and Recorded
17	Formal Methods for Security	FMS	Modelling and Abstraction	Security models	Formal security modelling and analysis	Found and Recorded
21					Physical security controls	Not Found
22					Information security project management, Technical aspects, Non-technical aspects	Not Found

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.

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword or a set of Keywords	Searching in Tabular representation of CyBOK broad categories, knowledge areas
2	CyBOK Introduction	CI	Foundational Concepts	Objective of cyber security	Confidentiality, availability, integrity	Found and Recorded
21					Physical security controls	Out of Scope
22					Information security project management, Technical aspects, Non-technical aspects	Out of Scope

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
Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	* * *	The business need for security
CyBOK Introduction	CI	Foundational Concepts	Objectives of cyber security	Confidentiality, availability, integrity
CyBOK Introduction	CI	Foundational Concepts	Definition of cyber security	Components of an information system: Software, hardware, data, people, procedures
Software and Platform Security	SSL	Motivations for secure software lifecycle	* * *	System and security development lifecycles
Human, Organisational and Regulatory Aspects	RMG	Risk Definition	Risk management	Risk Management terminology
Attacks and Defences	AB	Characterisation of Adversaries	* * *	Agents, threats, vulnerabilities
Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	Risk assessment and management methods	Risk Identification, assessment (quantitative and qualitative)
Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	Elements of risk	Risk appetite and residual risk
Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	Risk assessment and management methods	Selecting a risk control strategy
Human, Organisational and Regulatory Aspects	RMG	Risk Assessment and Management Principles	Risk assessment and management methods	Methodologies for Information Security Evaluation and Assurance
Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	Risk assessment and management methods	ISO 27000, Common Criteria
Human, Organisational and Regulatory Aspects	HF	Awareness and education	Terms	Security education and training
Human, Organisational and Regulatory Aspects	RMG	Business continuity: incident response and recovery planning	ISO/IEC 27034 or NCSC guidance	Continuity Strategies
Systems Security	C	Schemes	AES or RSA or DES or PKCS or DSA or Kerberos or TLS	Cryptographic algorithms and their application
Systems Security	C	Public key cryptography	Public- key encryption or public key signature	Cryptographic tools, PKI, digital signatures
Formal Methods for Security	FMS	Modelling and Abstraction	Security models or Security properties	Examples of secure protocols
Formal Methods for Security	FMS	Modelling and Abstraction	Security models	Formal security modelling and analysis
Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Penetration testing approaches and tools
Infrastructure Security	NS	Network defence tools	Packet filters	Firewalls
Infrastructure Security	NS	Network defence tools	Intrusion detection systems	Intrusion detection, scanning and analysis tools
			Out of Scope	Physical security controls
			Out of Scope	Information security project management, Technical aspects, Non-technical aspects

Infrastructure Security	NS	Network defence tools	Link Layer Security	VPN

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://catalogue.surrey.ac.uk/2020-1/module/COMM037/SEMR1/1