Mapping University Degrees to CyBOK for NCSC Certification: Summary

Overview

This document summarises the process for mapping university degree content to the Cyber Security Body of Knowledge (CyBOK) to support applications for NCSC certification. It is intended for academic stakeholders and mapping practitioners. For the sake of clarity, we present an illustrative example derived from the Information Security Management module offered at the University of Surrey. The full example can be accessed at the following link. To support an application for NCSC certification, the steps outlined below must be applied to each individual module that contributes to the cyber security content of the degree programme analysed.

Step 1: Extract keywords from: module outlines, learning outcomes, assessment descriptions, lecture content, etc.

Note: Redundancy of keywords is not relevant in this phase.

Example: Confidentiality, availability, integrity et al, Physical security controls, Formal security modelling and analysis, Agents, threats, vulnerabilities, Penetration testing approaches and tools, Risk Management Terminology.

Step 2: Search the Alphabetical Indicative Material for direct matches, then populate Table 1.

Example:

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword(s)	Mapping Status
1					Confidentiality, availability, integrity	Found but not recorded(Not relevant as per context)
2					Physical security controls	Not Found
3					Formal security modelling and analysis	Not Found
4					Agents, threats, vulnerabilities	Not Found
5					Penetration testing approaches and tools	Not Found
6	Human, Organisational and Regulatory Aspects	RMG	Risk Definition	Risk Management	Risk Management Terminology	Found and Recorded

Note: At this step, it is likely that Table 1 will include many terms with a 'Not Found' mapping status. This is not an issue.

Step 3: Use the CyBOK Mapping Reference 1.3 for unmatched terms, then populate Table 2

Example:

S.No.	Broad Category	KA	Keyword(s)	Mapping Status
1			Confidentiality, availability, integrity	Found but not recorded(Not relevant as per context)
2			Physical security controls	Not Found
3			Formal security modelling and analysis	Not Found
4	Attacks and Defences	AB	Agents, threats, vulnerabilities	Found and Recorded
5	Software and Platform Security	SSL, SOIM	Penetration testing approaches and tools	Found and Recorded(Selected SSL as relevant)

Note: At this step, it is very likely that many of the terms with a 'Not Found' mapping status will be mapped. Those that are will be further contextualised in Step 4. Those that are not will be used in Step 5 and 6.

Step 4: Use the CyBOK Knowledge Trees to identify specific topics and indicative material for terms found in Step B, then populate Table 3.

Example:

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword(s)	Mapping Status
4	Attacks and Defences	AB	Characterisation of Adversaries	***	Agents, threats, vulnerabilities	Found and Recorded
5	Software and Platform Security	SSL, SOIM	Prescriptive Processes	SAFECode	Penetration testing approaches and tools	Found and Recorded(Selected SSL as relevant)

Note: At this step, it is possible that for some terms, an indicative material reference will not be found. This is not an issue, but needs to be marked with '***'.

Step 5: Search the CyBOK Knowledge Trees directly for any remaining unmatched terms, then populate Table 4.

Example:

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword(s)	Mapping Status
1					Confidentiality, availability, integrity	Found but not recorded(Not relevant as per context)
2					Physical security controls	Not Found
3	Formal Methods for Security	FMS	Modelling and Abstraction	Security Models	Formal security modelling and analysis	Found and Recorded

Note: At this step, it is possible that some terms will maintain the 'Not Found' mapping status. This is still not an issue.

Step 6: Use the Tabular Representation of CyBOK Categories to infer mappings for any final unmatched terms, then populate Table 5.

Example:

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword(s)	Mapping Status
1	CyBOK Introduction	CI	Foundational Concepts	Objective of cyber security	Confidentiality, availability, integrity	Found and Recorder
2					Physical security controls	Out of Scope

Note: If any of the terms still remains unmapped, it should be marked as 'Out of Scope'.

Step 7: Transfer all validated mappings to Table 6, then use it to populate the official NCSC Table 4.3, for the respective MSc or BSc programme.

Example:

Broad Category	KA	Topic	Indicative Material	Keyword(s)
CyBOK Introduction	CI	Foundational Concepts	Objective of cyber security	Confidentiality, availability, integrity
			Out of Scope	Physical security controls
Formal Methods for Security	FMS	Modelling and Abstraction	Security Models	Formal security modelling and analysis
Attacks and Defences	AB	Characterisation of Adversaries	***	Agents, threats, vulnerabilities
Software and Platform Security	SSL	Prescriptive Processes	SAFECode	Penetration testing approaches and tools
Human, Organisational and Regulatory Aspects	RMG	Risk Definition	Risk Management	Risk Management Terminology

We hope this summary supports those involved in the mapping process by offering a clear and structured approach. Your careful application of these steps will help ensure that each module is accurately and meaningfully aligned with CyBOK.

For further guidance and additional examples, please refer to the official CyBOK website at www.cybok.org, or contact us at contact@cybok.org with any questions.