CyBOK Mapping Framework

How to map concepts in academic and professional programmes to the Cyber Security Body of Knowledge

Awais Rashid | University of Bristol

Lata Nautiyal | University of Bristol

Joseph Hallett | University of Bristol

Ben Shreeve | University of Bristol

Version 1.0
February 22, 2021
http://www.cybok.org

COPYRIGHT

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at **contact@cybok.org** to let the project know how they are using CyBOK.

1 INTRODUCTION

The purpose of this document is to describe the overarching framework for mapping concepts covered in education and training programmes, e.g., undergraduate and postgraduate degrees at higher education institutions or professional certifications delivered by organisations such as (ISC)[2] and ISACA. The document describes the overall mapping approach and the resources available to undertake such mapping. It then summarises the use of the framework in mapping undergraduate and postgraduate programmes to the NCSC Certified Degree requirements.

> Details of the mapping to NCSC certified degrees have been published previously (see: **https://www.cybok.org/media/downloads/CyBOK_Mapping_Framework_Final_-_30_July_20.pdf**) and are, therefore, not repeated here. Interested readers are referred to the published approach and exemplars.

This is followed by a detailed description of how professional certification programmes may be mapped on to CyBOK along with an exemplar mapping of Certified Information Systems Security Professional (CISSP) and the method followed to undertake this mapping. The relevant dataset is made available[1].

This document should be read in conjunction with the materials available on the CyBOK website, primarily:

- CyBOK Version 1.0 – It is expected that the reader is, at the very least, familiar with the overall content of CyBOK, e.g., by reading the Table of Contents and Introduction to CyBOK as well as watching the webinar providing an overview of CyBOK, its background and the various use cases it enables.
- CyBOK Mapping Reference (Version 1.1 or 1.2 as appropriate) – which provides a quick lookup mechanism for identifying the Knowledge Areas (KAs) where common cyber security concepts may appear within CyBOK.
- CyBOK Knowledge Trees – which provide a hierarchical representation of the concepts covered within each of the KAs within CyBOK (knowledge trees are also available for the Introduction to CyBOK and the Formal Methods for Security KA, which is currently in development).
- Tabular representation of CyBOK's broad categories, knowledge areas and their description – providing a summary overview of the core elements covered within the detailed text of each KA.

[1] **https://cybok.org/media/downloads/cissp_data.zip**

2 MAPPING FRAMEWORK

The mapping framework (Figure 1) requires a list of concepts – typically in the form of key words or phrases (KWoPs)[2] that represent the concepts covered in the programme material – that are to be mapped on to CyBOK.

A user starts by looking up a KWoP using the CyBOK Mapping Reference (and any other additional look up material that may have been developed[3]) in order to identify the relevant KA (or Introduction to CyBOK) where the content may reside. The Knowledge Tree is then studied to identify the relevant concept within CyBOK. Note that the purpose here is not to do an exact string matching but to identify the topic or sub-topic within a knowledge tree to which a KWoP maps. If a suitable node cannot be found within the Knowledge Tree then the full text of the CyBOK Introduction or KA is studied to identify the mapping.

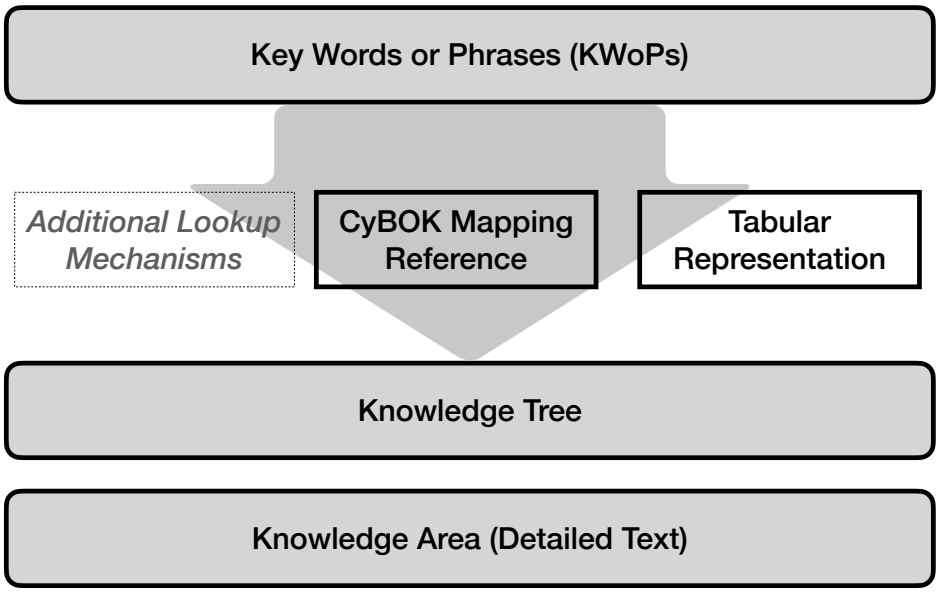

Figure 1: The General Mapping Framework

If the CyBOK mapping reference cannot identify a suitable knowledge tree then the tabular representation is used to identify the most suitable KA or KAs and the relevant knowledge trees and KA content are studied to identify the mapping.

Note that CyBOK's focus is to capture foundational knowledge. It is, therefore, by design, not encyclopaedic. A sufficient level of subject knowledge is required and expected to undertake the mappings. For instance, a KWoP or phrase "Writing SNORT Rules" is unlikely to find an exact mapping within CyBOK as writing such rules is a skill. However, the foundational knowledge is covered within the CyBOK KA on Security Operations and Incident Management (SOIM) under *analyse: analysis methods→misuse detection*[4].

Other knowledge that may be relevant to cyber security but is not within the direct scope of CyBOK is deemed out of scope. For instance, "Physical Security" of buildings and facilities

[2]For instance, as found in module descriptors in university education programmes or headings or topics covered in a reference guide for a professional programme.

[3]For instance, the mapping of degree programmes to NCSC certification includes an A to Z of the indicative material in the certification requirements as an additional look-up aid.

[4]SNORT is discussed as a specific example in the KA text under misuse detection.

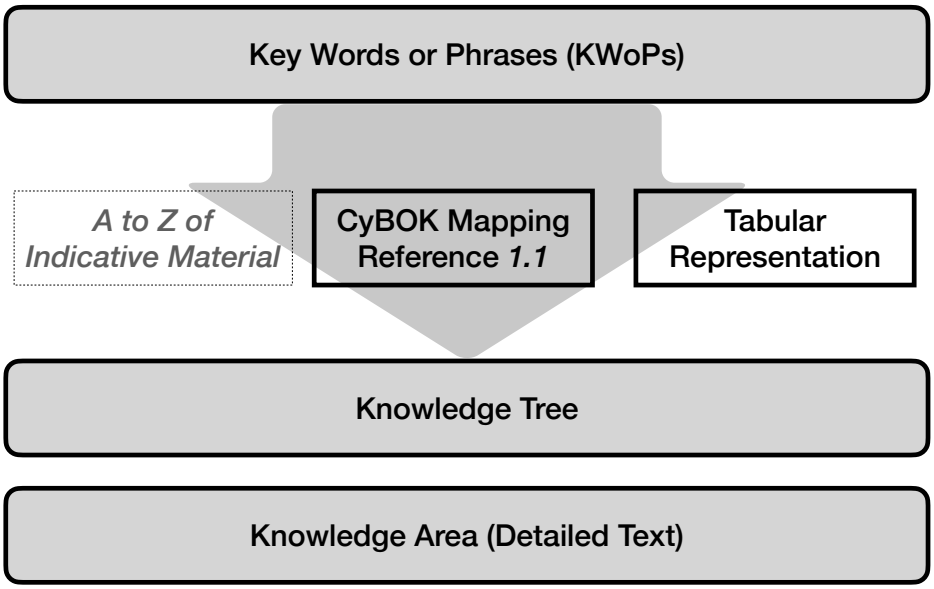

Figure 2: Instantiation of the Mapping Framework for Mapping University Degree Programmes to NCSC's Certification Requirements

is of high importance but this topic has extensive bodies of knowledge of its own and is out of scope of CyBOK. This is not meant to imply that it is not important but merely that the concepts are not covered within CyBOK and other suitable bodies of knowledge and guides should be consulted. Such concepts should be clearly denoted as *Out of Scope* when undertaking any mapping.

Finally, as CyBOK is a living document, it is likely that some relevant concepts are not covered or deemed too fine-grained for coverage in a foundational body of knowledge. These should be captured and users of the mapping framework are encouraged to get in touch with the CyBOK team[5]. CyBOK has been developed through input and efforts from the community within the UK and internationally. The team welcomes further feedback and community input on updates to CyBOK as it is a resource developed for the community and by the community.

3 MAPPING FRAMEWORK – USAGE IN MAPPING DEGREE PROGRAMMES TO NCSC CERTIFICATION

The Mapping Framework has been instantiated (Figure 2) to support mapping of degree programmes (undergraduate and postgraduate) to the NCSC's Certified Degrees requirements that are based on CyBOK. The NCSC Certification utilises level 2 (depth of nodes in the tree) in the CyBOK Knowledge Trees as *Indicative Material*. This specific instantiation, therefore, provides an additional quick look-up mechanism in the form of an *A to Z* based on this indicative material.

KWoPs are based on the contents of module descriptors developed as part of degree specifications in universities. A detailed step-by-step process for undertaking the mapping and developing the relevant Table required for submission to the NCSC Certification scheme is available on

[5]A web-based form is available to propose updates and revisions to CyBOK: **https://www.cybok.org/getinvolved/**

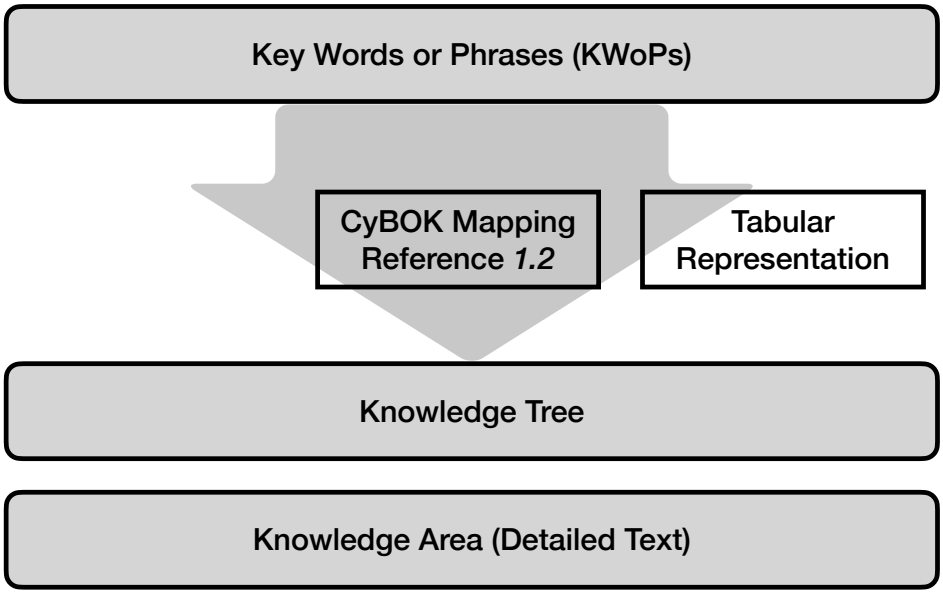

Figure 3: Instantiation of the Mapping Framework for Mapping Professional Certification Programmes to CyBOK. For this instantiation, we have updated the CyBOK Mapping Reference (to version 1.2) to include mapping of concepts to the CyBOK Introduction and the scope specification for the Formal Methods for Security KA.

the CyBOK website[6]. Note that the instantiation for degree programme mappings utilises the CyBOK Mapping Reference Version 1.1, the latest version at the time of instantiation. This version has since been superseded by Version 1.2 which is utilised in the mapping of professional certification programmes below. Both versions are available on the CyBOK website.

4 MAPPING FRAMEWORK – USAGE IN MAPPING PROFESSIONAL CERTIFICATIONS TO CYBOK

The Mapping Framework has also been instantiated (Figure 3) to support mapping of professional certifications, such as those offered by (ISC)[2] and ISACA, to CyBOK.

As shown in our prior investigations contrasting different certification programmes [1], such mappings can be used to understand the focus of different certification programmes and the knowledge they provide for a professional seeking to develop their knowledge with regards to particular KAs within CyBOK. The mappings (and resulting spider diagrams and bar charts) also provide a way for employers to contrast the suitability of different qualifications to the knowledge required for particular roles within the organisation[7].

[6] **https://www.cybok.org/usecases/**

[7] Note this equally applies to NCSC certified degrees where the mapping results in similar spider diagrams and bar charts to provide a high-level overview.

4.1 Mapping CISSP to CyBOK

For the CISSP mapping we utilised The Official (ISC)[2] CISSP CBK Reference, 5th Edition. The CISSP CBK is divided into 8 Domains. These domains encompass a range of topics. In order to identify KWoPs for mapping, we utilised the headings, subheadings and paragraph headings in each Domain. This provided us with a more detailed list of KWoPs compared to the Table of Contents[8]. An alternative would have been to use the Index. However, a number of the index terms overlap with the headings we utilised while others are too fine-grained and would normally fit under the broader umbrella of the concept covered by a heading as above. We excluded headings for shaded boxes as these are primarily specific examples relating to concepts being covered in the main text.

We undertook the mapping of each of the 8 domains individually and then aggregated the results to derive the overall spider diagrams and bar charts. This was done as domains are broad (and akin to CyBOK KAs) so the mapping of domain titles was unlikely to yield anything other than a very broad mapping to a KA title. This also enabled a level of depth whereby an interested reader can examine CISSP mapping to CyBOK as a whole or at the level of a Domain (we include such domain-level coverage in the Appendix).

The detailed method followed to derive the mappings – based on the framework in Figure 3 and is explained below. Multiple researchers cross-checked the mappings to validate them and ensure rigour.

1. Ten KWoPs were randomly selected from each of the 8 Domains – leading to 80 seed KWoPs to be mapped.
2. Two researchers jointly mapped the seed KWoPs (referring to their detailed descriptions as required) using the mapping framework in Figure 3. If a KWoP could not be mapped it was assigned to one of two categories: *Out of Scope* (e.g., physical security or basic software development knowledge that is not cyber security specific) or *Not in CyBOK* (a cyber security concept that is relevant but not found).

Examples of each mapping category:

- *Out of Scope:* Security and risk management → Contribute to and enforce personnel security policies and procedures → Candidate screening and hiring → Screening and interviewing
- *Not in CyBOK:* Security Architecture and Engineering → Implement and manage engineering processes using secure design principles → ISO/IEC 19249
- *Conceptual:* Asset security → Determine data security controls → Establishing the baseline Security ***maps to*** RMG → Risk assessment and management principles → Risk assessment and management methods
- *Specific:* Security and Risk Management → Establish and maintain a security awareness, education, and training program → Developing an awareness program → Security awareness strategy and plans ***maps to*** HF → Awareness and education → terms → training

[8] A total of 1158 KWoPs; we exclude the 8 top-level Domain headings as KWoPs as they are very broad and akin to CyBOK KAs and also generic headings such as “Summary”.

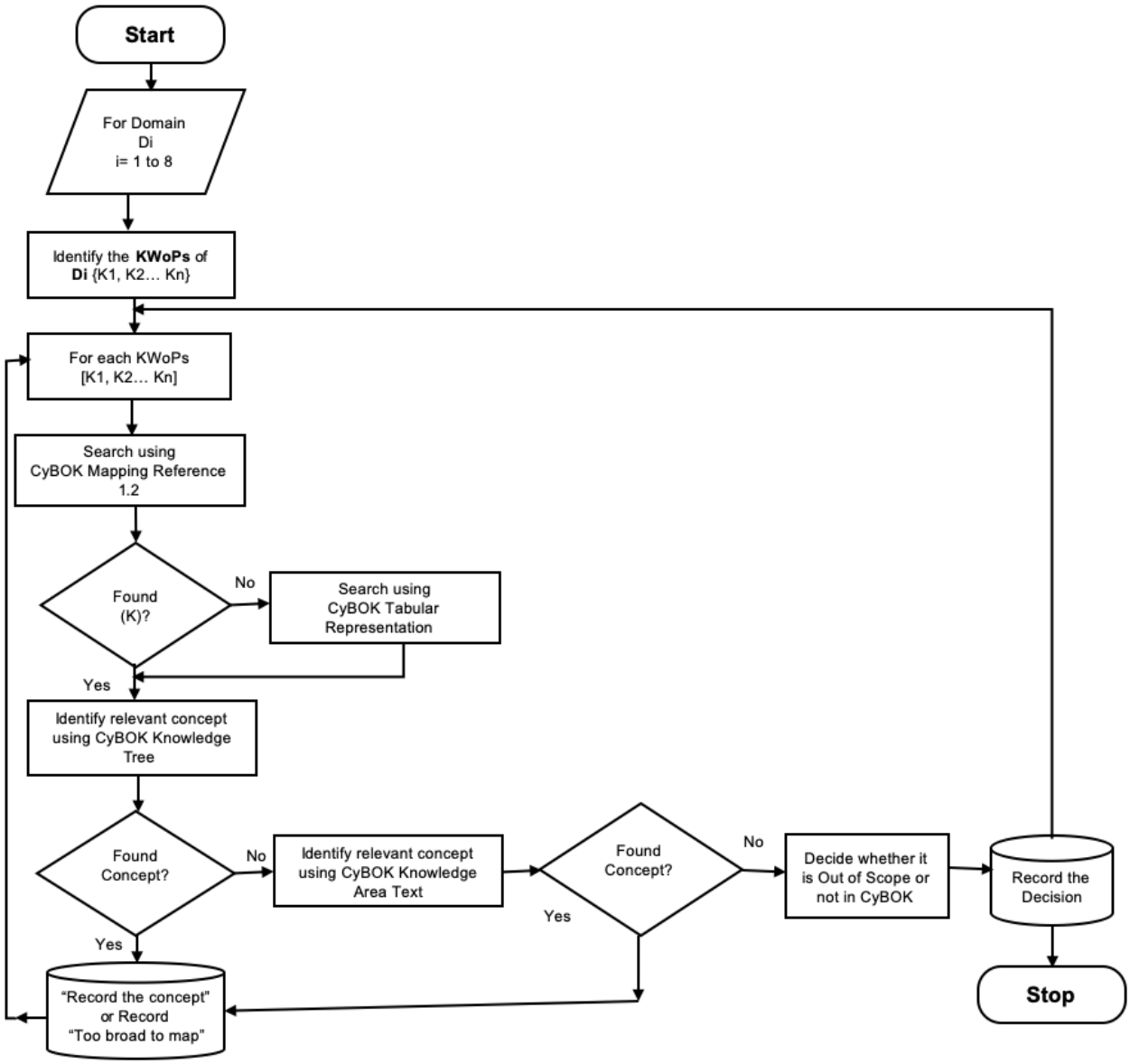

Figure 4: Flowchart depicting the mapping process followed by the researchers

The purpose of this collaborative coding was to establish a common understanding between the researchers regarding the mappings as well as what would be deemed out of scope or relevant but not found within CyBOK. KWoPs were mapped as *Conceptual* (e.g., where a KWoP refers to a specific tool that may not be directly covered in CyBOK but the overall concept and knowledge is covered; cf. example of SNORT rules above) or *Specific* where an exact mapping existed.

3. The researchers aimed to reach consensus but where consensus could not be reached this was referred to a senior researcher for discussion and decision.
4. The final seed mappings were reviewed by the senior researcher to ensure a further level of scrutiny on the mappings and their consistency.
5. The two researchers then independently mapped the remaining KWoPs per Domain. The process followed is shown as a flowchart in Figure 4. In some cases the KWoP (and the text underneath) covered abstract concepts that related to several CyBOK KAs. Such concepts were recorded as found but deemed "Too Broad to Map".

Mapping Type	Count
Specific	506
Conceptual	303
Out of scope	280
Too broad to map	47
Not in CyBOK	22

Table 1: KWoPs per mapping type

6. The two researchers then came together to discuss where their mappings agreed or disagreed with each other, aiming to resolve disagreements. This led to an initial proposal for the mappings.
7. The initial proposal for mappings (and researchers' individual mappings) were reviewed by a senior researcher who validated these further against the CISSP CBK text and CyBOK Knowledge Trees and KA texts. In cases where the mappings were inaccurate the senior researcher provided more accurate mappings with justifications. The two researchers then used these recommendations to update and finalise the mappings. The number of Conceptual and Specific Mappings as well as numbers of KWoPs deemed Out of Scope, Not in CyBOK or Too Broad to Map are shown in Table 1.
8. The spider diagrams and bar charts for each Domain and CISSP overall were then produced. These are shown in Figures 5 and 6.

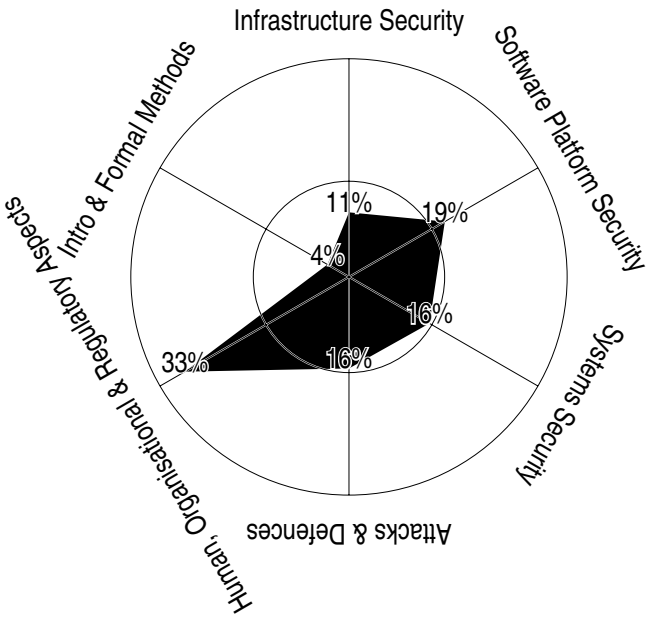

Figure 5: Mapping of CISSP to CyBOK's Broad Categories. Note that CyBOK Introduction and Formal Methods for Security KA are recorded as a sixth category.

As discussed above, the mappings enable one to establish how cyber security coverage in CISSP maps to the broad CyBOK categories and also the coverage on a per KA level. The analysis should not be read as a critique of CISSP but as an aide-mémoire to the level of coverage of particular knowledge types within CISSP. This can also serve a means to contrast CISSP with other professional certification frameworks. Further mappings of $(ISC)^2$ and ISACA certifications are under way and will be published in due course.

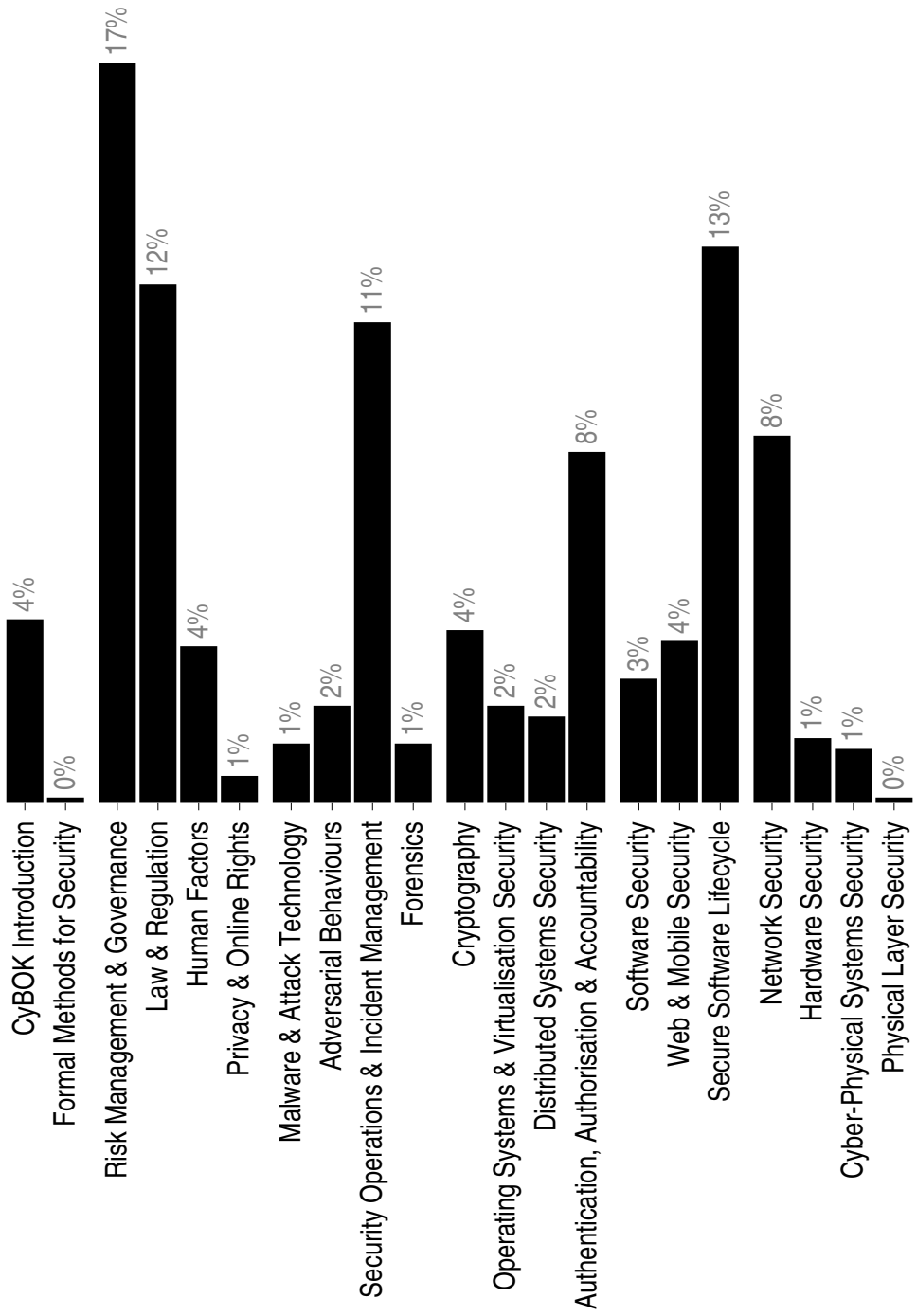

Figure 6: Mapping of CISSP to CyBOK's KAs.

The mapping of CISSP on a per-domain level also enables us to see coverage of CyBOK KAs in each CISSP domain. These are shown in Table 2 with detailed charts included in the Appendix.

CyBOK Knowledge Area	Security and Risk Management	Asset Security	Security Architecture and Engineering	Communication and Network security	Identity and Access Management	Security Assessment and Testing	Security Operations	Software Development Security	Total
Introduction	8	2	16	0	0	0	3	5	34
Formal Methods for Security	0	0	1	0	0	0	0	0	1
Risk Management & Governance	57	22	0	1	0	7	13	37	137
Law & Regulation	67	24	0	1	0	1	2	1	96
Human Factors	23	1	0	0	1	1	1	2	29
Privacy & Online Rights	0	5	0	0	0	0	0	0	5
Malware & Attack Technology	1	1	2	2	0	0	1	4	11
Adversarial Behaviour	17	0	0	0	0	0	0	1	18
Security Operations & Incident Management	14	7	2	2	0	12	40	12	89
Forensics	0	0	0	0	0	0	10	1	11
Cryptography	0	1	29	1	0	0	0	1	32
Operating Systems & Virtualization Security	1	1	6	4	0	0	2	4	18
Distributed Systems Security	0	1	2	3	0	0	0	10	16
Authentication, Authorization & Accountability	0	5	7	2	33	2	5	11	65
Software Security	0	0	3	0	0	1	0	19	23
Web & Mobile Security	0	0	23	0	0	0	0	7	30
Secure Software Lifecycle	5	0	2	0	0	16	1	79	103
Network Security	2	2	1	61	2	0	0	0	68
Hardware Security	0	2	10	0	0	0	0	0	12
Cyber-Physical Systems Security	2	0	4	2	0	0	0	2	10
Physical-Layer & Telecommunications	0	0	0	1	0	0	0	0	1

Table 2: Number of KWoPs per CISSP Domain mapped to each of the CyBOK KAs and the CyBOK Introduction

REFERENCES

[1] Joseph Hallett, Robert Larson, and Awais Rashid. Mirror, mirror, on the wall: What are we teaching them all? characterising the focus of cybersecurity curricular frameworks. In Wu-chang Feng and Ashley L. Podhradsky, editors, *2018 USENIX Workshop on Advances in Security Education, ASE 2018, Baltimore, MD, USA, August 13, 2018*. USENIX Association, 2018.

5 APPENDIX

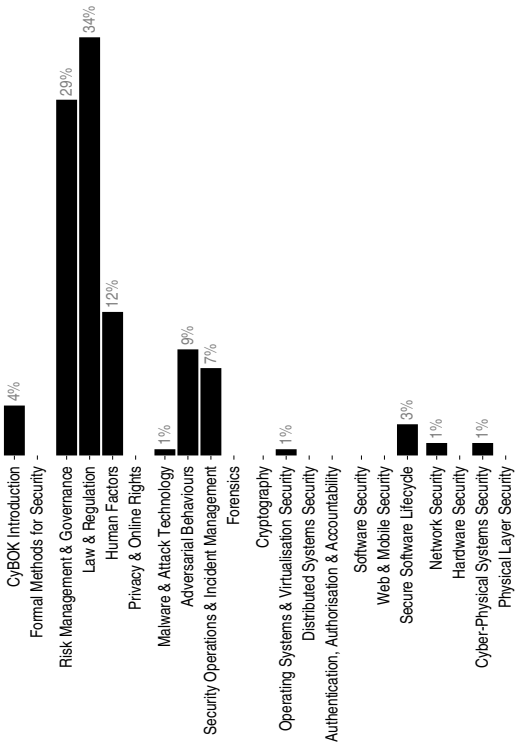

Figure 7: CISSP Domain 1: Security and Risk Management

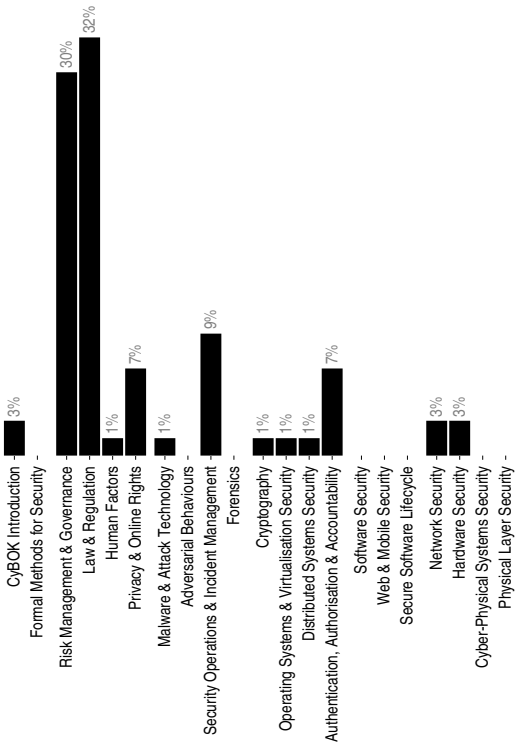

Figure 8: CISSP Domain 2: Asset Security

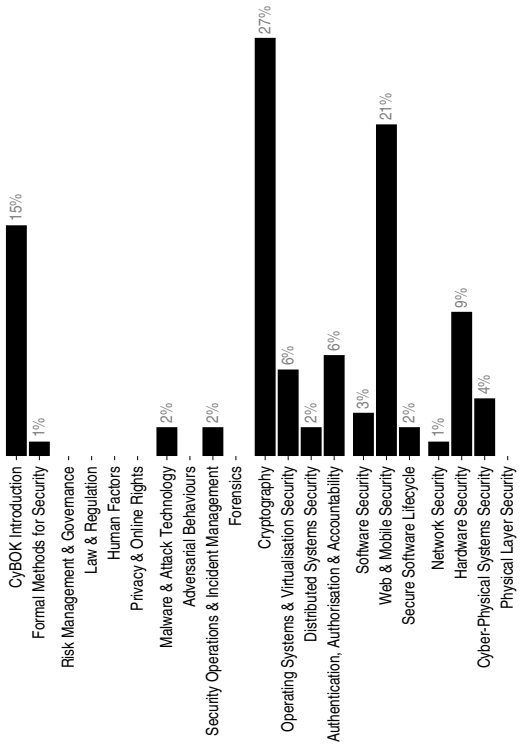

Figure 9: CISSP Domain 3: Security Architecture and Engineering

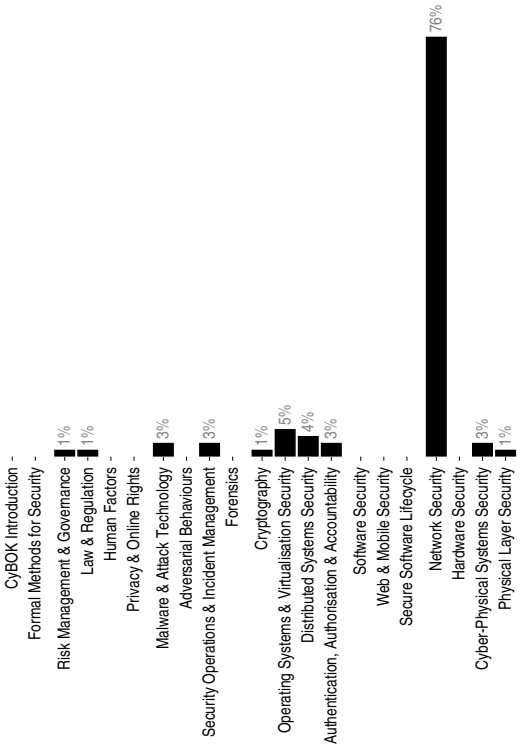

Figure 10: CISSP Domain 4: Communication and Network Security

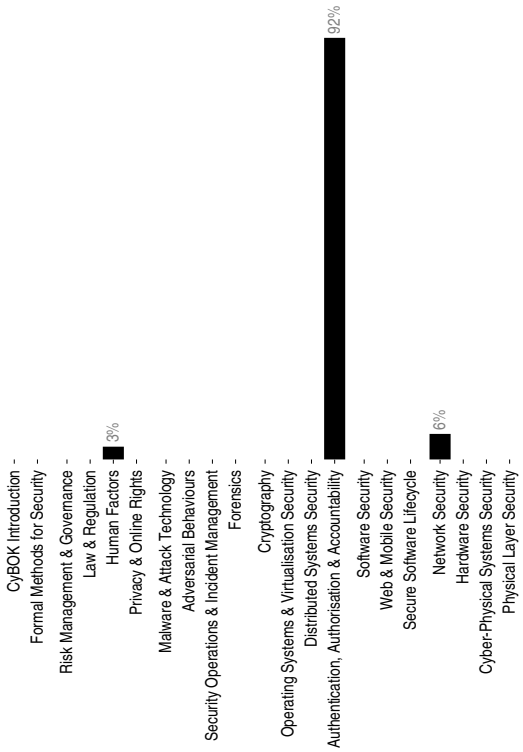

Figure 11: CISSP Domain 5: Identity and Access Management

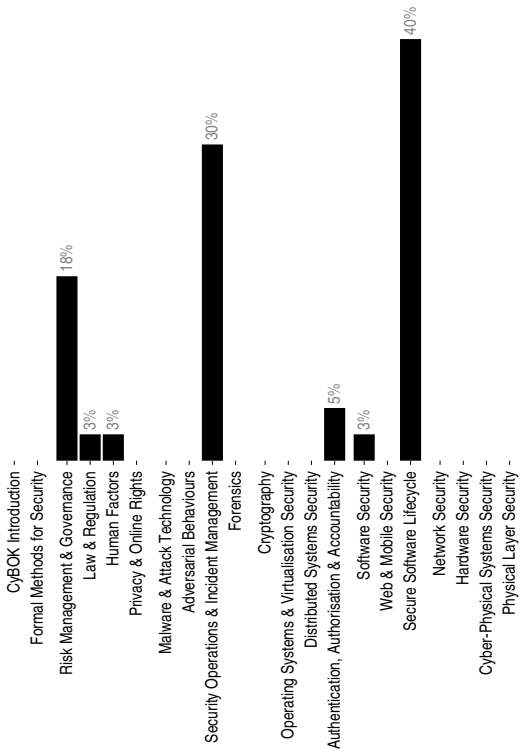

Figure 12: CISSP Domain 6: Security Assessment and Testing

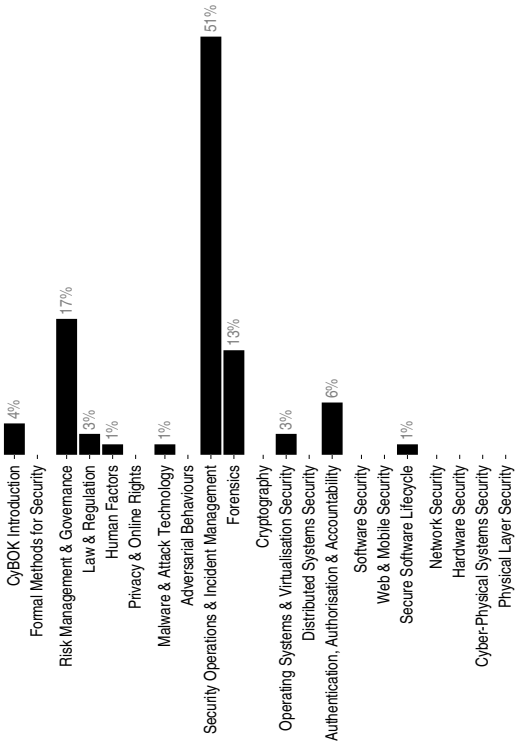

Figure 13: CISSP Domain 7: Security Operations

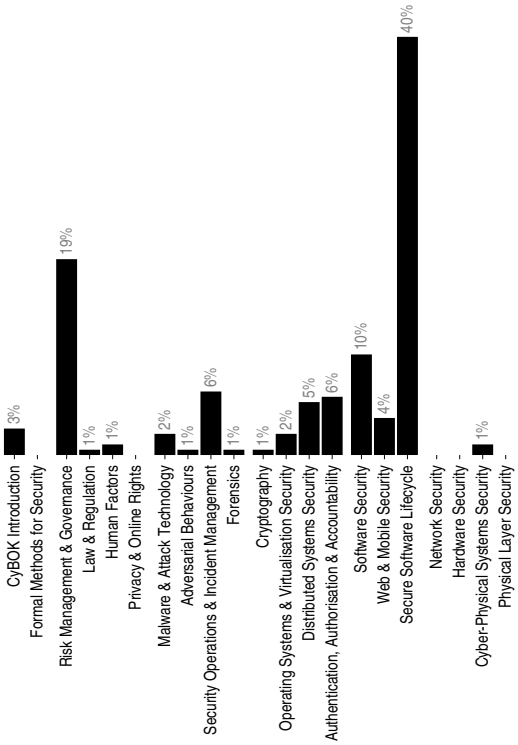

Figure 14: CISSP Domain 8: Software Development Security