CyBOK

Assessing the compatibility of CyBOK and the European Cybersecurity Skills Framework (ECSF)

Steven Furnell
University of Nottingham

Eliana Stavrou
Open University of Cyprus

July 2025

Table of Contents

1 Introduction

The need for suitably qualified and skilled cyber practitioners has achieved international recognition, with various initiatives having contributed towards an increased focus on understanding the requirements and growing the talent base. At the same time, however, there has been a clear divergence of approaches to understanding the associated knowledge and skills, and how these in turn are relevant to particular cyber security roles. In the UK there has been a move towards standardisation, with the UK Cyber Security Council defining a set of specialisms (UKCSC, 2025), which are in turn specified with direct reference to CyBOK (Rashid et al. 2021a) for Knowledge and the CIISec Skills Framework (CIISec, 2024) for Skills. In Europe, however, a more recent development has been ENISA's release of the European Cyber Skills Framework (ECSF), offering a set of 12 cyber role profiles (each of which is then specified based upon associated knowledge, skills and competencies). Given that CyBOK is explicitly mentioned in the ECSF User Manual (ENISA, 2022) as a possible external reference to enrich the framework's profile elements, it is therefore considered relevant to determine the extent to which CyBOK relates to ECSF profiles and can be utilized as a further reference point, supporting the interpretation, expansion, or practical application of ECSF's knowledge elements across its defined roles.

1.1 Aim and objectives

The aim of the study was to understand the potential for CyBOK to become a relevant knowledge reference for the ECSF roles, and to assess the extent to which the approaches (while not directly the same) are overlapping and potentially compatible in terms of their handling of cyber security knowledge.

The principal focus of the project activity has been to use the ECSF roles as currently specified as the starting point, then map the knowledge components of these against the CyBOK Knowledge Areas (KAs). Each ECSF profile includes an accompanying specification of key knowledge requirements, skills, and tasks, with the potential to extend or adapt them to meet specific needs. The project therefore assesses the extent to which CyBOK can be utilised as a reference source to ECSF roles. The investigations performed are based on the identification of key words and phrases from the ECSF profiles, and relate these to CyBOK via the use of Knowledge Trees and searching within the detailed content of the Knowledge Areas themselves.

In addition to providing a core mapping of the ECSF roles to CyBOK Knowledge Areas, the research investigates the following further issues of relevance and interest:

1. To what extent (if at all) do the knowledge requirements of the ECSF role descriptions reveal 'gaps' in the coverage offered by CyBOK?
2. Which KAs are the most prominently related to ECSF roles?
3. To what extent are any of the CyBOK KAs unused by ECSF role descriptions (i.e. which KAs are not clearly referenced for any roles)?

1.2 Report structure

The main content begins with a brief outline of the ECSF, highlighting the intention behind it and the 12 role profiles that it proposes. These – and in particular the Knowledge, Skills and Task descriptor statements used within them – provide the basis for the mapping to CyBOK.

Section 3 outlines the approach taken to map the ECSF material to the CyBOK Knowledge Base. The approach is based around key phases of the CyBOK Mapping Framework, and is focused upon the identification of Key Words and Phrases (KWoPs) from ECSF that can then be cross-referenced to tangible CyBOK content and coverage.

The main findings from the study are presented in Section 4, looking at the overall extent to which the ECSF roles can be related to CyBOK Knowledge Areas, and how this looks on a role-specific basis. The discussion also highlights areas of omission, where certain identified KWoPs could not be mapped to CyBOK, and where certain CyBOK Knowledge Areas remained unreferenced at the end of the process.

The report then concludes with reflections on the study, and potential implications for CyBOK and the ECSF as a result of the findings.

The main body is supported by two appendices, one presenting details of the KWoPs identified from each element of the ECSF source material, and the other detailing the mapping of the final KWoPs to the CyBOK Knowledge Areas and Knowledge Trees.

2 Background

The ECSF was released by the European Agency for Cybersecurity (ENISA) in 2022 and aims to provide "*an open tool to build a common understanding of the cybersecurity professional role profiles in Europe and common mappings with the appropriate skills and competences required*".

More specifically, ENISA outlines the role for the Framework as follows:

> "*The ECSF summarises the cybersecurity-related roles into 12 profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies. It provides a common understanding of the relevant roles, competencies, skills and knowledge mostly required in cybersecurity, facilitates recognition of cybersecurity skills, and supports the design of cybersecurity-related training programmes*."
>
> (ENISA, 2022)

The 12 profiles are as listed in Table 1, and it can be seen that these span a range of cybersecurity activities and responsibilities, as well as varying in terms of their areas of technical focus and specialisation. As a consequence, each role also varies in terms of the knowledge and skills that a role holder would be expected to have in order to undertake it.

Chief Information Security Officer (CISO)	Cybersecurity Educator
Cyber Incident Responder	Cybersecurity Implementer
Cyber Legal, Policy & Compliance Officer	Cybersecurity Researcher
Cyber Threat Intelligence Specialist	Cybersecurity Risk Manager
Cybersecurity Architect	Digital Forensics Investigator
Cybersecurity Auditor	Penetration Tester

Table 1 : The twelve ECSF Role Profiles

More specifically, all twelve roles are specified in terms of Knowledge, Skills, Tasks and e-Competences, and each is presented using a standardised template that also includes some other summary information. An example is provided in Figure 1, showing the profile for a *Cybersecurity Risk Manager*.

Profile Title	Cybersecurity Risk Manager	
Alternative Title(s)	Information Security Risk Analyst Cybersecurity Risk Assurance Consultant Cybersecurity Risk Assessor Cybersecurity Impact Analyst Cyber Risk Manager	
Summary statement	Manage the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports.	
Mission	Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls.	
Deliverable(s)	• Cybersecurity Risk Assessment Report • Cybersecurity Risk Remediation Action Plan	
Main task(s)	• Develop an organisation's cybersecurity risk management strategy • Manage an inventory of organisation's assets • Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems • Identification of threat landscape including attackers' profiles and estimation of attacks' potential • Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy • Monitor effectiveness of cybersecurity controls and risk levels • Ensure that all cybersecurity risks remain at an acceptable level for the organisation's assets • Develop, maintain, report and communicate complete risk management cycle	
Key skill(s)	• Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards • Analyse and consolidate organisation's quality and risk management practices • Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks • Build a cybersecurity risk-aware environment • Communicate, present and report to relevant stakeholders • Propose and manage risk-sharing options	
Key knowledge	• Risk management standards, methodologies and frameworks • Risk management tools • Risk management recommendations and best practices • Cyber threats • Computer systems vulnerabilities • Cybersecurity controls and solutions • Cybersecurity risks • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Cybersecurity-related certifications • Cybersecurity-related technologies	
e-Competences (from e-CF)	E.3. Risk Management E.5. Process Improvement E.7. Business Change Management E.9. IS-Governance	Level 4 Level 3 Level 4 Level 4

(Source: ENISA, 2022)

Figure 1 : The ECSF role profile for a Cybersecurity Risk Manager

It can be seen in Figure 1 that the key descriptive elements in characterising the role come from the lists of main tasks, key skills, and key knowledge. The e-Competences provide a broader view of the relevant ICT competences' areas linked to each role (based upon cross-reference to the European e-Competence Framework, e-CF).

The ECSF is the result of work conducted by ENISA's Ad-Hoc Working Group on the European Cybersecurity Skills Framework formed by experts representing various

viewpoints within the cyber security discipline. The developed framework is based on an analysis of existing frameworks, the results and findings from research on market needs, and resulting agreement among experts. The ECSF User Manual (ENISA, 2022) presents the principles that informed the design of ECSF, considering various stakeholders needs. As mentioned, "*the framework is designed to be suitably general to ensure that it may be easily understood and applied by a wider audience… This has been achieved by applying the appropriate level of detail to the content of the ECSF that is not too specific nor too abstract*". This characteristic enables ECSF to be extendable to meet specific needs. Indeed, the ECSF User Manual (ENISA, 2022) makes the specific statement that knowledge and skills within the role descriptions are provided as "guiding examples for flexible adaptation to the context" and that other sources may be used. It goes on to indicate the following in an associated footnote:

> "*The skills, knowledge and competences sections of the ECSF are neither exhaustive nor restrictive, allowing the user to enrich them by also including external resources e.g., the Cyber Security Body Of Knowledge (CyBOK) https://www.cybok.org/, JRC Classification https://joint-research-centre.ec.europa.eu/publications/unified-conceptual-framework-tasks-skills-and-competences_en*"
>
> (ENISA, 2022)

This having been said, and with CyBOK having been specifically identified as a potential reference, it is relevant to assess the extent to which it can serve this purpose by providing coverage of the issues and topics that the ECSF profiles suggest.

3 Approach

This section describes the main stages of the work undertaken to identify the key areas of coverage within the ECSF, and then map this to the Knowledge Base offered by CyBOK.

3.1 Identifying Key Words and Phrases

A fundamental part of the CyBOK mapping process is to identify Keywords and Phrases (KWoPs) from the source material that can then be cross-referenced to the CyBOK Knowledge Base.

Having examined the way in which the ECSF role profiles are presented, it was considered that drawing solely from the Knowledge statements for a given role could limit the potential for identifying sufficient KWoPs to characterise it. As such, the process also considered the text from the list of Skills and Tasks associated with each role.

Table 2 presents a series of illustrative extracts from the ECSF descriptor statements associated with Knowledge, Skills and Tasks, and demonstrates how KWoPs were identified and extracted from some of them. To explain the first three columns in the Table specifically:

- **Example Statements**: Presented examples of selected full 'statements' from the ECSF, using the same wording as the source material. These are grouped down the left side of the column to indicate whether the examples were sourced from Knowledge, Skill or Task statement sets.
- **Resulting KWoP(s):** Indicates whether or not the statement was considered suitable to be used as the basis for a KWoP (if so, then the resulting KWoP is indicated, otherwise there is a dash. The latter means that no attempt was then made to map the source statement against the CyBOK content).
- **CyBOK mapping:** Indicates the Knowledge Area(s) in which the chosen KWoPs were located within CyBOK (note that shaded boxes here indicate *Not Applicable* - they accompany the dashes from the *prior* column, which indicated that no KWoP was identified, and so no mapping was attempted). A dash in *this* column means that an attempt was made to map the selected KWoP, but related coverage was not found within CyBOK (or not found in a way that was compatible with the ECSF's intended usage – an aspect that is explained further below).

With the above in mind, it is important to note that a dash in the second column reflects a *decision* from the investigators that a given statement was not a suitable/appropriate candidate from which to draw a KWoP. Meanwhile, a dash in the third column means that a KWoP was chosen but then could not be mapped in CyBOK.

Example Statements		Resulting KWoP(s)	CyBOK mapping	Notes / Rationale
Knowledge	Advanced and persistent cyber threats (APT)	Advanced Persistent Threat / APT	MAT	Successful mapping.
	Auditing standards, methodologies and frameworks	Auditing	-	While CyBOK makes various references to audit and auditing, it is not doing so in a manner that matches the intention of the ECSF statement. ECSF is considering audit at the organisational level (e.g. institutional audit, audit plans, auditing standards, auditing frameworks etc), whereas the occurrences of the term within CyBOK relate to system-level audit and logging etc.
	Computer networks security	Network security	NS	Successful mapping.
	Computer programming	-		While CyBOK may mention aspects such as secure coding etc, the ECSF statement is referring to 'computing programming' in general, which is not what CyBOK is expected to be covering.
	Computer systems vulnerabilities	Vulnerability	RMG, SS	Successful mapping.
	Incident handling communication procedures	Incident handling	SOIM	Successful mapping.
	Conformity assessment standards, methodologies and frameworks	-		The issue of standards/methodologies/frameworks was picked up by other selected KWoPs. The issue in focus here is 'conformity', which CyBOK was not expected to cover in a significant way (a check of the content reveals there is passing mention in relation to certification marks).
	Cybersecurity trends	-		This was considered too broad/general to attempt to map, and CyBOK itself is not about tracking trends.
Skill	Manage and analyse log files	Log files	SOIM, SSL	Successful mapping.

Example Statements		Resulting KWoP(s)	CyBOK mapping	Notes / Rationale
	Manage cybersecurity resources	-		The is again a statement from which it was not considered meaningful to extract a KWoP – managing cybersecurity resources could involve elements from across a range of KAs rather than particular, focused content.
	Model threats, actors and TTPs	Threats / Threat actors / TTPs	AB, RMG, SOIM, SSL	Successful mapping.
	Motivate and encourage people	-		Related to soft skills, which are out of scope within CyBOK.
	Practice all technical, functional and operational aspects of cybersecurity incident handling and response	Incident handling / incident response	SOIM	Successful mapping.
	Perform social engineering	Social engineering	HF	Successful mapping.
	Review codes assess their security	-		An example of a statement from which a KWoP was not selected, but arguably could have been reframed as 'code review' and found a basic match within the SSL KA (where there is mention of code review tools)
	Select appropriate specifications, procedures and controls	-		The terms specifications, procedures and controls are all too general to be mapped to any specific content within CyBOK.
Tasks	Assess and manage technical vulnerabilities	Technical vulnerabilities	SS	Successful mapping.
	Collaborate with other teams and colleagues	-		Related to soft skills, which are out of scope within CyBOK.
	Develop, implement, maintain, upgrade, test cybersecurity products	-		The focus here is 'cybersecurity products' and CyBOK is not considered to be providing guidance specifically in this context. A broad match to the whole of the SSL KA could arguably be made, given that it refers to the lifecycle of software products, but this would not aid ECSF users in locating specific guidance.
	Ensure the organisation's resiliency to cyber incidents	Cyber incidents	SOIM	Successful mapping.

Example Statements		Resulting KWoP(s)	CyBOK mapping	Notes / Rationale
	Establish the target environment and manage auditing activities	Auditing	-	As above, the CyBOK coverage of auditing is not aligned to the interpretation that ECSF is using.
	Finding new approaches for education, training and awareness-raising	Education, training and awareness	HF, RMG	Successful mapping.
	Maintain and upgrade the security of systems, services and products	-		This is referring to a range of general activities, for which content from across the breadth of CyBOK could be relevant in different contexts, and so any KWoP-KA mapping would be too broad.
	Secure resources to implement the cybersecurity strategy	Cybersecurity strategy	-	Related coverage of this KWoP was not located in CyBOK.

Table 2 : KWoP identification based on example statements from ECSF Knowledge, Skills and Task descriptors

3.2 Subjectivity and threats to validity

As noted in Table 2, there are some instances where a different decision on the KWoP *selection* could have led to some broad mapping still being possible within CyBOK. This in turn reflects that the process of selecting KWoPs - from ECSF or any other source – will inevitably involve a level of subjectivity.

In practice, the KWoP section decisions then inform whether relevant CyBOK content will be identified or missed, and there are several challenges to the process:

- Some valid KWoPs can be very broad, making it difficult to narrow down the content (e.g. in the exercise it was found that several essentially mapped to whole KAs within CyBOK).
- Some are overly specific, such that a precise keyword match is not possible, and sometimes the concept is overly specific too.
- KWoPs may use different language and terminology to CyBOK, requiring the mappers to make associations and/or identify synonyms that enable relevant content to be identified even though not directly mapping the KWoP. Illustrative examples would be a KWoP relating to 'ethical hacking' where CyBOK more substantially refers to 'penetration testing'.
- Some of the KWoPs are closely related and sometimes represent duplicates (e.g. 'privacy by design' and 'privacy-by-design' were both identified from the ECSF source).

To reduce the level of subjectivity, the KWoP identification process involved distinct assessment of the ECSF statements by the investigators, to each identify KWoPs independently. Those identified by both parties were directly included, and others were discussed prior to inclusion or exclusion (with inclusion being the decision in most cases, to maximise the potential KWoPs being searched and mapped). Nonetheless, it is anticipated that if others were given the same 250+ ECSF statements and asked to select KWoPs from them, then they may still arrive at a final list that differs in *some* respects. However, given that most unused ECSF statements were excluded on the basis of being too broad or being out-of-scope for CyBOK, this would only leave a small number of edge cases where a KWoP may have been selected rather than not. As such, we do not consider that this will have affected the results significantly or represented a fundamental threat to the validity of the findings.

Additionally, the ECSF Skills statements have several points based around 'soft skills', some illustrative examples of which are listed below:

- Collaborate with other team members and colleagues
- Collect information while preserving its integrity
- Communicate, coordinate and cooperate with internal and external stakeholders

- Communicate, present and report to relevant stakeholders
- Conduct ethical hacking
- Conduct technical analysis and reporting
- Think creatively and outside the box
- Work ethically and independently; not influenced and biased by internal or external actors
- Work under pressure

Although all represent very reasonable skills to expect from cybersecurity practitioners across a number of roles, they are not the sort of skills from which it is possible to identify KWoPs that would map back to content within the CyBOK Knowledge Areas (on the basis that coverage of soft skills is out-of-scope for CyBOK as a whole).

3.3 Performing the mapping to CyBOK

The mapping process used the full CyBOK Knowledge Base v1.1 (i.e. as included in the file CyBOK_v1.1.0.pdf) as the basis for assessing coverage of the resulting KWoPs. Because it was relevant to consider the *extent* of the content/coverage, it was agreed to adjust the use of the *CyBOK Mapping Framework* (Rashid et al. 2021b) and omit the stages involving the use of the *CyBOK Mapping Reference* (Nautiyal et al. 2021) and *CyBOK Tabular Representation* (CyBOK, 2021) on the basis that neither would provide insight into the *depth* of coverage. Instead, a bottom-up approach was used, directly searching within the Knowledge Base text (i.e. the final stage of the Mapping Framework process), and then cross-referencing matches to the CyBOK Knowledge Trees.

Looking at the process in more detail, the key steps for each KWoP were then as follows:

- Search for the KWoP text, or a characteristic element of it (e.g. for the KWoP "cybersecurity policies" a search would be made for "security polic", in order to also return any hits for 'information security policy', etc).

- Assess how much material is included for each match in the knowledge base and determine if it constitutes a (relevant) *Passing Mention*, *Basic Coverage* or *Detailed Coverage*. Record which KA the matches are found in.

- Having found instances of Basic or Detailed coverage within given Knowledge Areas in the Knowledge Base, consult the related Knowledge Trees to determine if the KWoPS are also matched there. If so, record the level and path within the tree to where the match is found.

For the CyBOK content to be considered useful as a knowledge reference for the ECSF, it was necessary for at least *Basic Coverage* to be offered. Full details of the KWoPs and their mappings to CyBOK Knowledge Base can be found in Appendix B.

In some cases, the words will match but will not be relevant to the context we are interested in (e.g. 'maturity models' and 'audit' match at various points in the Knowledge Base, but were not being covered from the 'organisational level' standpoint that the ECSF role descriptions are intending).

It was also necessary to consider any obvious synonyms that may be getting used for the KWoP (e.g. 'best practices' could be 'good practices'; 'ethical hacking' can be 'penetration testing', etc).

Having performed the mapping of the KWoPs to the CyBOK material, there were various KWoPs for which the actual mappings were the same and so these were further consolidated into a single entry for the purposes of assessing the level of KA usage. A good example here is the following series of KWoPs, which had all been identified distinctly when parsing the ECSF Knowledge, Skills and Tasks:

- awareness, training and education
- cybersecurity awareness, training and education
- cybersecurity education and training
- education, training and awareness-raising
- training
- training and awareness

All of these were found to map to the same KA materials, and so were consolidated to a single KWoP (awareness, training and education) in the final version. It may, of course, be observed that the conceptual similarity between these KWoPs was clear from the outset, which may prompt the question of why they were included distinctly in the first place. The rationale here was that they had been *identified* distinctly from within the ECSF material, and so should be treated independently. As such, it was considered important that these and other such instances were not merged prior to the mapping exercise, as it was necessary to ensure that they did not turn out to map to distinct CyBOK content in practice.

There were some instances in which the process identified what could be regarded as KWoP groups. These were cases in which related KWoPs were found, but would not generally be regarded as synonyms as in the case of the 'awareness' example above. Table 3 illustrates this in relation to a series of KWoPs linked to digital forensics. As can be seen, the high level KWoP is able to be mapped (which is unsurprising given that CyBOK has a Knowledge Area specifically focused upon Forensics), but two of the six more specific KWoPs do not result in a mapping. In this case 'plan' and 'policy' cannot reasonably be considered to be the same as KWoPs that are mapped (e.g. 'procedures' and 'recommendations').

KWoP	Mapped in CyBOK
digital forensics	Yes
digital forensics best practices	Yes
digital forensics investigation	Yes
digital forensics plan	No
digital forensics policy	No
digital forensics procedures	Yes
digital forensics recommendations	Yes

Table 3 : Related KWoPs for Digital Forensics

The other notable KWoP groups were around Audit and Data Protection, which are listed in Table 4 and Table 5 respectively. Here we see fewer KWoPs resulting in a mapping, and this was particularly true for the case of the auditing items, which are all linked to the specific ECSF role of 'Cybersecurity Auditor'. Even where a mapping is made (for 'auditing tools and techniques') it is in relation to some basic coverage found within the AAA Knowledge Area, and this is somewhat tenuous insofar as what is likely to be intended for an auditor role (as it is more referring to system-level auditing, of more interest to a sysadmin than to audit at the business operations level).

KWoP	Mapped in CyBOK
Audit	No
audit plan	No
Auditing	No
auditing frameworks	No
auditing methodologies	No
auditing policy, procedures, standards and guidelines	No
auditing standards	No
auditing tools and techniques	Yes

Table 4 : Related KWoPs for Audit

KWoP	Mapped in CyBOK
data protection	Yes
data protection and privacy	No
data protection policy	No
data protection professional certifications	No
data protection standards, laws and regulations	Yes

data protection strategy	No

Table 5 : Related KWoPs for Data Protection

3.4 Classifying coverage levels

For CyBOK to be *useful* as a knowledge reference for topics raised in the ECSF, then it clearly needs to offer something of substance about the KWoPs concerned. Simply finding a mention of something is not likely to leave a reader more informed about it, whereas a definition, a description or a related discussion (especially if supported by references to the wider body of knowledge) is likely to be helpful. Resources such as the *CyBOK Mapping Reference* and the indexes in the individual Knowledge Areas do not make it clear what level of coverage is being represented. Locating a KWoP in the related Knowledge Trees was more indicative that a qualifying level of coverage would be found, but inspection of the text was still required in order to determine the actual extent. As such, a key part of the assessment involved determining the extent of coverage that CyBOK offered, in order to determine whether it was able to act as a suitable reference point or not. For this purpose, three categorisations were used:

- *Passing mention* (i.e. the words appear but there is little or no content to further explain them)
- *Basic coverage* (e.g. a sentence or two of description or mention in an explanatory context)
- *Detailed coverage* (e.g. reflecting a dedicated paragraph / sub-section, typically supported by references)

While this may sound somewhat subjective, in practice it was typically straightforward to determine the difference and classify the KWoP occurrences accordingly. In the spirit of CyBOK's role as a guide to the Body of Knowledge, the expectation is not that one should expect to find 'chapter and verse' on each topic, but rather that the reader should be able to use CyBOK as a meaningful reference point in order to discover something about the topic or be pointed towards a further source for doing so.

To illustrate the approach in practice, Figure 2 presents a series of CyBOK extracts with varying levels of coverage associated with the KWoP 'Risk Exposure'. In Figure 2a we have just a passing mention from the Cyber Physical Systems KA (actually of *security exposure*), being mentioned in the context of assessing risk (with the references all relating to wider risk management or CPS-related issues). In Figure 2b, taken from the Security Software Lifecycle KA, we have a more specific mention, defining what the concept is and supporting it with a related reference, as such this is deemed to represent 'basic coverage' of the KWoP. In Figure 2c, drawn from the Risk Management & Governance KA, we have a segment of more extensive description (in the KA itself the related text actually goes on for longer). Here it is clear that there is more extensive

description, placing risk exposure in context with other components, and again supported by a reference to further reading.

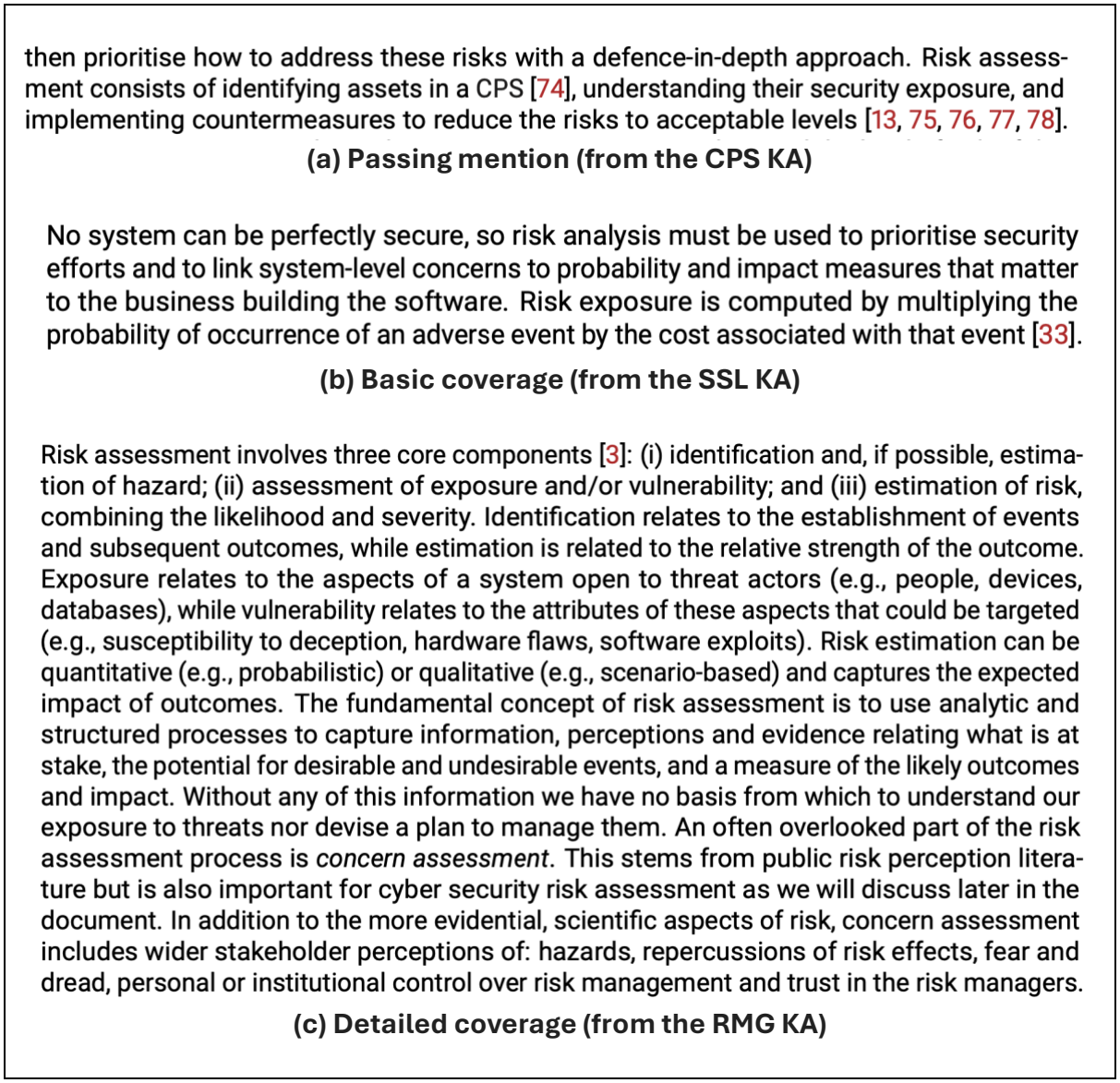


Figure 2 : A series of CyBOK extracts, comparing different levels of coverage for the KWoP 'Risk Exposure': (a) Passing mention, (b) Basic coverage, and (c) Detailed coverage

For example, one of the identified KWoP's (emerging from several descriptor statements) was 'Cybersecurity controls and solutions'. While there are several passing mentions of controls / solutions within the CyBOK material, this is ultimately not a very characteristic KWoP from which to search for content due to its broad coverage. In this sense, it highlights the relatively high-level way in which some of the ECSF knowledge and skills requirements are expressed. For several roles, ECSF indicates that Knowledge is

required in relation to 'Cybersecurity controls and solutions', but it does not more specifically indicate *what* these might entail. As a first-level reference, it is reasonable that professionals across roles such as *Cyber Threat Intelligence Specialist*, *Cybersecurity Architect*, *Cybersecurity Auditor*, *Cybersecurity Educator*, and *Cybersecurity Implementer* should possess a general awareness of commonly used cybersecurity controls and solutions. For example, such as those outlined in frameworks like ISO/IEC 27002 or the CIS Controls. However, the actual knowledge requirements can differ depending on the responsibilities and context of each role. For example, a *Cybersecurity Implementer* would need a deeper understanding of the specific solutions they are tasked with deploying, while an *Educator* may require a more pedagogical perspective. As such, the ECSF statements may benefit from greater specificity to support practical alignment with established knowledge references like CyBOK.

4 Analysis of findings

This section presents the outcomes of this study, beginning at a high-level mapping and then discussing the extent to which ECSF roles may already have a natural 'primary relationship' to a particular CyBOK Knowledge Area. It then proceeds to look at the detailed outcomes from the mapping process.

4.1 High-level mapping

Having looked at the granular approach, it is also apparent that a broad, high-level mapping may be possible for some of the roles. Indeed, regardless of the detailed mapping, there is often one CyBOK KA that would clearly be relevant as the primary reference for a given ECSF role, as illustrated in Table 6.

ECSF role	**Main CyBOK KA**
CISO	Risk Management & Governance
Cyber Incident Responder	Security Operations and Incident Management
Cyber Legal, Policy & Compliance Officer	Law and Regulation
Cyber Threat Intelligence Specialist	Security Operations and Incident Management
Cybersecurity Architect	N/A
Cybersecurity Auditor	-
Cybersecurity Educator	Human Factors
Cybersecurity Implementer	N/A
Cybersecurity Researcher	N/A
Cybersecurity Risk Manager	Risk Management & Governance
Digital Forensics Investigator	Forensics
Penetration Tester	Secure Software Lifecycle

Table 6 : General mapping of ECSF roles to a primary CyBOK Knowledge Area

At the same time, it is also clear from the N/A (i.e. Not Applicable) entries that this approach does not work in all cases. Roles such as *Cybersecurity Architect*, *Cybersecurity Implementer*, *Cybersecurity Researcher* are rather more difficult to associate to a specific CyBOK KA, as the relevant knowledge will clearly depend upon *what* they are architecting, implementing, or researching. Meanwhile, *Cybersecurity Auditor* does not have a strong association to a parent KA. Although there are some links from related tasks, knowledge and skills to KAs such as Law and Regulation, the fact that

CyBOK does not cover key topics relating to auditing means that role holders will not be able to use it as a reference for the core issues.

4.2 Extent of mapping per role

The ability to map each ECSF role to CyBOK was dependent upon the extent to which the descriptor statements could be used for identifying KWoPs, and then the extent to which resulting KWoPs could be mapped to CyBOK content. In practice, this mean that only a subset of the descriptor statements were ultimately usable in the mapping process.

Table 7 reports on the total number of descriptor statements associated with each ECSF role profile, and then the extent to which each of these had key words and phrases that could be mapped to CyBOK Knowledge Areas.

	Chief Information Security Officer (CISO)	Cyber Incident Responder	Cyber Legal, Policy & Compliance Officer	Cyber Threat Intelligence Specialist	Cyber security Architect	Cyber security Auditor
Total statements (Tasks + Knowledge + Skills)	41	30	25	35	37	28
Statements with mappable KWoPs	19	25	19	23	13	6
Statements with unmappable KWoPs	11	1	2	2	6	16
Statements without KWoPs	11	4	4	10	18	6
% statements mapped to Knowledge Area(s)	**46%**	**83%**	**76%**	**66%**	**35%**	**21%**

	Cyber security Educator	Cyber security Imple-menter	Cyber security Researcher	Cybersecurity Risk Manager	Digital Forensics Investigator	Penetration Tester
Total statements (Tasks + Knowledge + Skills)	26	28	24	24	24	31
Statements with mappable KWoPs	14	11	2	15	19	21
Statements with unmappable KWoPs	5	7	4	2	1	1
Statements without KWoPs	7	10	18	7	4	9
% statements mapped to Knowledge Area(s)	54%	39%	8%	63%	79%	68%

Table 7 : Summary of descriptor statements and mappings per role

Figure 3 uses the resulting percentages from the table to visualise the extent to which the total set of descriptor statements per role (i.e. combining the applicable statements from Tasks, Knowledge, and Skills) could be linked to at least Basic Coverage within CyBOK. In terms of the colour coding, green bars indicate those roles where more than two thirds

of the statements associated with the role could be mapped, amber for between a third and two thirds, and red for less than a third.

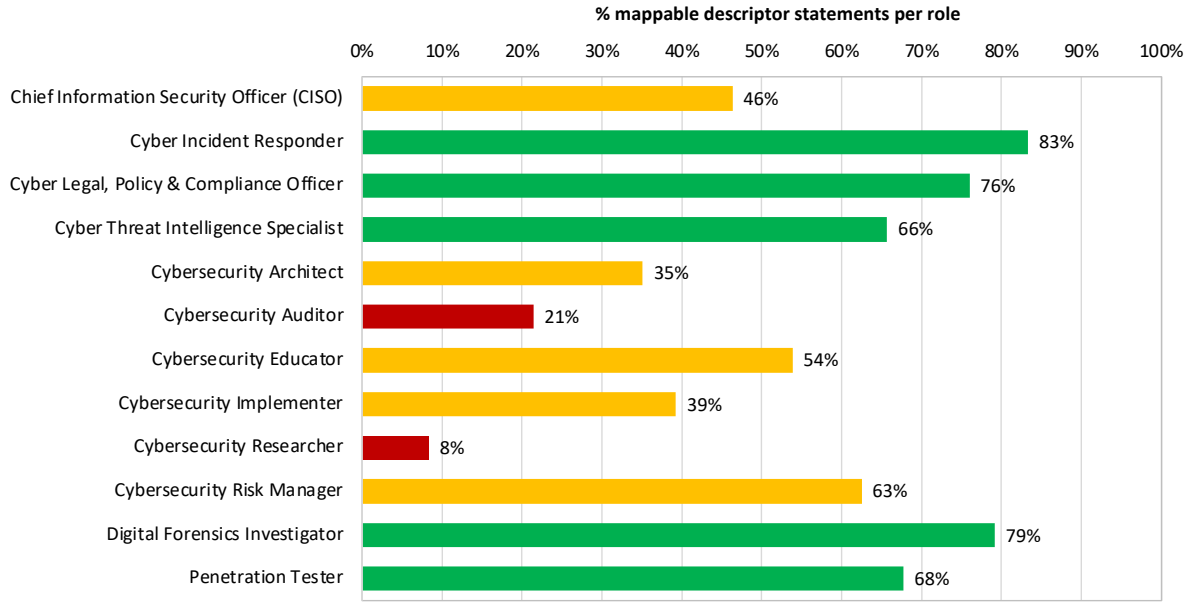


Figure 3 : Extent of KWoP mapping per ECSF role

It can clearly be seen that those roles that are more specific to a given topic area are the ones that map better (note that the exception here is *Cybersecurity Auditor*, where CyBOK lacks coverage of the core topic). The potentially surprising result is the relatively low showing for the *Chief Information Security Officer*. The CISO role had the highest number of related descriptor statements (41 in total, with 14 from Tasks, 11 from Knowledge, and 16 from Skills), but many of these were phrased to generally to extract KWoPs, or the KWoPs extracted were too broad/general or used a different jargon to map to CyBOK content.

4.3 Unmapped Keywords and Phrases

As previously indicated, a third of the KWoPs identified from the ECSF materials could not be mapped to a relevant level of coverage within CyBOK. To examine this further, Table 8 lists the full set of 42 identified KWoPs that remained unmapped at the end of the exercise.

- attacker profiles - audit - audit plan - auditing - auditing frameworks - auditing methodologies - auditing policy, procedures, standards and guidelines - auditing standards - business security requirements analysis - capacity building - cyber range - cyber threat information - cyber threat intelligence strategy - cybersecurity best practices - cybersecurity controls / Cybersecurity controls and solutions / security controls - cybersecurity events - Cybersecurity maturity models / maturity models - cybersecurity plan - cybersecurity procedures	- cybersecurity recommendations - cybersecurity solutions - cybersecurity strategy - data protection and privacy - data protection policy - data protection professional certifications - data protection strategy - digital forensics plan - digital forensics policy - information security strategy - mentoring - privacy by default - privacy compliance - Responsible information disclosure - risk remediation - security architecture design - security by default - security responsibilities - security reviews - SLAs - threat hunting - threat landscape - threat mitigation

Table 8 : Unmapped ECSF KWoPs

While this may seem like a considerable list, it should be noted that the items fall into several categories to explain the lack of mapping:

- KWoPs that are arguably too general / broad to expect that there would be a useful mapping (e.g. capacity building, cybersecurity procedures, cybersecurity recommendations risk remediation).
- KWoPs do not reflect terms that are in common use (e.g. cyber threat information, privacy by default', where the more expected terms would typically be 'cyber threat intelligence' and 'privacy by design' respectively, both of which were also identified as KWoPs and *were* able to be mapped).
- KWoPs relating to topics for which CyBOK does not have a related Knowledge Area (e.g. those relating to auditing).

Equally, there remain *some* instances in which it was surprising to find that CyBOK did not have some related coverage to offer (e.g. cyber range, maturity models, threat landscape). However, these ultimately represent a minority of cases, and so overall it

would be reasonable to conclude that the mapping process was successful in most instances where it would have been expected to be.

4.4 KWoP mapping results

From 118 distinct KWoPs remaining in the consolidated set, 62 of them (53%) resulted in mappings to detailed coverage within CyBOK. Expanding this to also include further KWoPs for which some basic coverage was found yields an additional 14, bringing the total of mapped KWoPs to 64%.

Where KWoPs were mapped, there was a noticeable difference in the extent to which different CyBOK Knowledge Areas became involved in the process. This is illustrated in Figure 4, which shows the raw number of instances in which each KA occurs as a match to either basic or detailed coverage[1]. While the overall spread of mappings is clearly involving the majority of CyBOK KAs, there is a noticeable skew towards a particular subset of them. Indeed, the mappings to RMG account for a quarter of the mappings made. Meanwhile, extending the consideration to the four most prominent KAs (RMG, LR, SSL and SOIM), it is found that they collectively account for 57% of the total mappings. With the remaining 43% of mappings spread across 12 KAs, it is clear that several Knowledge Areas – although utilised – are not featuring significantly.

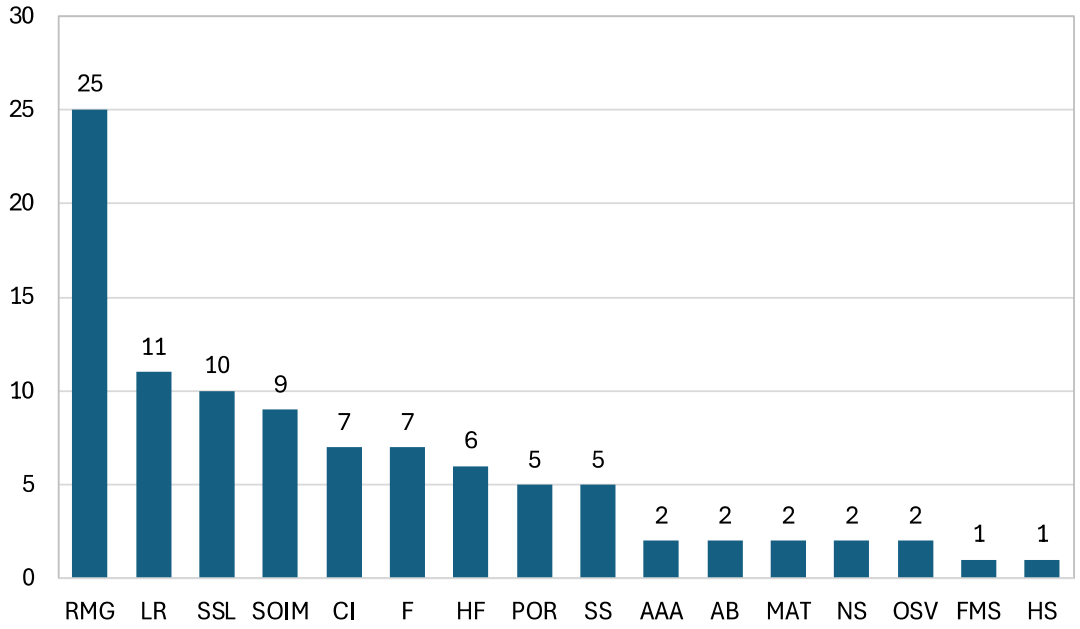


Figure 4 : Varying CyBOK KA representation in KwoP mappings

[1] It should be noted that some KWoPs map to multiple KAs, and so the total number of mappings (97) is greater than the total number of mappable KWoPs (75).

As readers may be aware, CyBOK grouped its 21 Knowledge Areas within five higher level categories:

- Attacks & Defences
- Human, Organisational & Regulatory Aspects
- Infrastructure Security
- Software & Platform Security
- Systems Security

It is notable that almost half (48%) of the KwoP matches fall within the *Human, Organisational & Regulatory Aspects* category.

The notable skew towards the RMG KA is ultimately somewhat reflective of the way in which the tasks knowledge and skills statements within the ECSF are ultimately presented. Many of them are framed at a relatively high level following ECSF's design principles.

What is also significant is the number and nature of the CyBOK Knowledge Areas that did not feature in *any* of the ECSF mappings.

- Applied Cryptography
- Cryptography
- Distributed Systems Security
- Cyber Physical Systems Security
- Physical Layer and Telecommunication Security
- Web and Mobile Security

Moreover, although they are included in mappings, the Formal Methods for Security and Hardware Security KAs are not represented in a significant way. Both are involved because of a single descriptor statement in the ECSF Skills list that refers to: "*Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls*". This skill then turns out to apply to only a single ECSF role (Cybersecurity Auditor), and so a resulting KwoP of 'Hardware security' then ends up broadly mapping to the Hardware Security KA and part of the Formal Methods for Security KA to this role. In reality, the Auditor role is unlikely to need much of what the Hardware Security KA involves, but the skill of 'reviewing hardware security' does not enable things to be narrowed down further.

Returning to the cases where mapping was achieved, it is then possible to look at how this was reflected in the different ECSF role profiles. To this end, Figure 5 shows the *overall* distribution of KA usage across the full set of 12 ECSF roles.

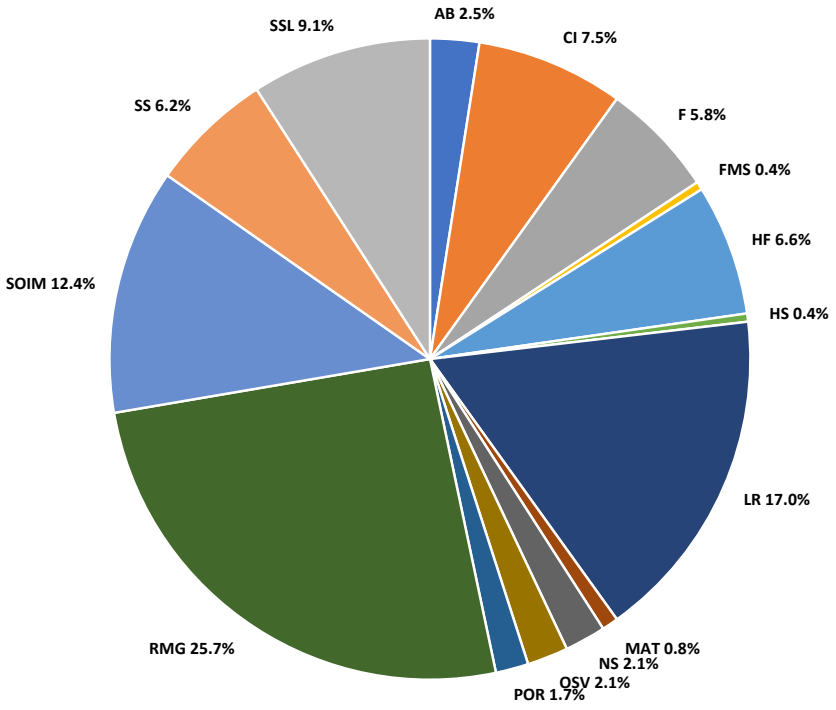


Figure 5 : Overall usage of CyBOK KAs across all ECSF roles

The most commonly used KAs are RMG, LR and SOIM, which collectively account for more than half of the overall KA usage[2]. Amongst the remaining KAs listed, some are clearly making a relatively incidental contribution and therefore being called upon to a much lesser degree across the ECSF as a whole.

A point worth noting is that some of the ECSF roles themselves are framed fairly specifically, whereas others are far more general – and this clearly emerges in the extent to which they can be mapped to Knowledge Area coverage (as can be seen by referring back to Figure 3). This approach is based on the principles that informed ECSF design to make it suitable and easily understandable and applied by a wider audience. At the same time, this provided a challenge to map to relevant Knowledge Areas.

It is also worth reflecting again on the CyBOK Knowledge Areas that are not included in the chart, and are therefore not reflected within any of the roles. In practice, it is hard to imagine that certain roles (e.g. *Cybersecurity Architect* and *Cybersecurity Implementer*) would *not* find reasons to draw upon Knowledge Areas such as *Applied Cryptography*,

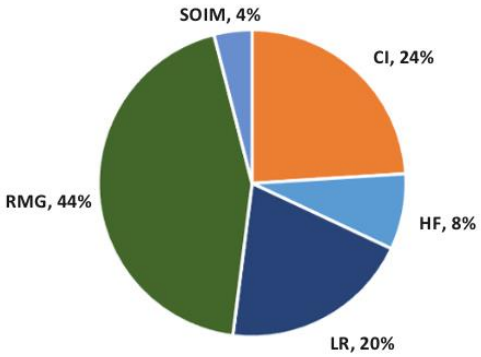
[2] As an aside, to explain the variation between KA ranking in this case compared to Figure 4, the former was showing which KAs the identified KWoPs were mapping against, whereas the current Figure is showing how the KAs are drawn upon by the roles. So, for instance, while more of the identified KWoPs map to the SSL KA, a lesser proportion of the roles are using actually them.

Distributed Systems Security, and *Web and Mobile Security*. The fact that such relationships do not emerge from the mappings raises some questions about the extent to which the Knowledge, Skills and Tasks requirements for such roles have been sufficiently captured. Concentration to specific KAs may reflect the current emphasis within the ECSF role descriptions. At the same time, it also suggests an opportunity for future investigations to explore whether underrepresented KAs correspond to emerging or overlooked areas of practice. Extending the ECSF to more explicitly incorporate these areas could help ensure broader coverage of the cybersecurity knowledge landscape and better alignment with evolving role demands.

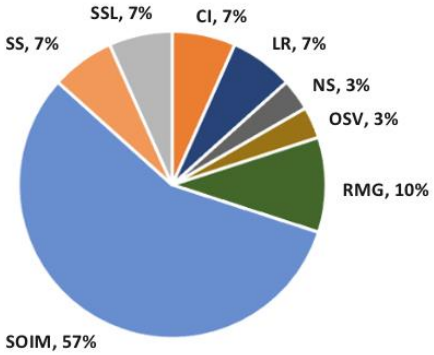
4.5 Role-specific Knowledge Area usage

It is also relevant to look at the CyBOK relationships for each of the ECSF roles individually. To this end, Figure 6 illustrates the more specific breakdown of usage of the Knowledge Areas on a per role basis. However, when interpreting these charts, it is important to remember that they are only reflecting the cases where KWoPs could be extracted from the role descriptor statements, and where those KWoPs could be mapped to CyBOK. So, referring back to Figure 3, this means that the chart for *Cyber Incident Responder* is based upon mapping 83% of the related statements to CyBOK, whereas for *Cyber Security Auditor* the KA usage is only related to the 21% of statements that were mappable.

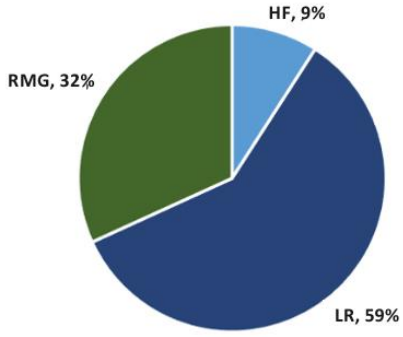
Chief Information Security Officer



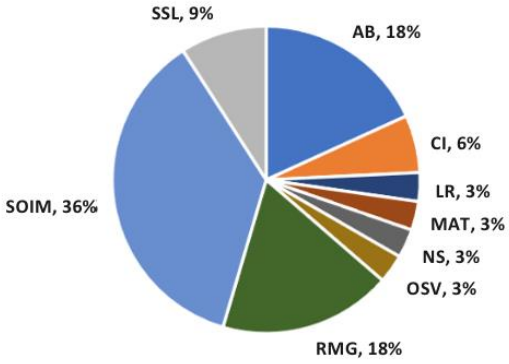
Cyber Incident Responder



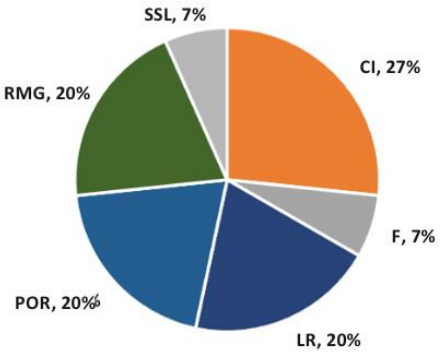
Cyber Legal, Policy and Compliance Officer



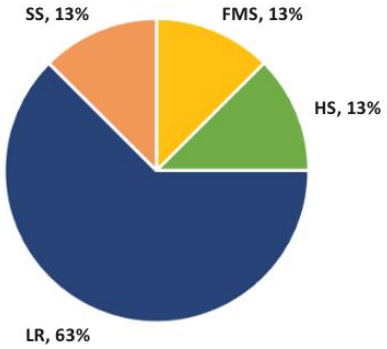
Cyber Threat Intelligence Specialist



Cybersecurity Architect



Cybersecurity Auditor



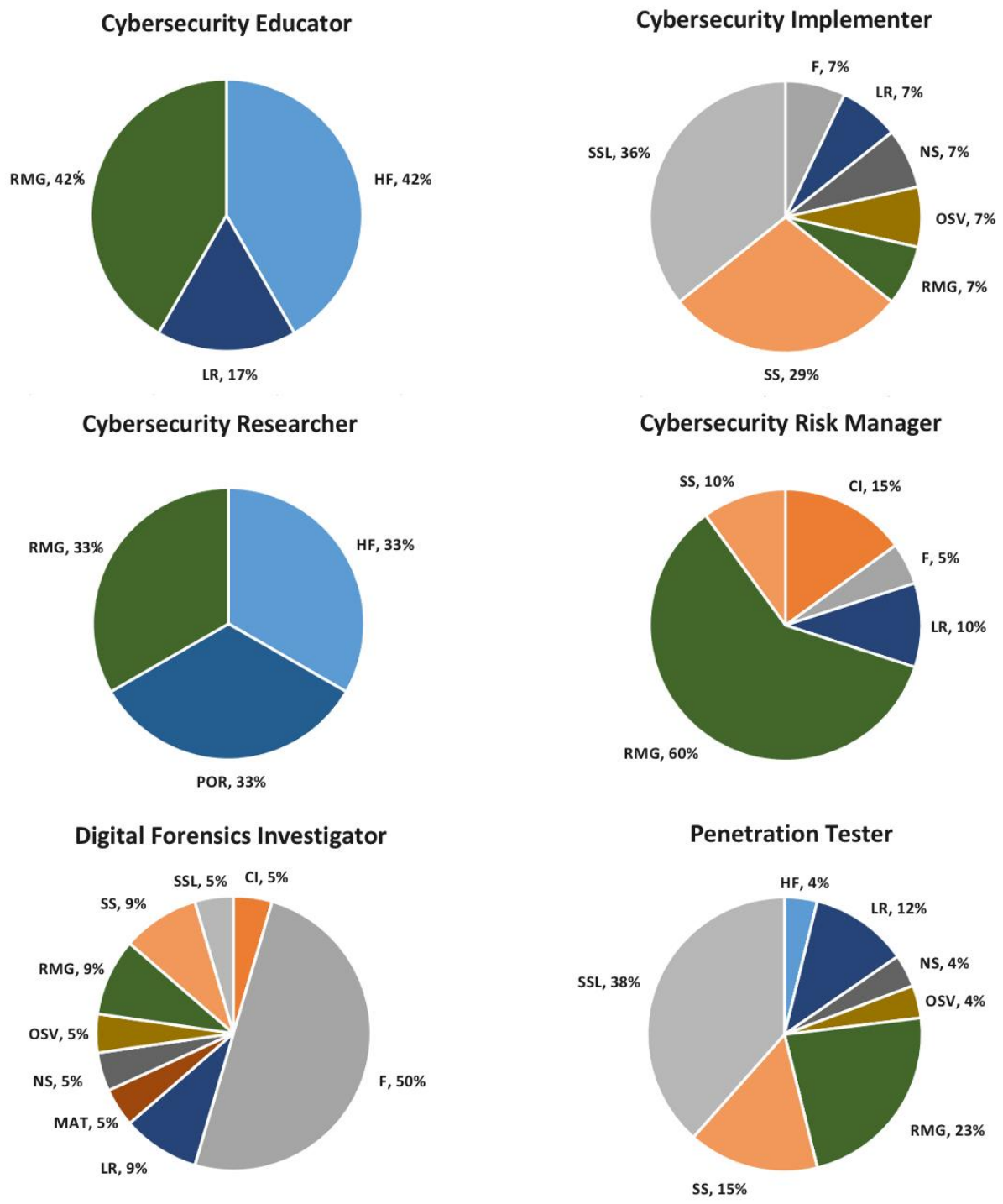


Figure 6 : CyBOK Knowledge Area usage per ECSF role

5 Conclusions

This study set out to evaluate the extent to which CyBOK can serve as a relevant knowledge reference for ECSF. Through a structured mapping process of ECSF profiles to CyBOK KAs, the investigation has provided valuable insight into areas of alignment, divergence, and opportunity.

Overall, the findings demonstrate that CyBOK has clear potential to act as a credible and valuable reference source for ECSF role profiles, particularly for roles that are conceptually well-aligned with established knowledge areas. However, it is equally evident that CyBOK alone would not be sufficient as the sole reference point for ECSF users. Its utility varies across roles. For example, it offers strong support for some roles such as the Cyber Incident Responder, the Risk Manager, and the Digital Forensics Investigator, while being less applicable to others such as the Cybersecurity Auditor or Cybersecurity Researcher.

The mapping revealed that certain CyBOK KAs (particularly RMG, LR, SOIM, SSL, and HF) are much more prominently connected to ECSF profiles than others, collectively accounting for the majority of the identified relationships. This emphasis suggests a governance- and operations-centric orientation in how the ECSF roles are currently articulated.

At the same time, several CyBOK KAs were not referenced in *any* ECSF mappings, notably including *Cryptography*, *Web and Mobile Security*, and *Distributed Systems Security*. Given the focus of these domains in contemporary cybersecurity practice, they were expected to be mapped to roles such as *Cybersecurity Implementer* and *Penetration Tester*. The omission of certain areas of technical knowledge is justified from the high-level design approach applied for the specification of ECSF profiles, so they could serve various use cases and stakeholders. Meanwhile, the non-use of more niche areas, such as *Cyber-Physical Systems Security* and *Physical Layer and Telecommunications Security*, may be more justifiably attributed to their specialized nature.

The analysis also identified gaps in CyBOK coverage, most notably in relation to auditing, which is central to the *Cybersecurity Auditor* role but is not addressed in the current CyBOK Knowledge Base. Similarly, CyBOK offers limited treatment of soft skills, which are frequently cited in ECSF profiles. In this particular case, the absence of coverage is directly linked to the intended scope of CyBOK. While soft skills are *complementary* to many cyber roles, they are not part of the body of knowledge for cyber security itself.

Nonetheless, given the importance of soft skills in operationalising some areas of cybersecurity that are covered, there may be ways in which CyBOK could acknowledge their role more prominently. This could include further highlighting or cross-referencing of them within the *Human Factors* KA, or explicitly mentioning them in other KAs where

certain soft skills are more prominent. Alternatively, there may be opportunities to develop supplementary materials (outside of CyBOK) that map KAs to roles and to skills.

From the ECSF perspective, an area for enhancement involves the specificity of role descriptions, particularly for generalist or broadly defined roles such as Cybersecurity Researcher and Cybersecurity Implementer. These roles included broad statements, e.g. cybersecurity controls and solutions, which made it difficult to match them to CyBOK KAs as it would depend on the case that they are applied. For example, what the cybersecurity implementer is actually implementing. These profiles could be expanded to represent different situations and to benefit from more technically grounded knowledge requirements, potentially guided by CyBOK KAs to ensure appropriate depth. This will also be an opportunity to reference the CyBOK KAs that were not currently mapped to any ECSF profile, or they were underrepresented.

The findings suggest actionable recommendations for both resources. Maintaining a dialogue between ECSF and CyBOK will be essential to inform cybersecurity initiatives and support the growth of a well-informed, adaptable, and competent cybersecurity workforce.

6 References

CIISec. 2024. *Skills Framework*. The Chartered Institute for Information Security, September 2024. https://www.ciisec.org/frameworks/skills-framework (accessed 1 July 2025).

CyBOK. 2021. *The Cyber Security Body of Knowledge - Tabular representation of CyBOK Broad Categories, Knowledge Areas and their descriptions*. July 2021. https://www.cybok.org/media/downloads/CyBOK_Tabular_Representation_1_1_July_2021.pdf (accessed 1 July 2025).

ENISA. 2022. *User Manual - European Cybersecurity Skills Framework (ECSF)*. European Union Agency for Cybersecurity. September 2022. https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf (accessed 1 July 2025).

ENISA. 2025. *European Cybersecurity Skills Framework (ECSF)*. European Union Agency for Cybersecurity. 10 April 2025. https://www.enisa.europa.eu/press-office/press-and-media/european-cybersecurity-skills-framework-ecsf (accessed 1 July 2025).

Nautiyal, L., Hallett, J., Clements, J., Shreeve, B. and Rashid, A. 2021. *CyBOK Mapping Reference - Issue 1.3.0*. July 2021. https://www.cybok.org/media/downloads/CyBOK_Mapping_Reference_v1.3.0.pdf (accessed 1 July 2025).

Rashid, A., Chivers, H., Lupu, E., Martin, A. and Schneider, B. 2021a. *CyBOK - The Cyber Security Body of Knowledge*, Version 1.1.0, 31 July 2021. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf (accessed 1 July 2025).

Rashid, A., Nautiyal, L., Hallett, J. and Shreeve, B. 2021b. *CyBOK Mapping Framework - How to map concepts in academic and professional programmes to the Cyber Security Body of Knowledge*. Version 1.0. 22 February 2021. https://www.cybok.org/media/downloads/CyBOK_Mapping_Framework_academic_professional_progs_Feb21.pdf (accessed 1 July 2025).

UKCSC. 2025. *Cyber Career Framework*. UK Cyber Security Council https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/ (accessed 1 July 2025).

A Appendix A – Keywords and Phrases

The following pages present alphabetical lists of the Keywords and Phrases (KWoPs) identified from across the set of ECSF role profiles, looking at the tasks, knowledge and skills components used within the profiles.

Note that several of the KWoPs recurred multiple times *within* each category, but the frequency was not relevant to capture as *any* occurrence meant that it would be relevant to then determine if an associated knowledge reference could be found within CyBOK.

KWoPs also recurred across the categories, and hence an overall consolidated set is presented in the final list, which was then used as the basis for the CyBOK mapping exercise.

A.1 KWoPs from ECSF Task statements

attacker profiles
audit
audit plan
auditing
auditing policy, procedures, standards and guidelines
awareness
Awareness training
capacity building
certification
compliance
Computer Security Incident Response Teams (CSIRTs)
cyber incidents
cyber threat actors
cyber threat intelligence strategy
cybersecurity certification
cybersecurity controls
cybersecurity incidents
cybersecurity policy
cybersecurity procedures
cybersecurity risks
cybersecurity solutions
cybersecurity strategy
data privacy
data protection
data protection standards, laws and regulations
digital evidence

digital forensic analysis
digital forensics investigation
digital forensics plan
digital forensics policy
digital forensics procedures
education, training and awareness-raising
incident handling
incident handling reporting
Incident Response Plan
incidents detection and response
Information Security Management System (ISMS)
laws
mentoring
penetration testing
privacy compliance
privacy impact assessments
privacy requirements
regulations
risk exposure
risk management
risk mitigation
risk remediation
Risk treatment
Secure Operation Centres (SOCs)
security architecture design
security controls
security responsibilities
security reviews
Tactics, Techniques and Procedures (TTPs)
technical vulnerabilities
third-party relations
threat hunting
threat landscape
threat mitigation
threat modelling
threats
threats and vulnerabilities
training
training and awareness
vulnerabilities

(Total 66 Tasks KWoPs)

A.2 KWoPs from ECSF Knowledge statements

Advanced and persistent cyber threats (APT)
Auditing
certification
Computer Security Incident Response Teams (CSIRTs)
Cyber Threat Intelligence (CTI)
Cybersecurity awareness, education and training programme development
Cybersecurity controls and solutions
Cybersecurity education and training
Cybersecurity maturity models
Cybersecurity policies
Cybersecurity recommendations -- best practices
Cybersecurity risks
Digital forensics
Digital forensics recommendations and best practices
Ethical cybersecurity
Incident handling
Incident handling
Incident handling recommendations and best practices
laws, regulations and legislations
Malware analysis
networks security
Offensive and defensive security practices
Operating systems security
operational technology (OT)
Penetration testing
Privacy impact assessment
Privacy-by-design
Privacy-Enhancing Technologies (PET)
Responsible information disclosure
Risk management recommendations and best practices
Risk management standards, methodologies and frameworks
Risk management tools
Secure coding
Secure development lifecycle
Secure Operation Centres (SOCs)
Security architecture
Testing
threat actors
Tactics, Techniques and Procedures (TTPs)
threats
vulnerabilities

(Total 41 Knowledge KWoPs)

A.3 KWoPs from ECSF Skills statements

auditing
auditing frameworks
auditing methodologies
auditing standards
auditing tools and techniques
awareness, training and education
business security requirements analysis
certification
CTI
cyber range
cyber threat information
cybersecurity and privacy policies
cybersecurity awareness, training and education
cybersecurity best practices
cybersecurity culture
cybersecurity events
cybersecurity management
cybersecurity plan
cybersecurity policies
cybersecurity policy
cybersecurity posture
cybersecurity recommendations
cybersecurity strategy
cybersecurity strategy
data protection and privacy
data protection policy
data protection professional certifications
data protection strategy
digital evidence
ethical hacking
exploit vulnerabilities
hardware security
incident handling and response
Information Security Management System (ISMS)
information security strategy
laws, regulations and legislations
log files
manage and mitigate risks
maturity models

Model threats, actors and TTPs
penetration testing
privacy by default
privacy by design
regulations and standards
risk management frameworks
risk management guidelines
risk management methodologies
risk management practices
security by default
security by design
security objectives
security policy
SLAs
social engineering
software security
threat actors
threat intelligence
threats
TTPs

(Total 59 Skills KWoPs)

A.4 Consolidated list KWoPs from ECSF Task, Knowledge and Skills

Advanced and persistent cyber threats (APT)
attacker profiles
Audit
audit plan
auditing
auditing frameworks
auditing methodologies
auditing policy, procedures, standards and guidelines
auditing standards
auditing tools and techniques
awareness
Awareness training
awareness, training and education
business security requirements analysis
capacity building
certification
compliance
Computer Security Incident Response Teams (CSIRTs)

CTI
cyber threat information
Cyber Threat Intelligence (CTI)
cyber threat intelligence strategy
cyber incidents
cyber range
cyber threat actors
cybersecurity and privacy policies
Cybersecurity awareness, education and training programme development
cybersecurity awareness, training and education
cybersecurity best practices
cybersecurity certification
cybersecurity controls
Cybersecurity controls and solutions
cybersecurity culture
Cybersecurity education and training
cybersecurity events
cybersecurity incidents
cybersecurity management
Cybersecurity maturity models
cybersecurity plan
cybersecurity policies
cybersecurity policy
cybersecurity posture
cybersecurity procedures
cybersecurity recommendations
cybersecurity risks
cybersecurity solutions
cybersecurity strategy
data privacy
data protection
data protection and privacy
data protection policy
data protection professional certifications
data protection standards, laws and regulations
data protection strategy
digital evidence
digital forensic analysis
digital forensics
digital forensics best practices
digital forensics investigation
digital forensics plan
digital forensics policy
digital forensics recommendations

digital forensics procedures
education, training and awareness-raising
Ethical cybersecurity
ethical hacking
exploit vulnerabilities
hardware security
incident handling
incident handling and response
Incident handling recommendations and best practices
incident handling reporting
Incident Response Plan
incidents detection and response
Information Security Management System (ISMS)
information security strategy
laws
laws, regulations and legislations
log files
Malware analysis
manage and mitigate risks
maturity models
mentoring
Model threats, actors and TTPs
networks security
Offensive and defensive security practices
Operating systems security
operational technology (OT)
penetration testing
privacy by default
privacy by design
privacy compliance
privacy impact assessments
privacy requirements
Privacy-by-design
Privacy-Enhancing Technologies (PET)
regulations
regulations and standards
Responsible information disclosure
risk exposure
risk management
risk management frameworks
risk management guidelines
risk management methodologies
risk management practices
Risk management recommendations and best practices
Risk management standards, methodologies and frameworks

Risk management tools
risk mitigation
risk remediation
Risk treatment
Secure coding
Secure development lifecycle
Secure Operation Centres (SOCs)
Security architecture
security architecture design
security by default
security by design
security controls
security objectives
security policy
security responsibilities
security reviews
SLAs
social engineering
software security
Tactics, Techniques and Procedures (TTPs)
technical vulnerabilities
Testing
third-party relations
threat actors
threat hunting
threat intelligence
threat landscape
threat mitigation
threat modelling
threats
threats and vulnerabilities
training
training and awareness
TTPs
Vulnerabilities

(Total 142 overall KWoPs)

B Appendix B – ECSF to CyBOK mapping

The pages that follow presents the full list of Key Words and Phrases (KWoPs) identified from the ECSF descriptor statements. All KWoPs are listed alphabetically, and if a CyBOK match was found then the related Knowledge Area(s) are named, indicating whether they contained basic or detailed coverage. In addition, where a KWoPs could be found or related to the content of Knowledge Trees, the table lists the related path. It should be noted that in a small number of cases Knowledge Areas were considered to offer coverage even though the KWoPs did not appear in the related Knowledge Tree. It should also be noted that some of the Knowledge Tree mappings are a 'best fit' rather than an exact match to the KWoP name.

Key Words and Phrases (KWoPs)	KA Coverage		Knowledge Tree	
	Basic	Detailed	Tree and level	Path
Advanced and persistent cyber threats (APT)	MAT		MAT.3	MAT/malware taxonomy/kinds/advanced persistent threats
attacker profiles				
Audit				
audit plan				
auditing				
auditing frameworks				
auditing methodologies				
auditing policy, procedures, standards and guidelines				
auditing standards				
auditing tools and techniques	AAA			
awareness	AAA	RMG, HF	HF.3 RMG.3	HF/awareness and education/terms/awareness RMG/risk governance/security culture/awareness
Awareness training	RMG		HF.3	HF/awareness and education/terms/training

Key Words and Phrases (KWoPs)	KA Coverage		Knowledge Tree	
	Basic	Detailed	Tree and level	Path
awareness, training and education / cybersecurity awareness, training and education / training / training and awareness / education, training and awareness-raising / Cybersecurity education and training		RMG, HF	HF.3 RMG.3	HF/awareness and education/terms/awareness HF/awareness and education/terms/education HF/awareness and education/terms/training RMG/risk governance/security culture/awareness
business security requirements analysis				
capacity building				
certification / cybersecurity certification	LR			
compliance	LR	RMG	RMG.3	RMG/risk assessment and management principles/security metrics/regulatory compliance
Computer Security Incident Response Teams (CSIRTs)	SOIM		SOIM.3	SOIM/ human factors: incident management/ prepare: incident management planning/TF-CSIRT
CTI / Cyber Threat Intelligence (CTI) / threat intelligence		SOIM	SOIM.3	SOIM/ fundamental concepts/ architectural principles/ cyber-threat intelligence (CTI)
cyber threat information				
cyber threat intelligence strategy				
cyber incidents	RMG	SOIM	SOIM.1 SOIM.3	SOIM/ human factors: incident management SOIM/ plan: security information and event management/ alert correlation/ incident and information exchange
cyber range				
cyber threat actors / threat actors		AB	AB.1	AB/ Characterisation of Adversaries
cybersecurity and privacy policies		RMG, POR	POR.2, RMG.2	POR/ control/ privacy policy negotiation RMG/ risk governance/enacting security policy
Cybersecurity awareness, education and training programme development	HF			
cybersecurity best practices				

Key Words and Phrases (KWoPs)	KA Coverage		Knowledge Tree	
	Basic	Detailed	Tree and level	Path
cybersecurity controls / Cybersecurity controls and solutions / security controls				
cybersecurity culture		HF, RMG	RMG.2	RMG/ risk governance/security culture
cybersecurity events				
cybersecurity incidents	HF	CI	CI.2	CI/ Foundational Concepts/Failures and Incidents
cybersecurity management		CI		
Cybersecurity maturity models / maturity models				
cybersecurity plan				
cybersecurity policy / security policy / cybersecurity policies		RMG	RMG.2	RMG/ risk governance/enacting security policy
cybersecurity posture	RMG			
cybersecurity procedures				
cybersecurity recommendations				
cybersecurity risks		RMG	RMG.1	RMG/ risk definition
cybersecurity solutions				
cybersecurity strategy				
data privacy		POR	POR.2	POR/confidentiality/ data confidentiality
data protection		LR	LR.1	LR/ data protection
data protection and privacy				
data protection policy				
data protection professional certifications				
data protection standards, laws and regulations		LR	LR.2	LR/ data protection/core regulatory principles
data protection strategy				

Key Words and Phrases (KWoPs)	KA Coverage		Knowledge Tree	
	Basic	Detailed	Tree and level	Path
digital evidence		F	F.3	F/ definitions and conceptual models/legal concerns and the Daubert Standard/ ACPO good practice guide for digital evidence
digital forensic analysis		F	F.2	F/ operating system analysis F/ main memory forensics F/application forensics F/cloud forensics F/artifact analysis
digital forensics		F	F.3	F/ definitions and conceptual models/definitions/digital forensics
digital forensics best practices		F	F.3	F/ definitions and conceptual models/legal concerns and the Daubert Standard/ ACPO good practice guide for digital evidence
digital forensics investigation		F		
digital forensics plan				
digital forensics policy				
digital forensics recommendations		F	F.3	F/ definitions and conceptual models/legal concerns and the Daubert Standard/ ACPO good practice guide for digital evidence
digital forensics procedures		F		
Ethical cybersecurity		LR	LR.1	LR/ethics
ethical hacking		SSL	SSL.3	SSL/ prescriptive processes/Touchpoints/penetration testing
exploit vulnerabilities	AB		AB.3 SSL.2	AB/ Models/ Kill chains/Exploitation SSL/ motivations for secure software lifecycle/vulnerabilities can be exploited without being noticed
hardware security		FMS, HS	FMS.1 HS	FMS/ Hardware HS
incident handling / Incident handling recommendations and best practices / incident handling reporting		SOIM	SOIM.2	SOIM/ human factors: incident management/ handle: actual incident response
incident handling and response		RMG, SOIM, SSL	RMG.1, SOIM.2, SSL.3	RMG/ business continuity: incident response and recovery planning SOIM/ human factors: incident management/ handle: actual incident response SSL/ prescriptive processes/ Microsoft SDL/ establish a standard incident response process
Incident Response Plan		RMG, SOIM, SSL	RMG.1, SOIM.2	RMG/ business continuity: incident response and recovery planning SOIM/ human factors: incident management/ prepare: incident management planning

Key Words and Phrases (KWoPs)	KA Coverage		Knowledge Tree	
	Basic	Detailed	Tree and level	Path
incidents detection and response		NS, SOIM	NS.2, SOIM.3	NS/ Network Security Tools/ Intrusion Detection and Prevention Systems SOIM/ fundamental concepts/ workflows and vocabulary/ intrusion detection
Information Security Management System (ISMS)	CI			
information security strategy				
laws / laws, regulations and legislations		LR	LR	LR
log files	F	SOIM, SSL	SOIM.2	SOIM/ monitor: data sources/ application logs: web server logs and files SOIM/ monitor: data sources/ system and kernel logs
Malware analysis		MAT	MAT.1	MAT/malware analysis
manage and mitigate risks		RMG	RMG.1	RMG/ risk assessment and management principles
mentoring				
Model threats, actors and TTPs		RMG, SSL	RMG.3, SSL.3	RMG/risk assessment and management principles/risk assessment and management methods/attack trees SSL/ adaptations of secure software lifecycle/ agile and DevOps/perform threat modelling
networks security		NS	NS	NS
Offensive and defensive security practices	LR			
Operating systems security		OSV	OSV.1	OSV/ OS security principles
operational technology (OT)		RMG	RMG.3	RMG/risk assessment and management principles/risk assessment and management in cyber-physical systems/OT
penetration testing		SSL	SSL.3	SSL/ prescriptive processes/Touchpoints/penetration testing
privacy by default				
privacy by design / Privacy-by-design		POR	AAA.3	AAA/ authentication/ identity management/privacy by design
privacy compliance				
privacy impact assessments	LR			
privacy requirements		POR	POR.1	POR/confidentiality POR/control POR/transparency
Privacy-Enhancing Technologies (PET)		POR	POR.1	POR/ privacy technologies and democratic values

Key Words and Phrases (KWoPs)	KA Coverage		Knowledge Tree	
	Basic	Detailed	Tree and level	Path
regulations		LR	LR	LR
regulations and standards		LR, RMG	LR, RMG.3	LR RMG/ risk assessment and management principles/ risk assessment and management methods/ NIST guidelines RMG/ risk assessment and management principles/ risk assessment and management methods/ ISO/IEC 27005 RMG/ risk assessment and management principles/ risk assessment and management methods/TOGAF
Responsible information disclosure				
risk exposure	SSL	RMG	RMG.1	RMG/ risk definition
risk management		RMG	RMG.1	RMG/ risk assessment and management principles
risk management frameworks/ guidelines/ methodologies/ practices/ recommendations and best practices/ standards, methodologies and frameworks/ tools		RMG	RMG.2	RMG/ risk assessment and management principles/ risk assessment and management methods/
risk mitigation		RMG		
risk remediation				
Risk treatment	RMG			
Secure coding	SSL	SS	SS.2 SSL.4	SS/ prevention of vulnerabilities/ coding practices SSL/ prescriptive processes/ SAFECode/ application security control definition/ secure coding practices
Secure development lifecycle		SSL	SSL.1	SSL/ motivations for secure software lifecycle
Secure Operation Centres (SOCs)		SOIM	SOIM.2	SOIM/ plan: security information and event management/ security operations and benchmarking
Security architecture		CI	CI.2	CI/ Crosscutting Themes/ Security Architecture and Lifecycle
security architecture design				
security by default				
security by design	OSV			
security objectives		CI	CI.2	CI/ Foundational Concepts/ Objectives of Cyber Security

Key Words and Phrases (KWoPs)	KA Coverage		Knowledge Tree	
	Basic	Detailed	Tree and level	Path
security responsibilities				
security reviews				
SLAs				
social engineering	HF			
software security		SS	SS	SS
Tactics, Techniques and Procedures (TTPs) / TTPs		SOIM	SOIM.1	SOIM/knowledge: intelligence and analytics
technical vulnerabilities		SS	SS.1	SS/categories of vulnerabilities
Testing		SS, SSL	SS.1 SSL.3	SS/detection of vulnerabilities SSL/prescriptive processes/[SAFECode or Microsoft SDL]/perform static analysis security testing SSL/prescriptive processes/[SAFECode or Microsoft SDL]/perform dynamic analysis security testing
third-party relations		LR	LR.1	LR/contract
threat hunting				
threat landscape				
threat mitigation			SOIM.3	SOIM/human factors: incident management/handle: actual incident response/mitigation
threat modelling		RMG, SSL	RMG.3 SSL.3	RMG/risk assessment and management principles/risk assessment and management methods/attack trees SSL/ adaptations of secure software lifecycle/ agile and DevOps/perform threat modelling
threats		CI, RMG	CI.3 RMG.3	CI/ Foundational Concepts/ Risk Management/ Nature of Threat RMG/ risk assessment and management principles/ elements of risk/threat
threats and vulnerabilities		CI, RMG	CI.3 RMG.2	CI/ Foundational Concepts/ Risk Management/ Nature of Threat CI/ Foundational Concepts/ Risk Management/The Presence of Vulnerabilities RMG/ risk assessment and management principles/ elements of risk
vulnerabilities		RMG, SS	RMG.3 SS.1	RMG/ risk assessment and management principles/ elements of risk/vulnerability SS/categories of vulnerabilities