Array 30 (2026) 100728

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/locate/array

Towards a unified European Cybersecurity Skills Framework: Structural insights from expert elicitation and international standards

Gaetano Perrone [a,*], Nicola d'Ambrosio [b], Roberto D'Isanto [b], Massimiliano Rak [b], Lavinia Russo [b], Simon Pietro Romano [b], Mario Varlese [b]

[a] Department of Electrical Engineering and Information Technology, University of Naples Federico II, Italy
[b] University of Naples Federico II, Italy

ARTICLE INFO

Dataset link: https://zenodo.org/records/18312770, 10.5281/zenodo.18312770

Keywords:
Cybersecurity skills
Workforce development
Cybersecurity education
Skills gap analysis

ABSTRACT

The increasing complexity of cyber threats and the widening skills gap in Europe underscore the urgent need for coherent, interoperable strategies to build the cybersecurity workforce. Although several cybersecurity initiatives and frameworks have been proposed, their heterogeneous structures and modelling choices hinder harmonisation across education, training, and labour-market ecosystems. The European Cybersecurity Skills Framework (ECSF) represents a major step toward a common European reference model. However, its adoption raises several challenges related to its internal structure and interoperability with other frameworks.

This study analyses the ECSF from a structural perspective, focusing on hierarchical organisation, component granularity, and the relationships among roles, tasks, skills, and knowledge. We employ a structured expert elicitation protocol to carry out a comparative structural analysis of eight cybersecurity skills frameworks, including internationally adopted standards such as NICE, SFIA, ESCO, and CyBOK. Based on this analysis, we identify six structural limitations of the ECSF and propose corresponding enhancement strategies to support its evolution toward a more coherent, expressive, and interoperable European framework.

The study was conducted in the context of the AKADIMOS project, which aims to support the development of the European Cybersecurity Skills Academy and contribute to a coordinated effort to bridge the cybersecurity skills gap across the European Union.

1. Introduction

Cyber threats pose a significant challenge in Europe. The 2024 ENISA report [1] recorded approximately 161 security incidents across EU Member States, and malware families targeting banking applications grew by 200% year-on-year, increasing from 10 to 29 families and raising the number of affected applications globally from 600 to 1800. A robust response requires a well-trained European workforce, and cybersecurity skills frameworks are indispensable for defining clear learning pathways. In recent years, numerous European and global initiatives have developed comprehensive cybersecurity frameworks, each with strengths and limitations. However, their parallel evolution has produced notable divergences, underscoring the need for a common standard. A major step in this direction is ENISA's European Cybersecurity Skills Framework (ECSF) [2], which aims to create a common understanding among individuals, employers, and providers of learning programmes across EU Member States.

Despite its strategic relevance, the ECSF includes structural features (such as coding, hierarchy, and the relationships among roles, tasks, skills, and knowledge) that require careful analysis to ensure consistency and interoperability across the cybersecurity education ecosystem. Prior work by [3] and EU-funded initiatives have compared the ECSF with other competence systems. However, to our knowledge, no study has systematically analysed its structural limitations or proposed evidence-based improvement directions grounded in expert judgement and cross-framework comparisons with internationally adopted models such as National Institute for Cybersecurity Education (NICE), the Skills Framework for the Information Age (SFIA), the European Skills, Competences, Qualifications and Occupations framework (ESCO), and the Cybersecurity Body of Knowledge (CyBOK).

This gap in structural analysis limits the ECSF coherence, its interoperability with international standards, and its applicability to curriculum design, job profiling, and workforce development.

In addition, while the European Cybersecurity Skills Framework (ECSF) is often praised for its simplicity, this characteristic deserves a more in-depth examination. In particular, simplicity in ECSF primarily

* Corresponding author.
E-mail address: gaetano.perrone@unina.it (G. Perrone).

https://doi.org/10.1016/j.array.2026.100728
Received 4 December 2025; Received in revised form 25 February 2026; Accepted 25 February 2026
Available online 21 March 2026

serves semantic accessibility and shared understanding across heterogeneous stakeholders, rather than facilitating automated processing or direct tool integration. Recent empirical evidence from EU innovation projects shows that ECSF functions effectively as a common language through intensive human mediation by educators, trainers, and project teams, rather than through machine-level interoperability [4,5]. This observation motivates a deeper investigation into how simplicity interacts with usability, automation, and structural expressiveness.

The goal of our study is to analyse the structural properties of the ECSF in order to identify validated structural limitations and targeted improvement directions, derived from expert elicitation and cross-framework analysis.

From the systematic literature review conducted by [6], we identified eight cybersecurity skills frameworks, prioritising those with strong structural relevance and stable, publicly available documentation.

Then, we conducted a structured expert elicitation in which the experts identified the key limitations of the ECSF and proposed enhancement strategies based on related cybersecurity frameworks.

The contributions of this study can be summarised as follows:

1. We identify and categorise ECSF structural limitations through structured expert elicitation and cross-framework analysis.
2. We present a consolidated taxonomy that links each limitation to its rationale and to targeted enhancement directions.
3. We propose a set of evidence-based structural enhancements addressing each limitation, informed by mechanisms used in international frameworks.
4. We provide mapping strategies to align ECSF with NICE, SFIA, ESCO, and CyBOK, clarifying convergences, divergences, and interoperability gaps.

This work is structured as follows. Section 2 presents the European Cybersecurity Skills Framework (ECSF) and the international frameworks considered in this study, together with prior comparative analyses. Section 3 details the research design, including framework selection and the expert elicitation protocol. Section 4 reports the results of the study, describing the structural limitations identified in the ECSF, the corresponding enhancement strategies, and the cross-framework evidence underpinning them. Section 5 discusses the theoretical and practical implications of our findings, as well as study limitations. Finally, Section 6 concludes the work and outlines directions for future research.

2. Background and related works

This section presents the European Cybersecurity Skills Framework (ECSF) and other international cybersecurity skills frameworks relevant to our study. We provide a brief overview of research activities and cybersecurity frameworks, primarily within the context of European research projects, focusing on cybersecurity tasks, skills, and knowledge.

2.1. Design philosophies and governance models of competence frameworks

Competence frameworks differ not only in their internal structure and content, but also in their underlying design philosophies and governance models. These dimensions influence how competences are conceptualised, structured, maintained, and ultimately used in education, workforce planning, and professional development.

Design philosophy refers to the conceptual assumptions guiding how competences are identified, organised, and operationalised. In the literature, three main design orientations can be distinguished [7–9].

First, *knowledge-centric* frameworks prioritise the systematic organisation of disciplinary knowledge. These frameworks aim at conceptual completeness and epistemic coherence rather than direct role definition.

Second, *workforce- and role-centric* frameworks derive competences from professional practice, organising them around job roles, tasks, and operational responsibilities. In such frameworks, competences are primarily defined in relation to what professionals are expected to perform in real organisational contexts.

Third, *capability- and maturity-based* frameworks conceptualise competence as a progressive construct linked to increasing levels of autonomy, responsibility, and organisational impact. Skills Framework for the Information Age (SFIA) [10] embodies this philosophy by structuring skills across responsibility levels rather than fixed occupational roles, thus supporting career pathways and professional development across sectors.

Recent work on competence modelling further emphasises that frameworks may also differ in how they integrate technical, personal, and professional competences, extending the notion of competence beyond purely technical knowledge [11].

Beyond design philosophy, competence frameworks also differ in their governance models, which shape their evolution, adoption, and scope [7,8].

Public institutional governance refers to the frameworks maintained by governmental or supranational bodies. These frameworks are typically aligned with policy objectives, regulatory requirements, and labour market standardisation.

Academic governance models are driven by scholarly communities and emphasise disciplinary consensus, methodological transparency, and conceptual stability.

Finally, industry-driven governance models, such as that of SFIA, prioritise responsiveness to professional practice and market needs, enabling rapid updates and widespread organisational adoption.

The interplay between design philosophy and governance model strongly influences both the structural properties of a framework and its intended use contexts.

Table 1 summarises the main design philosophies and governance models of the competence frameworks analysed in this study, highlighting their conceptual diversity beyond mere structural and content differences.

2.2. The european cybersecurity skills framework

The European Cybersecurity Skills Framework [2] aims to ensure a common terminology to strengthen European cybersecurity culture, identify the critical skill set from a workforce perspective, and promote harmonisation in education and training. The ECSF identifies 12 cybersecurity professional role profiles that are typically required by organisations with regard to cybersecurity. Each profile can be adapted, or roles can be combined to meet the requirements of specific situations, organisations, and stakeholder needs. For each role, its mission, a set of tasks, skills, and knowledge are identified, along with a mapping to the e-CF [12] (which corresponds to the EN16234-1 e-Competence Framework, a common European framework for ICT professionals across all sectors). One of the main objectives of ECSF is simplicity, which ensures that the framework is comprehensive and thus applicable to as wide an audience as possible. The framework is also flexible and scalable, so each component can be extended or used independently. The ECSF working group was also composed of different experts following a multi-perspective approach in order to make it open and impartial. The benefits of using ECSF are applicable to organisations, trainers, and individuals. From the perspective of organisations, the framework can be seen as a support in the recruitment process and analysis of cybersecurity skill gaps. It also provides a common language and supports the development of a cybersecurity strategy and organisational structure. Providers of learning programs can find support for designing learning programs and curricula, as well as aligning training courses with cybersecurity gaps and workforce demand. Additionally, individuals can benefit from the ECSF because it helps them make informed professional career choices, understand practical job requirements, and reskill or upskill accordingly.

Table 1
Design philosophies and governance models of analysed frameworks.

Framework	Design philosophy	Governance model
ECSF	Workforce-oriented, role-based	Public institutional (ENISA/EU)
REWIRE	Structural extension of ECSF (workforce-oriented, role-based)	EU-funded project consortium
NICE	Workforce-oriented, task-based	Public institutional (NIST/US Gov.)
SPARTA	Empirical extension of NICE (workforce- and task-based)	EU-funded project consortium
SFIA	Capability- and maturity-based	Industry-driven (SFIA Foundation)
CyBOK	Knowledge-centric, domain-based	Academic consortium
ESCO	Labour-market and occupation-oriented	Public institutional (European Commission)
JRC Taxonomy	Policy-oriented, multidimensional classification	Public institutional (EU JRC)

2.2.1. ECSF key concepts

The ECSF was designed with four key principles in mind:

1. *Simple yet comprehensive*: suitable for a wide audience yet sufficiently detailed to provide in-depth cybersecurity insights across a broad spectrum of activities and environments, and for stakeholders from a variety of backgrounds;
2. *Flexible and scalable*: modular and flexible structure, tailored to be extendable or useable independently by organisations;
3. *Open and impartial*: developed by a large and diverse working group of professional cybersecurity experts. ECSF profiles and components follow a multi-perspective approach, eliminating bias toward specific areas of interest. It is publicly available, accessible, and open;
4. *European*: aimed at minimising gaps in cybersecurity skills and workforce shortages across Europe.

The three key goals that ECSF enables are:

1. *Employing cybersecurity professionals in an organisation*: by using the ECSF, hiring managers can identify competence gaps within their organisation and guide the employment process accordingly;
2. *Skilling cybersecurity professionals*: the framework helps security professionals focus their learning efforts on the specific skills required for their career path, ensuring targeted and efficient professional development;
3. *Making informed career choices*: the framework assists individuals in finding workplaces that best align with their personal ambitions and expectations.

2.2.2. Role profiles

The ECSF identifies twelve key profiles:

1. CISO (Chief Information Security Officer) — Leads the organisation's cybersecurity strategy and oversees its implementation.
2. Cyber Incident Responder — Detects and handles cyber incidents to restore normal operations.
3. Cyber Legal, Policy & Compliance Officer — Ensures legal and regulatory compliance in cybersecurity.
4. Cyber Threat Intelligence Specialist — Gathers and analyses threat data to inform security actions.
5. Cybersecurity Architect — Designs secure system architectures and integrates security by design.
6. Cybersecurity Auditor — Evaluates systems for compliance with security standards and regulations.
7. Cybersecurity Educator — Provides cybersecurity training, awareness, and education.
8. Cybersecurity Implementer — Develops and maintains cybersecurity solutions and systems.
9. Cybersecurity Researcher — Conducts research to innovate and improve cybersecurity practices.
10. Cybersecurity Risk Manager — Manages cybersecurity risks aligned with the organisation's strategy.
11. Digital Forensics Investigator — Analyses digital evidence to support cybercrime investigations.
12. Penetration Tester — Simulates attacks to identify vulnerabilities and assess security controls.

Each profile has a set of key components:

- **Profile Title** — Official name of the role.
- **Alternative Title(s)** — Common variations or similar role names.
- **Summary Statement** — One-sentence summary of the role's purpose.
- **Mission** — Core responsibilities and objectives.
- **Deliverable(s)** — Tangible outputs the role is expected to produce.
- **Main Task(s)** — Key duties and activities.
- **Key Skill(s)** — Abilities required to perform the role effectively.
- **Key Knowledge** — Required areas of understanding and expertise.
- **e-Competences** — Mapped skills from the European e-Competence Framework, including proficiency levels.

Appendix A shows the Cyber Incident Responder role profile from the framework.

2.2.3. ECSF design considerations

According to the design philosophies described in Section 2.1, the ECSF can be classified as a workforce- and role-centric framework governed by a public institutional model. This positioning aligns ECSF with other workforce-oriented public frameworks such as NICE, while distinguishing it from capability-based (SFIA) and knowledge-centric (CyBOK) models.

Its primary focus is on defining professional roles and associated competences to support workforce development across Europe.

This design choice implies that its structural simplicity is optimised for semantic alignment among stakeholders rather than for machine-actionability.

Empirical evidence from EU innovation projects shows that ECSF effectively supports process-based integration through expert-driven workflows, but provides limited support for automated mapping, computational interoperability, or large-scale analytical processing [5].

Fig. 1 shows an Entity-Relationship diagram representing the ECSF structure. This diagram highlights the simplicity of the ECSF design, which prioritises simple core concepts (Role, Task, Skill, and Knowledge) in spite of more structural expressiveness desirable for interoperability and automation.

2.3. International cybersecurity skills frameworks

The NIST NICE Workforce Framework for Cybersecurity [13] is one of the most widely adopted international references for structuring the cybersecurity profession. NICE organises the field through Work Roles composed of Tasks, Knowledge, and Skill statements, grouped into Categories and Speciality Areas. The framework provides consistent terminology and a modular architecture that enables organisations to describe work activities and the competences required to perform them.

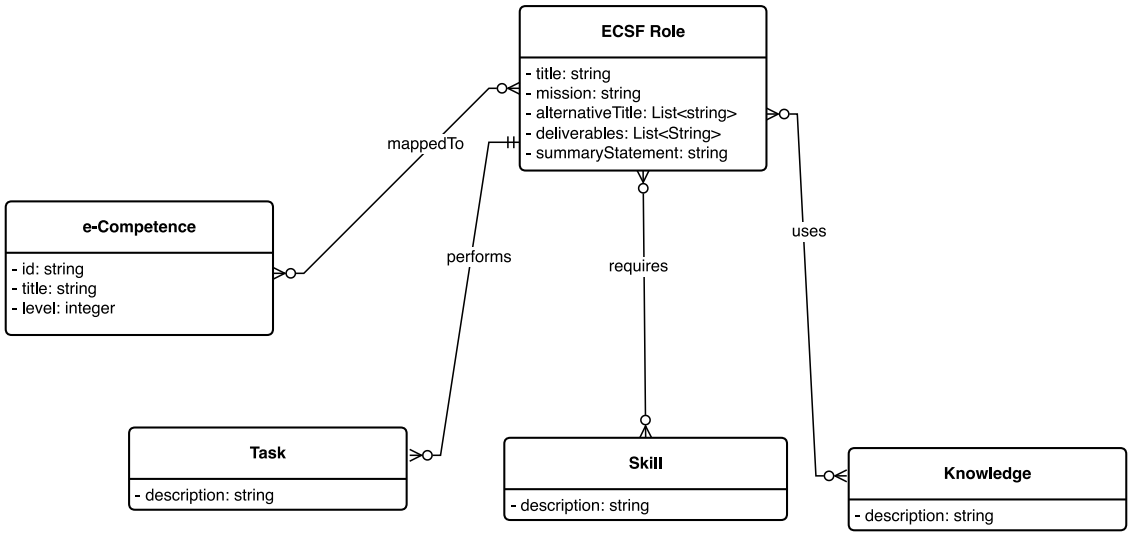


Fig. 1. Entity-relationship diagram of the current ECSF framework.

NICE is used extensively in workforce planning, curriculum development, and job profiling, and serves as a baseline for understanding how cybersecurity tasks and competences can be formally modelled. Its influence extends across academic, industrial, and governmental settings, making it a central point of reference for many comparative studies on cybersecurity skills frameworks.

According to the classification introduced in Section 2.1, NICE reflects a workforce-oriented design supported by a public institutional governance model.

The Skills Framework for the Information Age (SFIA) [10] is an internationally recognised skills and competence framework covering digital, IT, and cybersecurity-related professions. It defines seven levels of professional responsibility and autonomy, which provide a graded structure for modelling increasing degrees of complexity and proficiency. SFIA's skills catalogue is designed to be cross-sector and role-agnostic, enabling consistent representation of digital competences across diverse organisational contexts. Although not limited to cybersecurity, SFIA is frequently used by organisations for career pathway design, HR processes, and training planning. Its maturity-level structure and controlled vocabulary have made SFIA a reference model for representing progression and professional development within digital occupations.

Unlike role-based frameworks, SFIA adopts a capability- and maturity-based design governed by an industry-led model, which distinguishes it structurally from ECSF and NICE.

The Cyber Security Body of Knowledge [14] is a comprehensive academic reference that consolidates cybersecurity knowledge into 21 domain-specific Knowledge Areas. Each area provides an in-depth synthesis of foundational concepts, techniques, and theoretical perspectives. CyBOK is not a role-based framework; rather, it establishes a stable conceptual ontology of the cybersecurity discipline that informs curriculum design, certification schemes, and research agendas. The project has been influential in aligning educational programmes with a common cybersecurity knowledge baseline, and it serves as a foundation for many initiatives seeking to classify or structure cybersecurity learning outcomes.

By contrast to NICE and SFIA, CyBOK follows a knowledge-centric design under academic governance, which explains its limited role-based operationalisation and its primary function as a conceptual reference rather than a workforce model.

2.4. Related frameworks not focused on security

Other frameworks are not specifically related to cybersecurity, but provide relevant insights for the aims of our study.

The European Skills, Competences, Qualifications and Occupations (ESCO) [15] framework is the European multilingual classification of Skills, Competences and Occupations. It functions as a dictionary, providing detailed descriptions of professional occupations and skills relevant to the EU labour market, as well as education and training. The latest version of the framework (v1.2) offers 3039 occupations and 13,939 skills linked to occupations, providing a comprehensive set of competences.

From a design perspective (Section 2.1), ESCO adopts a labour-market and occupation-oriented philosophy, focusing on the standardised representation of skills and occupations across sectors rather than on domain-specific professional roles.

Its governance model is public institutional, as it is maintained by the European Commission to support regulatory alignment, workforce mobility, and interoperability among national education and employment systems.

The Joint Research Centre (JRC) [16] maintains a taxonomy for digital competences that groups skills across application domains, technological areas, and sectoral contexts. The taxonomy provides a high-level classification to support policy development, digital skills monitoring, and cross-domain comparability. Although not focused solely on cybersecurity, its multidimensional organisation highlights how digital competences can be aggregated and contextualised across sectors. The taxonomy has been used in EU-level analyses of digital skills demand and serves as a complementary reference for understanding broader competence structures beyond cybersecurity.

In terms of design philosophy, the JRC taxonomy follows a policy-oriented, multidimensional classification approach, structuring competences across domains, technologies, and application contexts rather than by occupational roles.

The governance model is public institutional, as the taxonomy is developed and maintained by the EU Joint Research Centre to support policy analysis, skills monitoring, and evidence-based decision-making at the European level.

Other generic competence frameworks support the design and evaluation of domain-specific professional frameworks. Several studies employ methodologies that differ from ours, thereby offering complementary perspectives. In the nursing domain, inductive content analysis [17,18] and qualitative document analysis [19] have been used to classify professional competences.

In the cybersecurity domain, the approach is similar to that followed by [3] but differs from ours, which relies on structural refinement driven by experts. In contrast, these studies primarily focused on descriptive classification and cross-context comparison. In medical

education, [20] designed a generic competence framework using an action research methodology. The authors identified four main domains, namely patient-centred care, teamwork, system-based practice, and personal and professional development. This work emphasised iterative refinement through stakeholder engagement and demonstrated how generic competence domains can guide domain-specific adaptations without enforcing rigid prescriptions. Our study differs from these approaches by placing a stronger emphasis on expert involvement to improve the structural properties of the ECSF. In this respect, our work aligns with studies that explicitly stress the importance of professional expertise in the development of competence frameworks. For instance, [21,22] conducted structured literature reviews to examine existing competence frameworks and proposed systematic and replicable methodologies grounded in both scientific evidence and practitioner input. Both studies underscore the importance of expert participation to ensure methodological rigour and practical relevance in the design of competence frameworks. Other contributions integrate multiple competence models using alternative strategies. For example, [7] conducted an integrative literature review to design a comprehensive taxonomy of competence models. Although we did not follow a systematic literature review process, our approach is comparable, as we extracted a set of cybersecurity frameworks from the systematic literature review conducted by the CyberSecPro [6] initiative and synthesised their structural features through expert elicitation. Competence frameworks also depend on the availability of adequately prepared educators, since competences cannot be developed without competent instructional actors. Several initiatives, therefore, focus on educator-specific competence modelling. A prominent example is the European Framework for the Digital Competence of Educators (DigCompEdu) [23], which organises twenty-two digital competences into six areas. Although DigCompEdu does not target cybersecurity directly, digital competence constitutes an enabling layer for cybersecurity education and training.

2.5. Theoretical foundations for the structural analysis of competence frameworks

This section presents the theoretical foundations that underpin our analysis of the ECSF and related cybersecurity competence frameworks. It focuses on three complementary dimensions: the structural foundations of competence frameworks, learning taxonomies for competence progression, and the role of competence mappings to courses and certifications.

2.5.1. Structural foundations of competence frameworks

Competence frameworks aim to represent professional activities in a form that supports comparison, reuse, and alignment across organisational, educational, and policy contexts. This objective requires sufficient structural expressiveness, including explicit decomposition into roles, tasks, skills, and knowledge, as well as mechanisms for hierarchy, abstraction, and formal coding.

Prior studies in competence modelling argue that well-formed competence hierarchies improve interpretability and operationalisation by enabling consistent mappings between occupational profiles, curricula, and qualification schemes [24–26]. International frameworks such as NICE and SFIA exemplify this approach by introducing intermediate abstraction layers and graded structures that support interoperability and progressive competence development [10,27].

These principles provide the theoretical grounding for analysing the ECSF not only in terms of coverage but also in terms of internal structure, granularity, and interoperability.

2.5.2. Learning taxonomies and competence progression

Educational taxonomies provide established theoretical tools for representing progression in learning and competence acquisition. Bloom's taxonomy organises cognitive processes into hierarchical levels of complexity and has been widely adopted for specifying learning outcomes and designing assessments [28,29]. Constructive alignment [30] further requires that learning activities and assessment methods align with explicitly defined learning outcomes.

These models motivate the introduction of graded competence levels in professional skills frameworks. Proficiency tiers enable transparent progression pathways and support consistent interpretation across roles, training programmes, and certification schemes. Learning taxonomies, therefore, provide a relevant theoretical basis for analysing skill-level expressiveness and progression in cybersecurity competence frameworks.

2.5.3. Mapping strategies to courses and certifications

The structural analysis of competence frameworks also includes an examination of mapping strategies between cybersecurity courses and certifications. This mapping is an important mechanism for aligning educational programs with professional standards and workforce requirements.

Empirical studies demonstrate that systematic mapping improves coherence between learning objectives, instructional design, and labour market expectations [31,32]. Educational institutions can therefore translate abstract competence descriptions into concrete learning activities and assessment strategies.

Additionally, this mapping supports consistent credentialing and continuous curriculum improvements by defining structured learning outcomes, performance milestones, and evaluation criteria driven by stakeholder feedback [33,34]. This structure ensures that learning outcomes remain relevant and measurable.

Finally, competence mapping clarifies targeted proficiency levels and enables tailored learning outcomes and specialisation pathways [31,35].

In certification and credentialing systems, competence-based frameworks provide transparent assessment criteria and enhance the credibility and comparability of qualifications [36,37]. Empirical evidence indicates that integrating competences across curricula improves graduate readiness and employer satisfaction [33,38]. Such integration also strengthens quality assurance mechanisms and supports professional development across career stages [32,34].

Linking knowledge and skills frameworks to courses and certifications extends beyond technical correspondence and involves systemic and market considerations. Higher education systems and certification ecosystems operate within competitive knowledge-based labour markets. Institutional strategies, policy incentives, and employer demand shape curricular and credentialing decisions [39].

National education policies, competitive university dynamics, and accreditation regimes mediate curricular responsiveness to labour market needs. Framework design alone does not determine such responsiveness [39]. The feasibility of linking a skills framework to concrete educational offerings, therefore, depends on institutional embedding as much as on formal structure.

Certification schemes play a critical role in this process. The integration of industry-recognised certifications into instructional design bridges gaps between learning outcomes and industry requirements and improves graduate employability [40].

Competitive certification markets also enhance job readiness, including for candidates from non-traditional educational backgrounds, by providing alternative pathways to recognised qualifications [41].

Recent integrated models demonstrate that combining courses, competitions, and certifications aligned with job roles strengthens workforce competences and supports sustainable career development [35, 42]. These models position certification systems and labour market

signalling mechanisms as core components of educational design alongside formal curricula.

Systemic and market factors determine the feasibility of linking knowledge and skills frameworks to courses and certifications more strongly than technical mapping alone [39,41]. Framework operationalisation, therefore, constitutes a socio-technical coordination problem rather than a purely formal alignment task.

Taken together, these considerations underscore the importance of analysing the feasibility of mapping the ECSF.

2.6. Cybersecurity initiatives

Several European projects have contributed artefacts, taxonomies, and methodologies relevant to cybersecurity competence modelling. Initiatives such as REWIRE [43], SPARTA [44], CONCORDIA [45], and ECSO [46] have produced mappings, training guidelines, and specialised role definitions tailored to specific sectors or threat domains. These projects vary widely in scope, methodology, and outputs, reflecting the heterogeneity of the European cybersecurity skills landscape. While they provide valuable domain-specific insights and training resources, their approaches are not standardised, and their outputs differ in granularity, terminology, and structural assumptions. Collectively, they illustrate the fragmented nature of cybersecurity competence development across Europe and underscore the need for harmonisation efforts such as the ECSF.

2.7. Prior comparative studies and ECSF analyses

Research on the European Cybersecurity Skills Framework (ECSF) is still in its early stages, but initial studies highlight both its potential and the need for further evaluation. Early findings indicate that the implementation of the ECSF provides practical benefits for organisations, policymakers, and educational institutions by supporting the development of a skilled cybersecurity workforce and promoting best practices in training and education [47]. However, detailed assessments of its strengths and weaknesses are still limited, as the framework is relatively new and comprehensive empirical studies are lacking.

The most relevant study is provided by Almeida [3]. In this work, the author conducted a quantitative content analysis [48,49] of 10 EU-based cybersecurity skills frameworks, obtained from a systematic literature review developed by the CybersecPro [50] initiative. The study defined several strengths and limitations of the analysed cybersecurity skills frameworks.

Focusing on the ECSF (Table 2), [3] shows that the framework provides strong policy alignment, workforce mobility, and career pathway support, but suffers from excessive complexity, incomplete coverage, and limited skill matching. These structural issues motivate the analysis proposed in our study.

With respect to methodology, we followed the same criteria for selecting the most relevant frameworks, but there are a number of important differences between our study and that of [3]. First, [3] does not describe the participants involved in the thematic coding process. Our analysis involved expert elicitation and included a hybrid group of researchers and security experts to identify a shared agreement in order to pinpoint key strengths and limitations. Secondly, while [3] provides a comparative study of frameworks across different aspects, including adoption issues, stakeholder representations, and knowledge coverage, our analysis focused on the ECSF, concentrating on structural aspects such as coherence, hierarchy, and granularity. This distinction is important because our findings, by examining internal structural qualities, indirectly address some of the issues identified by Almeida.

Recent studies have produced a substantial body of evidence on cybersecurity skills frameworks, curriculum design approaches, and mechanisms for workforce alignment. Taken together, these studies provide important context for understanding the current limitations of the ECSF and the broader landscape in which it operates.

Table 2
Strengths and limitations of EU-based cybersecurity frameworks, with ECSF coverage [3].

Theme	ECSF
Strengths	
Alignment with Policy Goals	Y
Decision-Making Tool	N
Enhanced Collaboration	N
Enhanced Training and Education	Y
Improved Workforce Mobility	Y
Increased Cybersecurity Readiness	Y
Resource Optimisation	N
Standardised Skill Definitions	Y
Support for Career Pathways	Y
Support for Cybersecurity Startups	N
Support for Research and Innovation	N
Limitations	
Broad Scope	Y
Complexity	Y
Dependency on Adoption	Y
Geographical Disparities	N
Incomplete Coverage	Y
Lack of Alignment with Local Regulations	Y
Lack of Specific Skill Matching	Y
Lack of Target for SMEs	Y
Limited Focus on Soft Skills	Y
Limited Interaction and Collaboration Data	N
Narrow Stakeholder Representation	N

A recurrent theme in prior research concerns the structural fragmentation of cybersecurity skills frameworks. Comparative analyses consistently report significant heterogeneity in how roles, tasks, skills, and knowledge elements are conceptualised across European and international models [3]. Studies examining NICE, CSEC2017, ECSF, SPARTA, and CyBOK highlight pronounced structural divergence and the absence of a shared meta-model that could support systematic cross-framework harmonisation [51,52]. Related research in human resource development similarly identifies the lack of a unified competence reference as a critical barrier to strategic workforce planning and cross-domain integration [53].

Another substantial line of work focuses on misalignment between academic curricula and workforce-oriented frameworks. Quantitative mappings between educational guidelines such as CSEC2017 [54] and workforce taxonomies like NICE [13] reveal notable discrepancies in knowledge coverage and cognitive depth [51]. Algorithmic analyses based on association-rule learning further demonstrate that competence priorities inferred from workforce needs diverge from traditional academic emphases [55]. Data-driven evaluations expose systematic differences between industrial and academic perspectives, especially regarding organisational, human-centric, and governance-related competences [56]. Complementary evidence from scenario-based educational studies reinforces the need to map learning outcomes directly to competences articulated in the workforce frameworks [57].

A further line of research highlights persistent gaps in human, behavioural, and wider non-technical competences. Workforce-oriented studies underscore communication, teamwork, adaptability, and other soft skills as essential yet underrepresented in existing frameworks [58]. Gender-focused analyses emphasise the importance of soft skills for career progression while noting that such competences remain marginal in ECSF and NICE profiles [59]. Research on team-centric learning additionally demonstrates that socio-technical and collaborative capabilities are fundamental for effective cybersecurity practice [60].

Emerging technological and socio-technical domains also appear insufficiently covered in current frameworks. Curriculum studies and cross-framework comparisons highlight limited treatment of AI security, quantum-resistant cryptography, cloud–edge architectures, and cyber–physical systems [51,52]. Broader scoping reviews point to a convergence among cybersecurity, data science, and Cyber–Physical

Systems (CPS), suggesting the need for integrated models that span technical, organisational, and ethical dimensions [61]. Finally, several studies identify systemic challenges affecting cybersecurity education and workforce development in Europe. A recent PESTLE-based investigation identifies fragmented certification systems, limited coordination across Member States, resource constraints, and sustained misalignment between education systems and labour-market requirements [62]. These findings echo a broader consensus that, despite numerous initiatives, Europe still lacks a unified structural model to guide skills development and competence standardisation.

Taken together, prior comparative studies and empirical analyses indicate that, while existing research has thoroughly documented individual frameworks, structural misalignments, and domain-specific gaps, no study to date has proposed a coherent, evidence-based enhancement of the ECSF grounded in cross-framework synthesis. This gap provides the motivation for the present work.

3. Methodology

This section outlines the research methodology used to analyse the structural limitations of the ECSF and propose enhancement strategies. We first describe the overall study design, followed by details on framework selection, expert elicitation protocols, mapping procedures, and data analysis techniques.

3.1. Study design

The study integrates two methodological pillars:

- structured expert elicitation [63] to gather qualitative insights regarding ECSF structural limitations;
- framework analysis [64], through which experts systematically compared ECSF with established international cybersecurity skills frameworks.

Fig. 2 summarises the overall methodological pipeline, which begins with the identification of relevant frameworks, proceeds through expert-based analysis, and culminates in the synthesis of structural limitations and improvement proposals.

3.2. Framework selection

The selection of comparative frameworks for analysis followed a two-step process combining grey literature-driven identification and expert validation.

First, following the approach of [3], a preliminary set of candidate cybersecurity skills and competence frameworks was identified through systematic literature reviews and project surveys provided by the CybersecPro initiative [6]. This initial screening focused on frameworks widely referenced in the context of European cybersecurity workforce development and skills policy.

Second, the expert group refined this preliminary list by applying two complementary selection dimensions:

1. *Structural relevance*, defined through formal indicators enabling analytical comparison with ECSF from a design and modelling perspective;
2. Availability of stable and publicly accessible documentation allowing meaningful inspection of the framework structure.

We defined a set of *structural relevance indicators*, which characterise the suitability of a framework for structural analysis and comparison: (i) explicit hierarchical organisation, (ii) decomposition into core competence components (tasks, skills, knowledge or equivalent), (iii) the presence of a coding or identification scheme, (iv) explicit interdependency or relational models among components, and (v) structural documentation maturity (Table 3).

Table 3
Structural and methodological indicators satisfied by the analysed cybersecurity frameworks. H = hierarchical structure; TSK = explicit Tasks–Skills–Knowledge decomposition; C = coding scheme; R = explicit relationships; D = documentation maturity (stable and publicly accessible structural documentation).

Framework	H	TSK	C	R	D
Included frameworks					
ECSF (ENISA)	✓	✓	–	–	✓
CyBOK	✓	–	✓	–	✓
NIST NICE	✓	✓	✓	✓	✓
SFIA	✓	–	✓	–	✓
ESCO	✓	✓	✓	–	✓
SPARTA CSF	✓	✓	–	✓	✓
REWIRE	✓	✓	–	–	✓
JRC Cybersecurity Taxonomy	✓	–	✓	–	✓
Excluded frameworks					
CONCORDIA CSF	✓	–	–	–	–
CyberSec4Europe CSF	✓	✓	–	–	–
ECHO CSF	✓	–	–	–	–

Note that inclusion was not determined solely by the number of satisfied indicators.

Rather, a framework was included if it was structurally comparable or complementary to the ECSF for the purposes of this analysis, and if its documentation provided a level of detail comparable to that of the ECSF. In particular, frameworks were selected when they either featured a decomposition that enabled structural alignment with the ECSF (e.g., roles, tasks, skills, knowledge), or offered a formally defined structural dimension that complemented the ECSF (e.g., a systematic organisation of cybersecurity knowledge or graded skill hierarchies).

The final inclusion and exclusion decisions, integrating structural relevance, adoption, and documentation availability, are reported in Table 4.

3.3. Expert elicitation protocol

We followed the structured expert elicitation protocol proposed by [65,66], which consists of four main steps: *Investigate*, *Discuss*, *Estimate*, and *Aggregate*. Fig. 3 illustrates the expert elicitation protocol.

In the first step (*Investigate*), each expert individually reviewed the selected cybersecurity skills frameworks to identify potential structural limitations. Subsequently, two rounds of group discussions were held (*Discuss*) to brainstorm and share insights among the experts.

In the third step (*Estimate*), experts collaboratively refined the list of limitations and improvement areas. A qualitative severity assessment (low/medium/high) was assigned to each limitation based on relevance and impact on interoperability and clarity. No numerical aggregation was applied.

Finally, in the *Aggregate* step, the findings were synthesised into a semi-structured format for further analysis, capturing the following for each framework:

- key structural features;
- strengths;
- limitations;
- implications for ECSF.

In addition to qualitative elicitation, a structured survey was administered to the participating experts to assess the perceived relevance of each identified limitation. Each item was rated on a five-point Likert scale [67] ranging from “ineffective” (1) to “essential” (5). The resulting distributions allowed us to quantify convergence patterns among experts and to empirically weight the relative importance of each limitation.

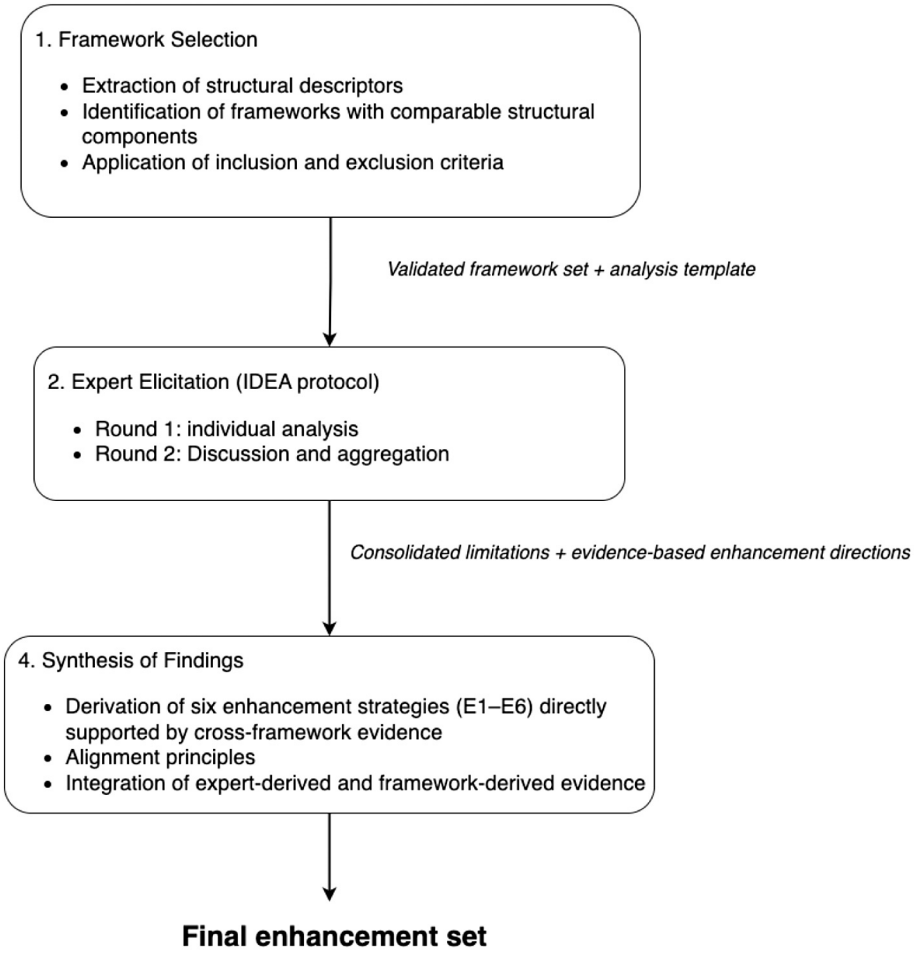


Fig. 2. Overall methodology pipeline.

Table 4
Frameworks considered and inclusion decisions based on structural relevance, adoption, and documentation availability.

Framework	Included	Rationale	Source
ECSF (ENISA)	Yes	Core object of analysis. Provides role–task–skill structure with EU policy relevance.	EU
CyBOK	Yes	Mature knowledge-domain hierarchy with codified areas; essential for evaluating modularity and domain coverage.	UK
NIST NICE	Yes	Provides hierarchical tasks and KSAs with formal relations; widely adopted reference for benchmarking granularity.	US
SFIA	Yes	Provides graded skill levels with codified identifiers and cross-domain competence structure.	Intl.
ESCO	Yes	Offers EU-wide classification of occupations and skills with explicit coding; useful for mapping roles and transversal skills.	EU
JRC Cybersecurity Taxonomy	Yes	Provides conceptual categories and codified knowledge domains; supports structural comparison at the knowledge level.	EU
SPARTA CSF	Yes	Extends NICE with EU-oriented topic taxonomy and task–skill relations; high granularity and documentation maturity.	EU
CONCORDIA CSF	No	Limited structural depth (focus on training initiatives); insufficient formal task–skill specification.	EU
CyberSec4Europe CSF	No	Provides competence mapping but lacks stable, publicly available structural documentation.	EU
ECHO CSF	No	High-level role descriptions without sufficient structural detail for analytical comparison.	EU
REWIRE Cybersecurity Skills Framework	Yes	Provides structured role profiles, competence clusters, and learning pathways aligned with ECSF.	EU

Ten experts participated in the elicitation process, divided into two groups. The primary group consisted of six experts: five academic researchers (two senior researchers, one postdoctoral researcher, and two late-stage PhD candidates) and one senior cybersecurity consultant with 10 years of industry experience and multiple relevant professional certifications, including the Offensive Security Certified Professional (OSCP) [68] and the Certified Information Systems Security Professional (CISSP) [69,70]. The validation group consisted of four professionals in education, industry, and government with extensive experience in cybersecurity training and workforce development.

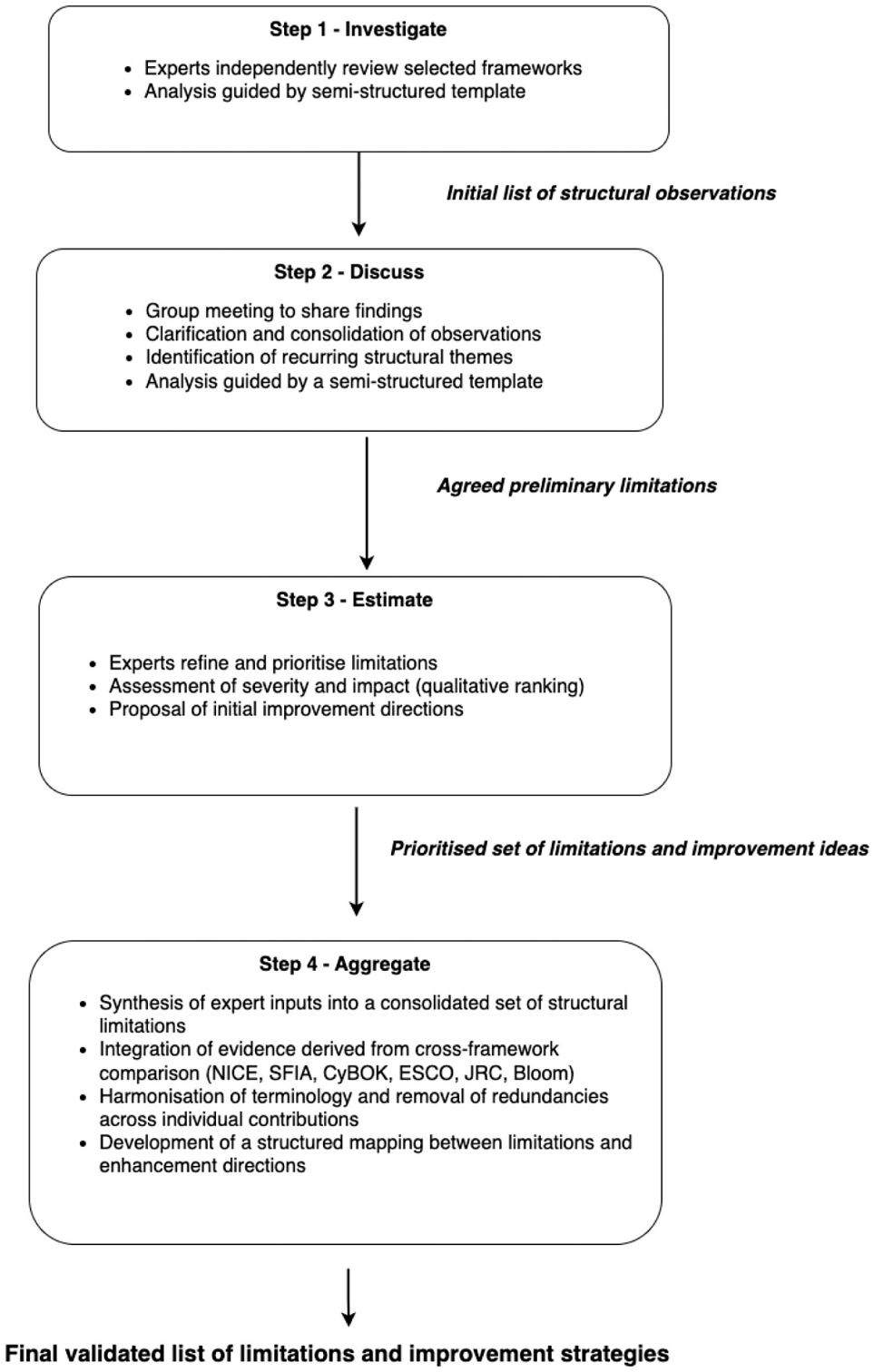


Fig. 3. Expert elicitation protocol.

The primary group was based in Italy, whereas the validation group was geographically distributed across Italy and Greece. Experts were selected based on reputation, domain expertise, and direct involvement in cybersecurity skills initiatives, including participation in EU-funded projects and alignment with the objectives of the AKADIMOS initiative.

The final elicitation process produced:

1. a consolidated set of ECSF structural limitations;
2. a corresponding list of proposed structural improvements;
3. a cross-framework evidence base linking each limitation to specific external frameworks.

Severity assessments and consensus interpretation were handled qualitatively, following standard guidelines for structured expert elicitation.

3.3.1. Recruitment and ethical considerations

Participants were recruited through targeted invitations sent to known experts who participated in the AKADIMOS project. This approach ensured the selection of individuals with high-level professional reputations and direct involvement in EU-level skills initiatives.

Informed consent was obtained from all subjects involved in the study. Participants were fully informed of the study's purpose regarding ECSF evaluation and the IDEA protocol methodology. In accordance with the principles of professional ethics and conduct, participation was entirely voluntary. Agreement to participate in interview rounds and group discussions was considered implied verbal consent. To ensure confidentiality and impartiality, the identities of the experts have been anonymised. Aggregated data supporting these findings are included in the article and its supplementary materials,[1] while all the raw digital data used during the interviews were stored in an encrypted repository and protected by Multi-Factor Authentication (MFA).

4. Results

This section presents the obtained results. We illustrate the limitations identified, related enhancement proposals, and mapping strategies proposed by experts to ensure interoperability across frameworks.

Several of the structural issues identified in this section echo patterns observed in prior comparative studies discussed in Section 2.7. However, the present analysis reformulates these issues in terms of internal structural properties of the ECSF and translates them into concrete enhancement strategies grounded in expert elicitation and cross-framework evidence.

4.1. Structural limitations of ECSF

The study revealed six key limitations of the ECSF and identified the frameworks that address these shortcomings.

L1 — Unstructured tasks, skills, and knowledge

Knowledge items in ECSF are expressed as flat enumerations without hierarchical grouping, coding, or domain clustering. This makes it difficult to reuse knowledge elements across roles, compare them across frameworks, or integrate them into curricula. Conversely, CyBOK organises knowledge into well-defined knowledge areas with consistent structures, enabling more rigorous curriculum alignment.

Body-of-knowledge initiatives and comparative studies argue that knowledge organisation benefits from coherent domain structures and modular decomposition, rather than flat enumerations [14,71,72].

Additionally, ECSF uses simple alphanumeric identifiers for roles but does not provide a coding structure for skills, tasks, or knowledge items. This limits extensibility, tool integration, and automated mapping. Other frameworks adopt hierarchical or semantically meaningful codes that support versioning, extensibility, and interoperability.

Competence modelling research highlights that consistent identifiers and structured representations support extensibility, interoperability, and integration with organisational systems [8,73].

Finally, while some ECSF roles are strategically scoped (e.g., Chief Information Security Officer), others are narrowly focused (e.g., Penetration Testers). Experts noted that this irregular granularity complicates mapping to workforce roles, curriculum units, and job market requirements. Other frameworks maintain more homogeneous granularity through hierarchical role families (NICE) or modular capability sets (SFIA).

[1] https://zenodo.org/records/18312770

Prior comparative research highlights heterogeneity in how cybersecurity roles and competence elements are scoped and decomposed, which complicates mapping across frameworks and translating framework elements into curricula and job profiles [3,51].

L2 — Missing interdependency among tasks, skills, and knowledge

The ECSF defines roles as collections of tasks, skills, and knowledge items, but the model does not explicitly articulate the relationships among these components.

Tasks do not reference the skills required to perform them, skills do not reference relevant knowledge, and knowledge items are not organised hierarchically.

This weak interdependency reduces the framework's expressiveness and makes it difficult to derive competence pathways or learning outcomes. Other frameworks, such as NICE and SFIA, provide stronger structural linkage through explicit role-task-skill mappings or hierarchical coding schemes, which enhance their usability in curriculum design and workforce development.

Prior work on cybersecurity curricula and skills frameworks emphasises the value of explicit mappings between competence components to support operational use in curriculum design and tooling [52,74]. Our findings indicate that ECSF currently provides limited explicit linkage between tasks, skills, and knowledge, which constrains traceability and reuse [3].

L3 — No competence levels for skills

Although ECSF roles are indirectly linked to the European e-Competence Framework (e-CF) through role-level mappings, competence levels are not defined at the skill level. This introduces ambiguity when comparing skills across roles or designing progressive learning trajectories. Competence levels are widely recognised as essential in frameworks such as SFIA (seven levels) and e-CF (five levels), and their absence reduces ECSF precision and interoperability.

The absence of skill-level proficiency tiers limits competence progression modelling and complicates assessment and curriculum alignment, as discussed in learning and competence structuring literature [28–30].

L4 — No seniority levels for roles

ECSF roles do not include seniority distinctions (e.g., junior, mid-level, senior). This hinders the representation of career progression and complicates the use of ECSF in recruitment, workforce planning, and certification alignment. Other frameworks (e.g., SFIA, e-CF) provide explicit responsibility levels, but ECSF currently lacks equivalent constructs.

The lack of seniority differentiation limits career pathway representation, which contrasts with models that explicitly encode responsibility or proficiency levels, such as SFIA and e-CF [10,75].

L5 — Missing coverage of emerging domains

Cybersecurity is a domain that evolves in parallel with technological advancements.

As the ECSF was published in 2022, it does not explicitly account for several rapidly evolving domains, such as artificial intelligence security [76], cloud–edge infrastructures [77,78], IoT security [79], and quantum-safe cryptography [80].

This temporal lag risks reducing ECSF relevance and may discourage

Table 5
Analysis of mean scores and top-2 Box proportions for limitations L1 through L6.

Limitation	Mean score	Top-2 box (4–5)
L1	3.94	0.72
L2	3.94	0.72
L3	3.28	0.35
L4	3.50	0.43
L5	4.15	0.79
L6	3.86	0.65

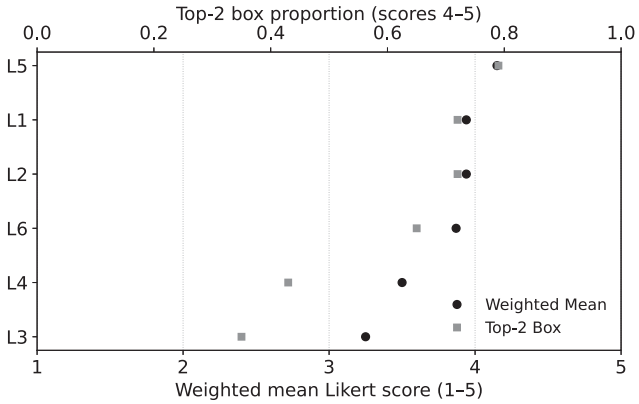


Fig. 4. Empirical weighting of ECSF limitations based on expert Likert ratings. Dots represent weighted mean scores, while squares indicate top-2 box proportions (scores 4–5).

its adoption in cybersecurity training and certification programs.

L6 — Limited linkage to training pathways and certification

Although ECSF is increasingly referenced by certification bodies and training providers, current mappings remain largely confined to the role level [81]. Skills and knowledge elements are not systematically connected to specific courses, curricula, or certifications. This limits ECSF effectiveness as a practical bridge between competence definitions and concrete learning or certification pathways, thereby constraining educator adoption and learner guidance [82].

4.1.1. Frequency and convergence patterns of limitations

To empirically weight the identified limitations, we complemented the qualitative expert elicitation with a Likert-scale survey. Table 5 reports the weighted mean scores and top-2 box proportions (scores 4–5) for each limitation.

All six limitations are consistently perceived as relevant, with none rated as marginal or negligible by the experts.

Fig. 4 shows that the most critical limitations are the lack of coverage of emerging domains (L5), followed by the absence of explicit structural organisation (L1) and missing interdependencies among tasks, skills, and knowledge (L2). By contrast, limitations related to skill-level granularity (L3) and role seniority differentiation (L4) receive comparatively lower ratings. Those considerations might drive a data-driven prioritisation of the ECSF framework (see Section 5.6).

4.2. Structural enhancement strategies

Experts identified six key enhancements to address the aforementioned ECSF limitations.

E1 — Organising tasks, skills, and knowledge into coherent categories

The current ECSF lists tasks, skills, and knowledge elements without any hierarchical or thematic organisation, which limits clarity and interoperability. Experts agreed that introducing well-defined categories would improve navigability and structural coherence. Several international frameworks offer mature categorisation models that ECSF could leverage:

- REWIRE provides a hierarchical organisation of skills into category and subcategory levels.
- CyBOK offers an established structure of knowledge areas that could serve as a basis for organising ECSF knowledge items.
- NIST CSF groups cybersecurity activities into five high-level functional pillars, which could be used to classify tasks.
- The JRC taxonomy provides contextual dimensions (sectors, applications, technologies) that may enhance ECSF applicability to real-world domains.
- ESCO offers a large repository of skills organised via occupational and transversal categories.

Integrative reviews of competence models identify hierarchical grouping and categorisation as prerequisites for reuse and comparability across frameworks [7].

Using these structures as reference points would improve the interpretability of the ECSF and support alignment with widely adopted international frameworks.

E2 — Defining explicit interdependencies between tasks, skills, and knowledge

A consistent finding from experts was that ECSF lacks explicit links between tasks, skills, and knowledge items. International frameworks such as NICE (and its European adaptation SPARTA) incorporate explicit relationships among these components, demonstrating their value for clarity and operationalisation.

Enhancing ECSF with clearly defined interdependencies would improve its structural coherence, support curriculum design, and enable more effective mapping to occupational profiles.

Such relationships can initially be defined qualitatively through expert judgment, which the present study has shown to be feasible, and may be formalised in future work using ontology-based representations or automated semantic similarity techniques [83–86].

Our findings align with the framework development research, which emphasises that explicit relationships between competence elements improve the operationalisation and replicability of competence frameworks [21,22].

E3 — Integrating competence levels into ECSF skills

ECSF currently assigns proficiency information only at the role level through its mapping to the European e-Competence Framework (e-CF), without defining competence levels at the skill level. Experts highlighted that assigning levels to individual skills would provide a more precise representation of proficiency progression.

Several well-established models offer guidance:

- Bloom's taxonomy provides a hierarchical abstraction of cognitive complexity;
- e-CF and SFIA define graded proficiency for ICT competences;
- NICE associates knowledge and skills statements with varying levels of responsibility across work roles.

Integrating skill-level proficiency tiers would therefore enhance consistency with major frameworks and support curriculum design and assessment processes.

E4 — Introducing seniority levels for ECSF roles

ECSF roles are not differentiated by seniority, despite the fact that the cybersecurity job market commonly recognises junior, mid-level, and senior profiles. Frameworks such as SFIA and e-CF include responsibility or proficiency levels, but do not map them directly to job seniority.

Experts noted that adding a lightweight seniority structure to ECSF roles would align the framework with labour-market conventions and make role definitions more interpretable for employers, educators, and practitioners. A three-level structure (junior, mid-level, senior) is consistent with industry practice and sufficiently expressive without significantly increasing the framework's complexity.

A lightweight seniority layer would align ECSF role descriptions with responsibility structures formalised in professional competence models such as SFIA and e-CF [10,75].

E5 — Addressing emerging cybersecurity domains

The ECSF was last updated in 2022 and does not reflect recent technological evolutions such as AI-driven systems, cloud–edge architectures, IoT ecosystems, and quantum-resistant computing. Experts agreed on the need to extend ECSF coverage to emerging domains.

New domains can be introduced using two approaches:

1. through the introduction of new domain-specific profiles where appropriate;
2. by enriching existing profiles by associating them with domain-specific knowledge areas (e.g., from CyBOK or JRC).

The first approach could cause an explosion of new roles.

Hence, the extension with a domain-specific knowledge area is preferred.

ECSF roles can be extended through knowledge areas using two strategies: specialisation and composition.

Fig. 5 illustrates an example of specialisation for the ECSF penetration testing role specialised in the generative AI domain.

The second strategy is to leverage modularity to combine more ECSF profiles.

The modular composition strategy allows the construction of roles by combining reusable knowledge, skills, and abilities from multiple profiles.

In particular, it is possible to cluster the set of tasks, skills, and knowledge, and use these resulting macro-categories to associate one or more ECSF roles with a specific job offer.

For example, the SecDevOps profile combines capabilities in automated security controls, secure infrastructure configuration, and CI/CD integration with architectural responsibilities.

These responsibilities include secure cloud and microservices design and alignment with standards such as NIST, ISO 27001, and CIS Benchmarks.

This compositional approach more accurately reflects contemporary labour market demands, in which job profiles routinely specify overlapping skills, knowledge domains, and responsibilities across traditionally distinct roles.

Fig. 6 illustrates this concept, showing how a DevSecOps Engineer profile can be dynamically generated by combining the Cybersecurity Implementer and Cybersecurity Architect ECSF profiles.

We discuss the difference between the two strategies in Section 5.

Recent scoping reviews in ICT and emerging technologies emphasise the need for competence models to evolve in response to AI-driven systems, cyber–physical environments, and rapidly changing technology stacks [61].

A modular structure would allow ECSF roles to evolve without generating unnecessary profile proliferation, supporting adaptability to rapidly changing technological landscapes.

E6 — linking ECSF to courses and certifications

Although ENISA provides a mapping between ECSF roles and cybersecurity certifications, no link exists at the level of skills and knowledge items.

Prior work on workforce-aligned cybersecurity curricula demonstrates the value of linking framework elements to educational design and assessment mechanisms [55,57].

Experts agreed that fine-grained alignment with courses and certifications would significantly enhance the framework's usability for educators.

Existing tools, such as the Cybersecurity Curricula Designer, already support partial mappings. However, these are not integrated with ECSF. Future enhancements may involve expert-curated mappings or automated text analysis to derive skill and knowledge associations from course descriptions.

4.3. Alignment between limitations and enhancements

Table 6 summarises this alignment by linking each ECSF limitation with the corresponding enhancement strategy and its expected impact. This mapping demonstrates that the proposed improvements are neither ad hoc nor speculative: they emerge systematically from (i) recurring expert observations and (ii) structural patterns identified across internationally recognised frameworks such as NICE, SFIA, ESCO, CyBOK, NIST CSF, and the JRC taxonomy.

The enhancement strategies, therefore, form a coherent set of design directions that target the core structural weaknesses of the ECSF, namely, lack of organisation, missing interdependencies, absence of competence and seniority levels, limited domain coverage, and insufficient linkage to learning pathways. Each enhancement strengthens a specific structural dimension while maintaining alignment with established global standards, thereby improving clarity, usability, and interoperability of the ECSF.

4.4. Framework-based evidence underpinning the enhancement strategies

During the expert elicitation process, international cybersecurity skills frameworks were used not only as contextual references but as analytical instruments to systematically identify structural gaps in the ECSF. Experts compared ECSF components against corresponding constructs from NICE, CyBOK, ESCO, and the JRC taxonomy (full mapping matrices available in Supplementary Materials S1–S4). These comparisons enabled the assessment of granularity, completeness, domain coverage, and cognitive structure, forming the empirical foundation for the enhancement strategies (E1–E6) presented in Section 4.2.

Three major categories of cross-framework evidence emerged.

1. Granularity mismatches and structural decomposition

Experts identified that ECSF tasks, skills, and knowledge items are often defined at a coarser granularity than in NICE (or the equivalent EU SPARTA framework), which provides significantly more fine-grained statements. This inconsistency affects mappability and interoperability.

Evidence from Supplementary Material S1 reveals two converging structural patterns: (i) limited coverage and (ii) granularity mismatch. First, only 39% of NICE Skills elements have a corresponding ECSF skill. Second, the mapping shows that multiple NICE TKS descriptions often map to a single ECSF skill, indicating a many-to-one compression effect.

This confirms that ECSF collapses several fine-grained competence statements into broader, multi-concept skills.

These two observations jointly reinforce the existence of ECSF limitations L1 (Unstructured tasks, skills, and knowledge) and L2 (Missing interdependency among tasks, skills, and knowledge). They also provide direct empirical support for enhancement strategies E1 (introducing coherent categorisation) and E2 (defining interdependencies).

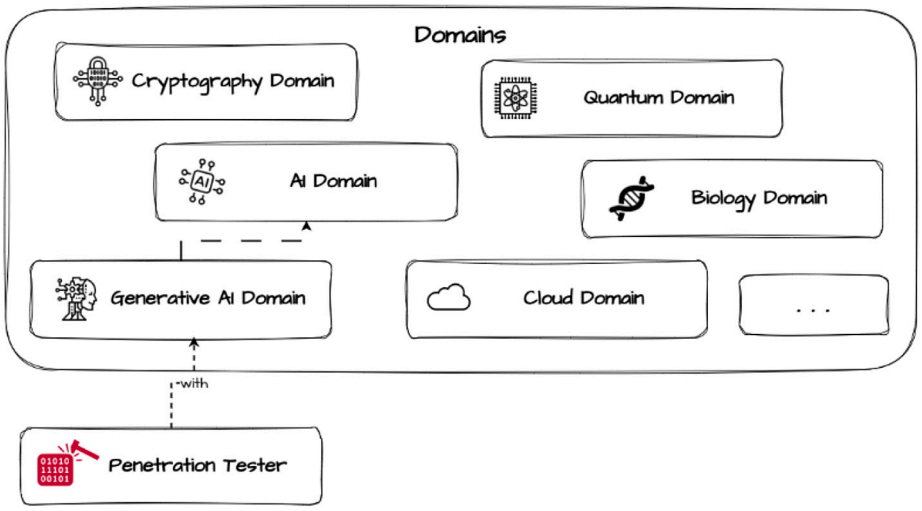


Fig. 5. Extending ECSF profiles using the specialisation strategy.

Table 6
Mapping ECSF structural limitations to corresponding enhancement strategies.

Limitation	Description	Enhancement strategy	Expected impact
L1 — Unstructured tasks, skills, and knowledge	Items are listed without categories or hierarchy, limiting clarity and cross-framework comparability.	**E1 — Organising Tasks, Skills, and Knowledge into Coherent Categories**, using REWIRE skill groups, CyBOK knowledge areas, NIST CSF functions, and JRC contextual dimensions.	Improved interpretability, stronger structural organisation, and better alignment with international models.
L2 — Missing interdependencies among tasks, skills, and knowledge	Relationships between components are absent, making the framework difficult to operationalise.	**E2 — Defining explicit interdependencies between tasks, skills, and knowledge** inspired by NICE/SPARTA links; introduce qualitative expert-defined relations among tasks, skills, and knowledge.	Greater structural coherence supports curriculum design, profile definition, and automated mappings.
L3 — No competence levels for skills	Proficiency levels exist only at the role level via e-CF; skills lack graded complexity.	**E3 — Integrating competence levels into ECSF Skills** grounded in Bloom's taxonomy, SFIA, and e-CF.	Clearer progression pathways; enhanced assessment and training design; consistency with global standards.
L4 — No seniority levels for roles	ECSF roles do not differentiate junior/mid/senior responsibilities, unlike labour-market conventions.	**E4 — Introducing seniority levels for ECSF Roles** (junior, mid, senior).	Better alignment with job-market practice; easier interpretation for employers and educators.
L5 — Missing coverage of emerging domains	ECSF (2022) does not reflect recent technological evolutions (AI, IoT, cloud–edge, automation, quantum).	**E5 — Addressing emerging cybersecurity domains**, through specialisation and composition strategies.	Future-proofing, adaptability to new technological domains, and manageable framework complexity.
L6 — Limited linkage to training pathways and certifications	Mappings exist only at the role level; skills and knowledge are not connected to learning offerings.	**E6 — Linking ECSF to courses and certifications** through expert-curated mappings and future NLP-assisted extraction.	Enhanced educator adoption; clearer upskilling pathways; integration with certification ecosystems.

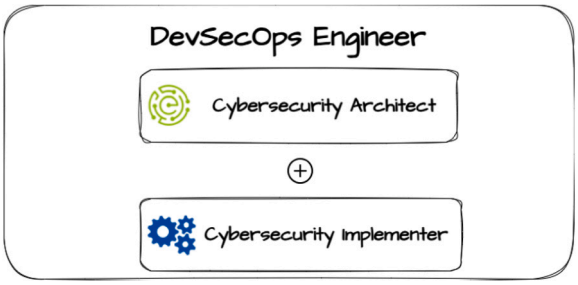


Fig. 6. Example of dynamic profile generation combining the composition strategy.

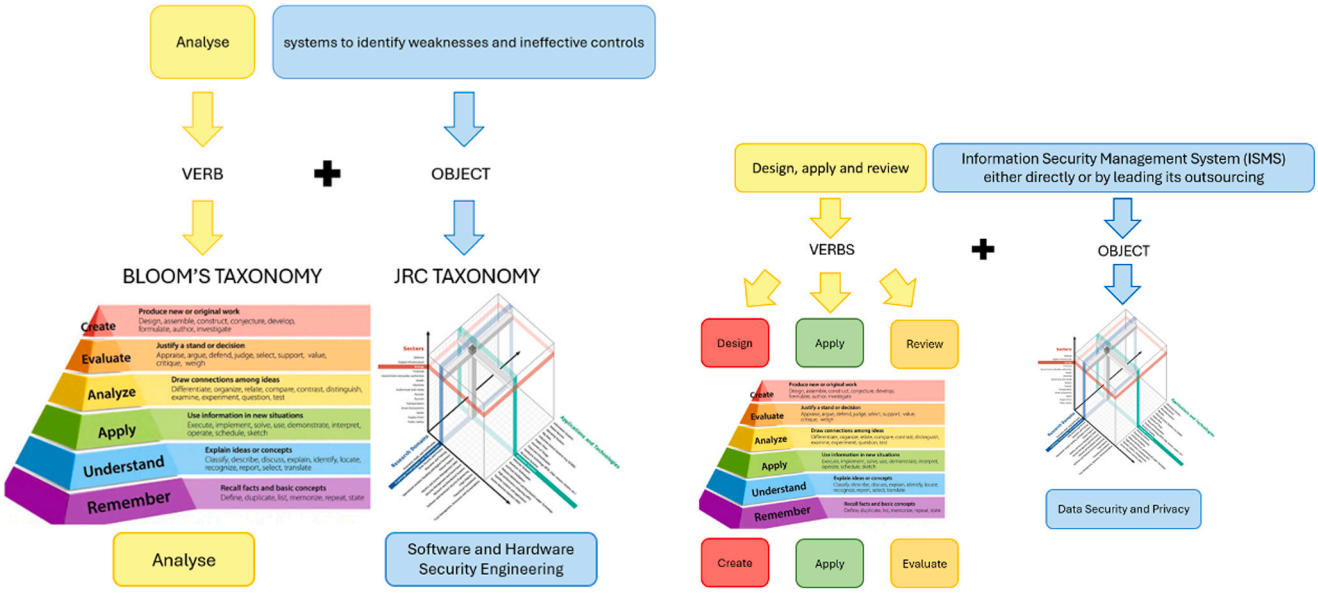
The aforementioned considerations also pertain to tasks and knowledge items.

NICE typically decomposes work roles into highly granular KSAT (Knowledge–Skill–Ability–Task) elements, while ECSF aggregates broader activities under a limited set of skills.

This mismatch reveals a significant coverage gap: many NICE skills lack corresponding ECSF equivalents, while ECSF skills often span the semantic space of multiple NICE KSATs.

Additionally, evidence from ESCO–ECSF mapping (Supplementary Material S3) shows that each ECSF skill typically corresponds to multiple ESCO skills.

Therefore, ESCO also expresses competences at a much finer level of granularity, using narrowly scoped skill descriptors that can be combined into occupational profiles. This implies that ECSF skills operate at a broader abstraction level and lack intermediate layers of detail present in ESCO.



(a) Example mapping of an ECSF skill to Bloom's cognitive levels and JRC domains

(b) Mapping a complex ECSF skill across Bloom levels ("Design-Apply-Review")

Fig. 7. Overview of ECSF–Bloom mappings.

Also this mapping highlights the structural limitations lack of decomposition (L1) and inconsistent granularity (L2), and directly motivate the need for structured categorisation of ECSF components (E1) and for the explicit articulation of task–skill–knowledge interdependencies (E2).

2. Knowledge-domain organisation and hierarchical knowledge modelling

Mapping ECSF knowledge items to CyBOK (Supplementary Material S2) highlighted that ECSF expresses knowledge as a flat, unordered list, whereas CyBOK organises knowledge into 21 coherent domains and subdomains. This comparison revealed patterns of:

- fragmented knowledge clusters;
- missing domain-specific grouping;
- partial coverage in certain areas (e.g., adversarial behaviours, hardware security).

These findings support the introduction of thematic knowledge organisation and modular domain extensions (E1, E5).

3. Competence-level and cognitive-structure analyses (Bloom's + JRC)

To evaluate the implicit cognitive complexity of ECSF skills, experts decomposed ECSF skill statements using a "verb + object" pattern and mapped them to Bloom's taxonomy. Similarly, the JRC taxonomy was used to identify the implicit knowledge domains associated with each skill object.

This analysis revealed:

- heterogeneous cognitive levels within the same skill;
- missing explicit competence levels;
- missing linkage between knowledge and skills.

These findings provided the empirical basis for Enhancement Strategy E3 (competence levels) and part of E5 (domain extensions).

Figs. 7(a) and 7(b) show two examples of mappings generated by experts.

These figures were produced directly during the "Discuss" and "Estimate" phases and demonstrate the heterogeneous cognitive structure of several ECSF skills.

The cross-framework analyses conducted by the expert groups provided direct empirical evidence for each Enhancement Strategy (E1–E6). They revealed:

- structural misalignments in granularity and decomposition;
- absence of knowledge-domain organisation;
- implicit yet inconsistent cognitive and competence levels;
- gaps in coverage of emerging domains.

These findings justify the enhancement directions proposed and provide a reproducible analytical basis for strengthening ECSF structure in line with international best practices.

5. Discussion

This section discusses the theoretical and practical implications of our findings, along with their limitations.

5.1. Theoretical implications

The findings of this study contribute to the theoretical understanding of cybersecurity skills frameworks in several ways.

First, structural expressiveness emerges as a key determinant of the usefulness and interoperability of skills models (see Section 2.5.1).

These findings also reflect a design trade-off rooted in the underlying philosophy and governance of the analysed frameworks (Section 2.1). ECSF prioritises semantic accessibility and stakeholder alignment under a public institutional governance model, whereas NICE and SFIA embed richer structural mechanisms that improve machine-actionability and career progression modelling. Our enhancement strategies are therefore framed as incremental additions that preserve ECSF human-oriented design while enabling selective interoperability where needed.

Prior comparative studies show that frameworks differ substantially in how they organise tasks, skills, and knowledge, with international models often employing intermediate abstraction layers or hierarchical decomposition schemes [10,27]. Our analysis confirms these observations. Whereas the ECSF adopts a largely flat representation, frameworks such as NICE and SFIA introduce intermediate

structural components that enable clearer mappings, more expressive role definitions, and improved interoperability. This finding aligns with established research in competence modelling, which argues that well-formed competence hierarchies enhance both interpretability and operationalisation [24–26].

Beyond technical interoperability, the structural properties of competence frameworks also shape the learning environments they implicitly support. Prior work in cybersecurity education shows that features such as task decomposition, progression pathways, and feedback mechanisms influence learner motivation, self-efficacy, and performance across genders and domains [87].

Although the present study does not evaluate educational interventions directly, our findings suggest that structural expressiveness in ECSF might indirectly affect inclusiveness and learning outcomes. In particular, a framework that supports transparent progression and modular task design may reduce entry barriers, facilitate differentiated learning paths, and better accommodate heterogeneous learner profiles.

From this perspective, structural refinement is not only a technical concern but also a lever for improving the social impact of cybersecurity workforce frameworks.

Second, applying cognitive modelling techniques based on Bloom's taxonomy (see Section 2.5.2), reveals that many ECSF skill statements implicitly embed multiple cognitive operations. This supports previous work in digital learning and curriculum theory, which emphasises that competences should be articulated at a consistent level of cognitive granularity to support assessment and instructional design [28–30]. Studies on cybersecurity education similarly highlight misalignment between skill statements and the cognitive levels required for practice [88,89]. Our results extend this line of research by demonstrating that cognitive heterogeneity is not only an educational issue but also a structural challenge in competence frameworks. However, these findings should be interpreted with caution, as professional competence does not depend solely on cognitive complexity, but also on responsibility, contextual judgement, and practice-based capability [10,90–92].

Third, the cross-framework comparison underscores the importance of modular knowledge modelling, consistent with the structural principles outlined in Section 2.5.1. The mapping to CyBOK illustrates that cybersecurity knowledge is most effectively represented through structured domains and well-defined thematic clusters [71]. This observation aligns with theories that advocate modular representations of knowledge to support curriculum alignment and maintain conceptual coherence [14,72]. Our results show that such modularity is not merely beneficial for educational purposes but also crucial for maintaining internal consistency between tasks, skills, and knowledge within a framework.

Taken together, these insights reinforce and extend theoretical discussions on the structure of cybersecurity competences.

They point toward the need for hierarchical decomposition, cognitively coherent skill formulation, and modular knowledge organisation, offering a conceptual foundation for the development of unified and interoperable cybersecurity skills models.

5.2. Practical implications

The study also offers several practical implications for stakeholders in education, industry, and policy.

From an educational perspective, the introduction of skill-level descriptors and structured knowledge domains can support the design of coherent learning pathways. Educational institutions may use the enhanced structure to align courses, microcredentials, and examinations with specific cybersecurity competences.

For industry and workforce development, the proposed enhancements allow for clearer job profiling and talent management. Employers may benefit from introducing seniority levels within roles, which clarify expectations for junior, mid-level, and senior professionals. The explicit mapping between tasks, skills, and knowledge also enables more accurate identification of skill gaps in organisational contexts.

At the policy level, the results offer actionable guidance for the future evolution of the ECSF and related European initiatives. The enhancement strategies provide a roadmap that can be integrated into future revisions of the ECSF without compromising its simplicity or scope. More importantly, the mapping strategies strengthen interoperability between European and international frameworks, thereby supporting worker mobility and the harmonisation of curricula across Member States.

Beyond technical structure, long-term uptake of curricular and workforce frameworks is shaped by policy diffusion dynamics, institutional incentives, and shared terminology across stakeholders. Evidence from the national-scale adoption of a Computer Science (CS) education framework shows that diffusion depends not only on the internal design of the framework, but also on alignment with institutional constraints, teacher capacity, and the negotiation of stable concepts across policy and practice [93].

The effectiveness of competence frameworks depends more on institutional embedding and market adoption than on formal structure alone [32–34]. European Cybersecurity Skills Framework alignment with courses and certifications therefore cannot be reduced to a technical mapping problem. Certification strategies, market competition among credential providers, regulatory environments, and employer recognition patterns shape the alignment process.

Broader educational and labour market research supports this interpretation. The practical relevance of skills frameworks derives from their operationalisation within curricula, assessment systems, and credentialing practices [39–41]. The expert elicitation protocol proposed in this study integrates perspectives from diverse stakeholders. This integration enables the ECSF refinement that remains formally coherent and institutionally viable while aligning with workforce realities.

In this respect, our structural enhancement strategies (E1–E6) should be interpreted as enablers of adoption, rather than as sufficient conditions, by improving both interoperability and interpretability.

However, sustained integration of ECSF into educational pathways will also require governance mechanisms, incentives for providers, and continuous alignment of terminology across the European education–training–labour ecosystem.

This also raises an additional requirement: ensuring governance and resourcing mechanisms that support continuous maintenance and periodic updating of competence and curricular frameworks over time.

During expert elicitation, several participants emphasised that high granularity, such as that found in NICE, can hinder practical adoption, especially among small and medium-sized enterprises (SMEs).

While granular frameworks enable higher precision in role decomposition and competence assessment, their operationalisation requires significant expertise, training, and organisational maturity. This observation is consistent with the literature, which shows that SMEs often struggle to adopt complex or highly structured cybersecurity models and instead benefit from simplified, actionable frameworks.

Recent studies confirm this tendency. For example, the NERO ecosystem explicitly highlights the need for lightweight, easy-to-adopt cybersecurity structures for SMEs, arguing that complexity can be a barrier to awareness, training, and resilience programmes [94]. Similarly, research on workforce development frameworks shows that overspecified competence models can reduce adoption and interoperability in organisational settings with limited cybersecurity expertise [53,56,58].

Therefore, the NICE–ECSF comparison does not indicate a flaw in ECSF per se: rather, it illustrates the design trade-off between completeness and precision (NICE) on one hand and simplicity and organisational usability (ECSF) on the other.

This trade-off underpins the proposed enhancement strategies, which aim to introduce more structure into ECSF without compromising its practical accessibility. This perspective is consistent with

empirical observations in EU innovation projects, where ECSF effectiveness is grounded in human-centred workflows rather than technological automation [5].

However, an important challenge must be addressed. The rapid emergence of new cybersecurity domains [95,96] requires the development of competence frameworks capable of supporting adaptable, modular, and partially automated updates [97,98].

Structural enhancement can support this evolution by simplifying interoperability across ECSF knowledge, skills, and tasks and by facilitating alignment with related Knowledge, Skills, and Abilities (KSA) frameworks.

Recent empirical studies based on labour-market signals complement the framework-to-framework evidence used in this work. For instance, job-posting analyses show that emerging domains such as AI-related competences (e.g., ML, NLP, predictive analytics) increasingly co-occur with multiple cybersecurity functions (e.g., threat intelligence, anomaly detection, incident response), rather than mapping neatly to isolated roles [99]. This data-driven evidence supports the need for extension mechanisms to properly cover cross-cutting competences present in the market. A strategy could be the adoption of the compositional roles' construction proposed by experts ().

5.3. Limitations

Although the study provides meaningful insights, several limitations must be acknowledged.

5.3.1. Expert group size

The expert elicitation involved ten participants. While this number aligns with established guidelines for structured expert judgement [63,100], a larger group might have provided additional perspectives. Future studies could benefit from broader participation, particularly from underrepresented sectors.

5.3.2. Geographic focus

Most experts had experience within European educational and industrial environments. As a result, interpretations may reflect region-specific assumptions. Additionally, the frameworks analysed were primarily European or international in scope. A notably absent framework is the Saudi Cybersecurity Workforce Framework (SCyWF), which has been studied in several works [101,102]. This geographic focus may limit the applicability of findings to non-European contexts. The decision to focus on European frameworks was motivated by the goal of developing a unified European cybersecurity skills framework that aligns with international standards while addressing region-specific needs. Including more non-European stakeholders in future studies might enhance the generalisability of the findings.

5.3.3. Limited coverage of social and adoption dimensions

The present analysis focused on the structural and representational properties of competence frameworks assessed through expert-based comparative evaluation. Therefore, we did not assess ethical alignment, gender inclusiveness, SME accessibility, or socio-economic impact, which are typically examined through educational, organisational, and policy lenses [87].

This limitation reflects a more general gap in current cybersecurity competence frameworks, which primarily emphasise technical and professional aspects while only marginally addressing their societal implications [103,104].

Additionally, our study does not model the long-term policy and institutional dynamics that shape adoption in education systems (e.g., diffusion mechanisms, organisational incentives, educator capacity, and terminology stabilisation). Prior evidence from large-scale diffusion of curricular frameworks suggests that these factors substantially affect whether a framework becomes embedded in formal curricula and practice [93].

Regarding courses and certifications, experts proposed a fine-grained mapping to the ECSF items to address gaps in the current framework. Although this approach is supported by the literature [105], other factors, such as competition among providers, reputational dynamics, and positioning strategies, may affect its feasibility [39,41].

Future research could complement this work by conducting systematic mapping studies [106] or systematic literature reviews [107] focused on these dimensions, thereby extending the analytical scope beyond structural expressiveness to the social and educational impact of competence frameworks.

5.3.4. Lack of quantitative validation

The study relied on qualitative severity assessments rather than numerical aggregation. Although this approach is consistent with structured expert elicitation protocols, quantitative validation through statistical techniques or automated text analysis could complement and strengthen the results.

5.3.5. Framework selection

In this study, we opted to analyse the most relevant cybersecurity skills and knowledge frameworks from grey literature, as the most pertinent works for developing a unified EU cybersecurity framework originate from industry-led or EU-funded initiatives rather than from peer-reviewed publications. Grey literature consists of research material produced by government, academics, business, and industry, and not controlled by commercial publishers. Since this material is not subject to peer review or quality checks, proper evaluation is essential. To address this issue, we followed the approach of [3], in which identified frameworks were selected using the systematic literature review provided by the Cybersecpro initiative [6].

Despite conducting a preliminary literature search before this study, only a few works have explored this problem (Section 2). A more in-depth exploration of recent research could yield additional solutions to the problem we addressed. In future work, we aim to provide a comprehensive systematic map review to verify the evidence found in this study.

5.3.6. Potential expert bias

Expert elicitation is inherently subject to individual judgment. We addressed this by involving two separate expert groups for validation. Additionally, multiple rounds of discussion and semi-structured outputs were used to mitigate bias. Nevertheless, residual subjectivity cannot be fully excluded.

5.3.7. Lack of field validation

The enhancement strategies have not yet been implemented or tested in operational settings. Future work should examine the practical adoption of the proposed modifications, for instance, through pilot implementations in curricula, certification pathways, or organisational workforce programmes.

5.4. Comparison with related works

As observed in Section 2, the most similar work to ours is that of [3], which compares ECSF with NICE and SFIA, identifies some limitations, and proposes improvements. We already noted that our work differs from [3] in that it explores the structural properties of ECSF and defines limitations and enhancements based on cross-framework analysis. Consequently, our findings emphasise conceptual inconsistencies that were not highlighted in prior work.

Our study yields divergent results in some aspects. While [3] classifies "Standardised Skill Definition" and "Support for Career Pathways" as strengths of ECSF, the structural decomposition in our study reveals that ECSF skill definition lacks cognitive uniformity (L2), competence levels (L3), and consistent role granularity. This suggests that when

analysing structural properties, the ECSF exhibits limitations that may not be apparent in higher-level comparisons.

Regarding knowledge coverage, our study identifies gaps in ECSF similar to those identified by [3]. However, our study proposes concrete strategies to address these gaps through knowledge representation (E1) and domain-specific extensions (E5) grounded in CyBOK and the JRC taxonomy.

Our results are also consistent with broader evidence on the fragmentation and heterogeneity of cybersecurity competence models reported in comparative and mapping studies, which highlight recurring misalignments in granularity and the absence of shared meta-models for interoperability [51–53]. However, other research lines emphasise complementary gaps such as curriculum–workforce misalignment and underrepresentation of non-technical competences [55,56,58]. Our structural analysis does not directly measure these aspects, as they might be covered using other methodologies (Section 5.3.3). Experts provided considerations on the most relevant limitations, which might lead to different prioritisation choices in the evolution of the framework. Results suggest addressing structural expressiveness first, by confirming the relevance of our structural analysis. Future works might evaluate the alignment of education and the coverage of socio-technical competence.

5.5. Considerations on the experts' findings

Several considerations can be made on the experts' findings. We analyse relevant comments from experts, the challenges of using Bloom's taxonomy to define competence levels, and the strategies proposed to address emerging domains.

5.5.1. Relevant comments from experts

Despite identifying limitations and potential enhancements, experts provided relevant considerations for extending the ECSF.

A first comment concerns the positive consequences of adding identifiers to the ECSF items.

Once these are properly identified with codes, it would be possible to create matrices that would simplify training and hiring planning at the company level. With well-structured tasks, it would be possible to simplify the development of Responsible, Accountable, Consulted, and Informed (RACI) matrices [108], thereby improving internal processes and workforce management.

A second relevant consideration concerns the types of ECSF roles. The ECSF is mainly based on technical roles, thereby underrepresenting categories such as governance, legal responsibilities, and risk management. The multidisciplinary nature of cybersecurity also requires roles in IT policy, digital ethics, and IT law [109]. The reorganisation of tasks, skills, and knowledge (E1 and E2) might help to better structure the ECSF items and simplify interoperability with governance laws and regulations.

A third expert suggested making the framework open-source. The expert had extensive experience in software development, where the open-source community contributes to projects using cloud-based development platforms that provide version control, maintenance, and issue tracking [110]. Open discussions among security experts may be held to modify the ECSF and provide relevant contributions. The suggestion is valuable, but should be carefully investigated (Section 5.6).

5.5.2. On the Bloom's taxonomy to define competence levels

To assign competence levels to the ECSF skills, experts suggested adopting Bloom's taxonomy, an educational framework for classifying cognitive learning objectives.

Although the framework has already been adapted to support workforce skill development in cybersecurity and IT [111,112], this approach might face two relevant challenges.

First, applying the taxonomy directly might not capture the complex, context-dependent, and heterogeneous nature of workforce skills [113].

Second, the hierarchical and linear progression may not fully represent the cyclic and dynamic nature of competence acquisition in workplace settings [114]. The Bloom's taxonomy emphasises higher-order thinking skills like analysis and creation, while workforce skills commonly demand transferrable skills, problem-solving in unfamiliar contexts, and collaboration. Those are only indirectly addressed in the original taxonomy [91,92].

To address these challenges, some researchers have investigated integrating other models, such as Simpson & Harrow's psychomotor taxonomy [113,115], to better capture the full range of hands-on and adaptive skills needed in real-world contexts.

All these considerations should be carefully analysed in future works aimed at extending the ECSF.

5.5.3. On the coverage of emerging domains

Experts suggested two approaches to cover emerging domains: specialisation and modularity.

The first technique has the advantage that some specialisation can be easily integrated by relating ECSF roles to specific knowledge areas. For instance, an "AI penetration tester" is an ECSF penetration tester specialised in the Artificial Intelligence domain, but has a significant disadvantage: it introduces rigid hierarchical dependencies that reduce flexibility and limit evolvability.

In fact, hierarchical extensions tightly couple a specialised role to its parent profile, thereby restricting the integration of interdisciplinary knowledge, skills, and abilities without redefining the overall role structure.

This limitation reflects a broader challenge in hierarchical system models, where tightly coupled structures hinder adaptability and reuse [116,117].

This is particularly challenging in emerging domains that cut across multiple roles and skills, by complicating the specialisation.

The modular composition represents a well-established design principle in systems engineering and organisational theory. This principle supports aggregating loosely coupled components to manage complexity and enable evolution [118].

In competence and role modelling, modular approaches allow capabilities to be recombined across contexts. This property better reflects the dynamic and multidimensional nature of professional roles [90,99].

Although software engineering often contrasts inheritance and composition, this distinction represents a specific instance of the broader modularity principle [119].

However, a proper encapsulation of these domains remains an open challenge. The heterogeneity of workforce competences and responsibilities is strongly influenced by the rapid evolution of industries and domains. A potential solution might be to construct hybrid profiles by combining skills and knowledge from different ECSF roles. Additionally, it could be possible to assign a "weight" to the coverage level of each skill and knowledge, using an approach similar to that in fuzzy logic (not exactly true or false, but a truth or falseness probability) [120].

Other studies successfully leveraged the approach to manage and assess role profiles using Knowledge, Skills, and Abilities (KSA) frameworks by addressing the inherent uncertainty and vagueness in human resource evaluations [121,122].

5.6. Towards a new design of the ECSF

Our work provides relevant findings to drive a new design of the ECSF framework. Section 2.2 discussed the ECSF design philosophy, which prioritises human usability and organisational accessibility over structural expressiveness and machine-actionability. Our study does not undermine the ECSF design philosophy, but highlights the opportunity to complement its human usability with enhanced structural formalisation.

Our study is positioned within this design space. We preserve the ECSF role as a common human language while introducing structural enhancements that enable automation, interoperability, and analytical scalability, without compromising accessibility or interpretability for human stakeholders.

Although our primary goal was not to redesign the ECSF, the expert elicitation process yielded several relevant considerations for its future evolution. A potential redesign is illustrated in Figure 8 (see MMC S1). This design includes all the enhancement strategies found by the experts. Tasks, skills, and knowledge items might be grouped by categories and relate to multiple ECSF roles (E1 and E2). Each skill would require a competence level (E3), and for each ECSF role multiple seniority levels could be defined (E4). Finally, emerging domains are covered through modular extensions and specialisations (E5), and skills and knowledge items are linked to courses and certifications through generic "learning units" (E6).

This design represents a preliminary conceptual model that could guide future ECSF revisions.

Note that, although this redesign would enhance the completeness of the framework, it might affect its simplicity. In fact, while the current ECSF has only four entities (role, knowledge, skill, and task), our proposal would include 14 entities.

A trade-off could be achieved by first addressing the most critical limitations.

Section 4.1.1 shows the distribution of scores on each limitation and enhancement provided by experts.

These convergence patterns strengthen the validity of the proposed redesign by demonstrating that the identified limitations are not merely conceptual but are empirically recognised by domain experts. Additionally, the differential weighting across limitations shows that not all design issues have the same structural impact. Therefore, it would be possible to follow a staged, prioritised redesign strategy for the ECSF that balances simplicity and completeness.

Another consideration concerns the factors that affect the impact of our work. Although our work primarily analysed structural artifacts, the real-world impact depends strongly on human factors.

In general, the ECSF effectiveness depends not only on its structure but also on clarity, readability, ease of interpretation, and human support for iterative enhancement [123].

All these aspects should be carefully considered in the future redesign of the ECSF. This puts the ECSF evolution in a human-centred perspective. As discussed in Section 5.5.1, a relevant suggestion from one of the experts is to make the framework open.

This direction could be valuable, but it should address political issues related to the European governance of the framework, which is maintained by ENISA [124,125]. Eventually, ENISA could publicly host the framework as an open-source project and maintain governance through a well-structured review process for community-suggested changes (in software development, this is achieved using the pull request mechanism [126]).

6. Conclusions

This study examined the structural properties of the European Cybersecurity Skills Framework and proposed a set of evidence-based enhancements grounded in expert elicitation and cross-framework comparison. By analysing the ECSF alongside internationally recognised models such as NICE, SFIA, CyBOK, ESCO, and the JRC taxonomy, the work has identified core structural limitations and formulated design directions to strengthen clarity, interoperability, and practical applicability.

The results indicate that introducing structured categorisation, explicit interdependencies, competence levels, seniority distinctions, and domain-specific extensions can substantially improve the expressiveness and usability of the ECSF. Furthermore, the cross-framework evidence presented in this study provides a robust foundation for these enhancements and demonstrates that they are consistent with mechanisms already adopted in mature cybersecurity competence systems.

Several avenues for future research remain open. One promising direction involves the development of a generic ontology capable of integrating the frameworks analysed in this study. Such an ontology would enable the creation of a comprehensive and interoperable dataset of skills, knowledge, and tasks, thereby supporting automated mappings and advanced analytical tools. We plan to start by formalising the redesign proposed in Section 5.6 using ontology engineering techniques [127,128].

Another opportunity for future work is to apply clustering and semantic-similarity techniques to investigate the relationships between ECSF roles and real-world job profiles. Insights derived from these analyses could support the alignment of ECSF with labour-market requirements and facilitate its adoption by organisations, training providers, and certification bodies.

Finally, linking ECSF skills and knowledge items to educational programmes and professional certifications represents a key step towards enhancing the framework's relevance for workforce development. Exploring this alignment through expert curation and AI-driven text analysis would further advance the practical usability of the ECSF within the wider cybersecurity education ecosystem.

Overall, it is hoped that the contributions of this study will inform ongoing discussions on the evolution of cybersecurity competence frameworks and will stimulate further research aimed at strengthening the coherence and interoperability of cybersecurity skills initiatives in Europe.

CRediT authorship contribution statement

Gaetano Perrone: Writing – original draft, Investigation, Conceptualization. **Nicola d'Ambrosio:** Writing – original draft. **Roberto D'Isanto:** Writing – original draft. **Massimiliano Rak:** Project administration. **Lavinia Russo:** Writing – original draft. **Simon Pietro Romano:** Writing – review & editing, Supervision, Project administration, Funding acquisition, Conceptualization. **Mario Varlese:** Writing – original draft, Investigation.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the authors used Grammarly and Copilot to refine the academic writing style and improve the clarity and readability of the manuscript text. `gpt-4o-mini` was used to generate the mapping between ECSF and NICE, which is provided in the supplementary material. Note that providing a comprehensive and fully validated cross-framework mapping was beyond the scope of this study. The mapping was designed to help experts obtain an overview of cross-interoperability issues across frameworks. These comparisons allowed them to assess granularity, completeness, domain coverage, and cognitive structure, forming the empirical basis for the enhancement strategies proposed in this study.

All AI-generated content was reviewed and edited to ensure accuracy and alignment with the research findings.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was carried out within the framework of the AKADIMOS ("Governance and Operational Support for the Development of the European Cybersecurity Skills Academy" - Digital Europe Programme DIGITAL-2023-SKILLS-05-CYBERACADEMY) project, funded under Grant Agreement N.101189712, and supported by the European Health and Digital Executive Agency (HaDEA).

This work was also supported by the "IDA — Information Disorder Awareness" Project funded by the European Union, Next Generation EU, within the SERICS Program through the MUR National Recovery and Resilience Plan under Grant PE00000014.

Appendix A. Supplementary data

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.array.2026.100728.

Data availability

The data supporting the findings of this study are openly available in the Zenodo persistent repository at https://zenodo.org/records/18312770 (DOI: 10.5281/zenodo.18312770). The repository contains the following supplementary materials: (S1) NICE–ECSF Mapping Matrix, (S2) CyBOK–ECSF Knowledge Mapping, (S3) ESCO-ECSF Mapping, and (S4) REWIRE–ECSF Skill Category Mapping. All materials are licensed under CC BY 4.0. Raw interview data and expert identities remain confidential to protect participant anonymity and are stored in an encrypted repository accessible only to the research team.

References

[1] Theocharidou M, Lella I, Naydenov R, Malatras A, Enisa. ENISA threat landscape: Finance sector. 2024, http://dx.doi.org/10.2824/5410466, URL: https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf. 2023 to June 2024.

[2] European Union Agency for Cybersecurity (ENISA). European cybersecurity skills framework (ECSF). 2024, URL: https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.

[3] Almeida F. Comparative analysis of EU-based cybersecurity skills frameworks. Comput Secur 2025;151. http://dx.doi.org/10.1016/j.cose.2025.104329.

[4] Douligeris C. Cybersecurity awareness and training: The cybersecpro and nero approaches. Proceedings of the 2024 European interdisciplinary cybersecurity conference. New York, NY, USA: Association for Computing Machinery; 2024, p. 225. http://dx.doi.org/10.1145/3655693.3661830.

[5] Rathod P, Polemi N, Lehto M, Kioskli K, Wessels J, Lugo R. Leveraging the European cybersecurity skills framework(ecsf) in eu innovation projects: Workforce development through skilling, upskilling, and reskilling. In: 2024 IEEE global engineering education conference. EDUCON, 2024, p. 1–9. http://dx.doi.org/10.1109/EDUCON60312.2024.10578846.

[6] CyberSecPro Project. Cybersecpro - cybersecurity skills professionalization. 2025, https://www.cybersecpro-project.eu/. [Accessed 18 November 2025].

[7] Mikhridinova N, Wolff C, Van Petegem W. Taxonomy of competence models based on an integrative literature review. Educ Inf Technol 2024;29:16997–7033. http://dx.doi.org/10.1007/s10639-024-12463-y.

[8] Calhau R, Almeida J, Kokkula S, Guizzardi G. Modeling competences in enterprise architecture: from knowledge, skills, and attitudes to organizational capabilities. Softw Syst Model 2024;23:559–98. http://dx.doi.org/10.1007/s10270-024-01151-7.

[9] Rodrigues M, Fernández-Macías E, Sostero M. A unified conceptual framework of tasks, skills and competences. (JRC121897). 2021.

[10] SFIA Foundation. SFIA 9: All skills A–Z. 2024, URL: https://sfia-online,org/en/sfia-9/all-skills-a-z/?collectionfilter=1.

[11] Prickett T, Crick T, Davenport JH, Bowers DS, Hayes A, Irons A. Embedding technical, personal and professional competencies in computing degree programmes. In: Proceedings of the 2024 on innovation and technology in computer science education, vol. 1, ACM; 2024, p. 346–52. http://dx.doi.org/10.1145/3649217.3653578.

[12] European Commission, ESCO. European e-competence framework (e-cf). 2025, https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf. Maintained by CEN/TC-428 ICT Professionalism and Digital Competences. [Accessed 3 February 2026].

[13] National Institute of Standards and Technology. Nice workforce framework for cybersecurity (nice framework). 2025, https://niccs.cisa.gov/tools/nice-framework. [Accessed 07 June 2025].

[14] CyBOK. The cyber security body of knowledge. 2024, https://www.cybok.org.

[15] DGEmployment, Social Affairs and Inclusion of the European Commission. About ESCO: European skills, competences, qualifications and occupations. 2024, https://esco.ec.europa.eu/en/about-esco. Last updated 15 May 2024. [Accessed 12 June 2025].

[16] Joint Task Force. Security and privacy controls for information systems and organizations. Technical Report 800-53 Revision 5, National Institute of Standards and Technology; 2020, http://dx.doi.org/10.6028/NIST.SP.800-53r5.

[17] Policies E, Nijz L, Wit S, De Batenburg R, Francke A. International comparison of professional competency frameworks for advanced practice nurses. Eur J Pub Health 2023;33. http://dx.doi.org/10.1093/eurpub/ckad160.744.

[18] Sidhu N, Allen K, Civil N, Johnstone C, Wong M, Taylor J, Gough K, Hennessy M. Competency domains of educators in medical, nursing, and health sciences education: An integrative review. Med Teach 2022;45:219–28. http://dx.doi.org/10.1080/0142159X.2022.2126758.

[19] Wit R, De Veer A, Batenburg R, Francke A. International comparison of professional competency frameworks for nurses: a document analysis. BMC Nurs 2023;22. http://dx.doi.org/10.1186/s12912-023-01514-3.

[20] Van Der Aa J, Aabakke A, Andersen B, Settnes A, Hornnes P, Teunissen P, Goverde A, Scheele F. From prescription to guidance: a European framework for generic competencies. Adv Health Sci Educ 2019;25:173–87. http://dx.doi.org/10.1007/s10459-019-09910-8.

[21] Ali M, Qureshi S, Memon M, Mari S, Ramzan M. Competency framework development for effective human resource management. SAGE Open 2021;11. http://dx.doi.org/10.1177/21582440211006124.

[22] Batt A, Williams B, Rich J, Tavares W. A six-step model for developing competency frameworks in the healthcare professions. Front Med 2021;8. http://dx.doi.org/10.3389/fmed.2021.789828.

[23] Caena F, Redecker C. Aligning teacher competence frameworks to 21st century challenges: The case for digcompedu. Eur J Educ 2019. http://dx.doi.org/10.1111/ejed.12345.

[24] Zafeiris A, Vicsek T. Group performance is maximized by hierarchical competence distribution. Nat Commun 2013;4. http://dx.doi.org/10.1038/ncomms3484.

[25] Khan KS, Coomarasamy A. A hierarchy of effective teaching and learning to acquire competence in evidenced-based medicine. BMC Med Educ 2006;6. http://dx.doi.org/10.1186/1472-6920-6-59.

[26] Ramanauskaitė S, Slotkienė A. Hierarchy-based competency structure and its application in e-evaluation. Appl Sci 2019;9:3478. http://dx.doi.org/10.3390/app9173478, URL: https://www.mdpi.com/2076-3417/9/17/3478.

[27] Cybersecurity, Agency, IS. NICE framework mapping tool. 2025, https://niccs.cisa.gov/workforce-development/nice-framework-mapping-tool.

[28] Bloom BS, Krathwohl DR, Masia BB. Taxonomy of educational objectives: The classification of educational goals. New York: Longmans, Green; 1956.

[29] Krathwohl DR. A revision of bloom's taxonomy: An overview. Theory Into Pr 2002;41:212–8. http://dx.doi.org/10.1207/s15430421tip4104_2.

[30] Biggs J. Enhancing teaching through constructive alignment. High Educ 1996;32:347–64. http://dx.doi.org/10.1007/bf00138871.

[31] Coombe L, Severinsen C, Robinson P. Mapping competency frameworks: implications for public health curricula design. Aust N Z J Public Health 2022;46. http://dx.doi.org/10.1111/1753-6405.13253.

[32] Grimaud O, Foucrier M, Czabanowska K, et al. Mapping competency in public health training – experience of the Europubhealth consortium. BMC Med Educ 2024;24. http://dx.doi.org/10.1186/s12909-023-05010-9.

[33] Carraccio C, Englander R, Gilhooly J, et al. Building a framework of entrustable professional activities, supported by competencies and milestones. Acad Med 2017;92:324–30. http://dx.doi.org/10.1097/ACM.0000000000001141.

[34] Vargas H, Heradio R, Farías G, Lei Z, De La Torre L. A pragmatic framework for assessing learning outcomes in competency-based courses. IEEE Trans Educ 2024;67:224–33. http://dx.doi.org/10.1109/TE.2023.3347273.

[35] Zheng L, Ge D. Cultivating key disciplinary competencies among university students. PLoS ONE 2025;20. http://dx.doi.org/10.1371/journal.pone.0318561.

[36] Stefani A, Vassiliadis B. A certification framework for e-commerce digital competencies. Open J Appl Sci 2023. http://dx.doi.org/10.4236/ojapps.2023.135061.

[37] Ngambeki I, Rogers M, Bates S, Piper M. Curricular improvement through course mapping: An application of the nice framework. In: 2021 ASEE virtual annual conference content access proceedings. ASEE Conferences, http://dx.doi.org/10.18260/1-2–36889.

[38] Carracedo F, Soler A, Martin C, Lopez D, Ageno A, Cabre J, Garcia J, Aranda J, Gibert K. Competency maps: an effective model to integrate professional competencies across a stem curriculum. J Sci Educ Technol 2018;27:448–68. http://dx.doi.org/10.1007/s10956-018-9735-3.

[39] Durazzi N. The political economy of high skills: higher education in knowledge-based labour markets. J Eur Public Policy 2018;26:1799–817. http://dx.doi.org/10.1080/13501763.2018.1551415.

[40] Aziz M, Surono S. Integration model of occupational certification scheme into instructional design to close the gap of learning outcomes and industry needs. J Transnatl Univers Stud 2024. http://dx.doi.org/10.58631/jtus.v3i6.97.

[41] Kovalev A, Stefanac N, Rizoiu M. Skill-driven certification pathways: Measuring industry training impact on graduate employability. 2025, http://dx.doi.org/10.48550/arxiv.2506.04588, arXiv abs/2506.04588.

[42] Ni M. Research on the cultivation system of digital new-quality skilled talents based on the integration of industry, education, and research. Int J Educ Humanit 2025. http://dx.doi.org/10.54097/5b5z8n70.

[43] Rewire. A cybersecurity sector skills alliance. 2024, https://rewireproject.eu. URL: https://rewireproject.eu/publications/.

[44] SPARTA. Strategic programs for advanced research and technology in Europe. 2024, https://cordis.europa.eu/project/id/830892/factsheet.

[45] Concordia Project. Consortium : Concordia. 2025, https://www.concordia-h2020.eu/consortium/. [Accessed 12 June 2025].

[46] ECSO. The European cyber security organisation (ECSO). 2024, https://ecs-org.eu.

[47] Rathod P, Rajamäki J, Kioskli K. Implementing the European cybersecurity skills framework (ecsf): A case study of eu innovation projects. Eur Conf Cyber Warf Secur 2025. http://dx.doi.org/10.34190/eccws.24.1.3369.

[48] Bengtsson M. How to plan and perform a qualitative study using content analysis. NursingPlus Open 2016;2:8–14. http://dx.doi.org/10.1016/j.npls.2016.01.001, URL: https://www.sciencedirect.com/science/article/pii/S2352900816000029.

[49] Vears DF, Gillam L. Inductive content analysis: A guide for beginning qualitative researchers. Focus Health Prof Educ: A Multi-Professional J 2022;23:111–27. http://dx.doi.org/10.11157/fohpe.v23i1.544.

[50] CyberSec4Europe Consortium. Education and Training Review. Technical Report D6.2, Version 1.2, CyberSec4Europe; 2020, URL: https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf.

[51] Ramezanian S, Niemi V. Cybersecurity education in universities: A comprehensive guide to curriculum development. IEEE Access 2024;12:61741–66. http://dx.doi.org/10.1109/ACCESS.2024.3392970.

[52] Hajny J, Ricci S, Piesarskas E, Levillain O, Galletta L, De Nicola R. Framework, tools and good practices for cybersecurity curricula. IEEE Access 2021;9:94723–47. http://dx.doi.org/10.1109/ACCESS.2021.3093952.

[53] Vong KC, Udomvitid K, Ueki Y, Intalar N, Pongsathornwiwat A, Pannakkong W, Komolavanij S, Jeenanunta C. Strategic human resource development for industry 4.0 readiness: A sustainable transformation framework for emerging economies. Sustainability 2025;17. http://dx.doi.org/10.3390/su17156988, URL: https://www.mdpi.com/2071-1050/17/15/6988.

[54] JTF. Cybersecurity curricular guidelines. 2020, https://cybered.hosting.acm.org/wp/. [Online 17 November 2025].

[55] Kang H, Lee S. Automated analysis with apriori algorithm: deriving guidance for working-level cybersecurity curricula. ACM Inroads 2020;11:20–6. http://dx.doi.org/10.1145/3410471.

[56] Budde CE, Karinsalo A, Vidor S, Salonen J, Massacci F. Csec+ framework assessment dataset: Expert evaluations of cybersecurity skills for job profiles in Europe. Data Brief 2023;48:109285. http://dx.doi.org/10.1016/j.dib.2023.109285, URL: https://www.sciencedirect.com/science/article/pii/S2352340923004043.

[57] Ghosh T, Francia G. Assessing competencies using scenario-based learning in cybersecurity. J Cybersecur Priv 2021;1:539–52. http://dx.doi.org/10.3390/jcp1040027, URL: https://www.mdpi.com/2624-800X/1/4/27.

[58] Armstrong ME, Jones KS, Namin AS, Newton DC. Knowledge, skills, and abilities for specialized curricula in cyber defense: Results from interviews with cyber professionals. ACM Trans Comput Educ 2020;20. http://dx.doi.org/10.1145/3421254.

[59] Benson V, Chiacchio LD, Frączek B. Why soft skills matter for women in cybersecurity. J Comput Inf Syst 2025;1–14. http://dx.doi.org/10.1080/08874417.2025.2492883.

[60] Katsantonis MN, Manikas A, Mavridis I, Fouliras P. Tcofelet: Conceptual framework for team-centric e-learning and training. IEEE Access 2024;12:78878–94. http://dx.doi.org/10.1109/ACCESS.2024.3408685.

[61] Nnadi LC, Ding D, Godwin-Ojukwu ED, Watanobe Y, Naruse K. Strategic human resource development for emerging technologies: A scoping review in ICT, robotics, data science, and CPS. IEEE Access 2025;13:133994–4013. http://dx.doi.org/10.1109/ACCESS.2025.3592301.

[62] Ricci S, Parker S, Jerabek J, Danidou Y, Chatzopoulou A, Badonnel R, Lendak I, Janout V. Understanding cybersecurity education gaps in Europe. IEEE Trans Educ 2024;67:190–201. http://dx.doi.org/10.1109/TE.2023.3340868.

[63] Cooke RM. Experts in uncertainty: Opinion and subjective probability in science. Oxford University Press; 1991, http://dx.doi.org/10.1093/oso/9780195064650.001.0001.

[64] Gale NK, Heath G, Cameron E, Rashid S, Redwood S. Using the framework method for the analysis of qualitative data in multi-disciplinary health research. BMC Med Res Methodol 2013;13. http://dx.doi.org/10.1186/1471-2288-13-117.

[65] Hemming V, Burgman MA, Hanea AM, McBride MF, Wintle BC. A practical guide to structured expert elicitation using the idea protocol. Methods Ecol Evol 2018;9:169–80. http://dx.doi.org/10.1111/2041-210X.12857, https://onlinelibrary.wiley.com/doi/abs/10.1111/2041-210X.12857 https://besjournals.onlinelibrary.wiley.com/doi/10.1111/2041-210X.12857. WGROUP:STRING:PUBLICATION.

[66] Hanea AM, McBride MF, Burgman MA, Wintle BC. Classical meets modern in the idea protocol for structured expert judgement. J Risk Res 2018;21:417–33. http://dx.doi.org/10.1080/13669877.2016.1215346, URL: https://www.tandfonline.com/doi/abs/10.1080/13669877.2016.1215346.

[67] Likert R. A technique for the measurement of attitudes. Arch Psychol 1932;22:1–55.

[68] Offensive Security. Offensive security certified professional (oscp) certification. 2024, https://www.offsec.com/. [Accessed 18 November 2025].

[69] Knapp KJ, Maurer C, Plachkinova M. Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. J Inf Syst Educ 2017;28:101–14.

[70] ISC2. CISSP - certified information systems security professional. 2025, https://www.isc2.org/certifications/cissp. [Accessed 18 June 2025].

[71] Rashid Awais, et al. CyBOK Mapping framework – academic and professional programmes. Technical Report, Cyber Security Body of Knowledge (CyBOK); 2021, URL: https://www.cybok.org/media/downloads/CyBOK_Mapping_Framework_academic_professional_progs_Feb21.pdf.

[72] Dkaidek Z, Rashid A. Bridging the cybersecurity skills gap: Knowledge framework comparative study. IEEE Secur Priv 2024;22:88–95. http://dx.doi.org/10.1109/MSEC.2024.3428892.

[73] Chen Y, Kostiuk D, Subbian K, Yu M, Sheth A, Gray A, Varshney KR. Skills and expertise in large organizations: An enterprise knowledge graph approach. Technical Report, IBM Research; 2022, URL: https://research.ibm.com/publications/skills-and-expertise-in-large-organizations-an-enterprise-knowledge-graph-approach.

[74] Hajny J, Sikora M, Grammatopoulos AV, Di Franco F. Adding European cybersecurity skills framework into curricula designer. In: Proceedings of the 17th international conference on availability, reliability and security. New York, NY, USA: Association for Computing Machinery; 2022, p. 1–6. http://dx.doi.org/10.1145/3538969.3543799.

[75] Commission, E. E-competence framework (e-cf). 2024, ICT professions and competences framework. Aligns with ECSF for cybersecurity competency assessment.

[76] Pasupuleti MK. Securing ai-driven infrastructure: Advanced cybersecurity frameworks for cloud and edge computing environments. Int J Acad Ind Res Innov(IJAIRI) 2025. http://dx.doi.org/10.62311/nesx/rrv225.

[77] Almutairi M, Sheldon FT. Iot–cloud integration security: A survey of challenges, solutions, and directions. Electronics 2025. http://dx.doi.org/10.3390/electronics14071394.

[78] Eren H, Karaduman Özgür, Gençoğlu M. Security and privacy in the internet of everything (ioe): A review on blockchain, edge computing, ai, and quantum-resilient solutions. Appl Sci 2025. http://dx.doi.org/10.3390/app15158704.

[79] Ali G, Samuel A, Kabiito SP, Morish Z, Thomas A, Robert W, Denis A, Sallam M, Mijwil MM, Ayad J, Salau AO, Dhoska K. Integration of artificial intelligence, blockchain, and quantum cryptography for securing the industrial internet of things (iiot): Recent advancements and future trends. Appl Data Sci Anal 2025. http://dx.doi.org/10.58496/adsa/2025/004.

[80] Sreerangapuri A. Post-quantum cryptography for ai-driven cloud security solutions. Int J Multidiscip Res 2024. http://dx.doi.org/10.36948/ijfmr.2024.v06i05.29032.

[81] ENISA. Certifications-mapped-to-the-ecsf. 2025, https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf/certifications-mapped-to-the-ecsf. [Online 23 January 2026].

[82] Lane A. The systemic implications of constructive alignment of higher education level learning outcomes and employer or professional body based competency frameworks. In: Proceedings of the online, open and flexible higher education conference, 25-27 October 2017, Milton Keynes. EADTU; 2017, p. 411–26, URL: https://conference.eadtu.eu/previous-conferences.

[83] Salton G, Buckley C. Term-weighting approaches in automatic text retrieval. Inf Process Manage 1988;24:513–23. http://dx.doi.org/10.1016/0306-4573(88)90021-0, URL: https://www.sciencedirect.com/science/article/pii/0306457388900210.

[84] Deerwester S, Dumais ST, Furnas GW, Landauer TK, Harshman R. Indexing by latent semantic analysis. J Am Soc Inf Sci 1990;41:391–407. http://dx.doi.org/10.1002/(SICI)1097-4571(199009)41:6<391::AID-ASI1>3.0.CO;2-9, URL: https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/%28SICI%291097-4571%28199009%2941%3A6%3C391%3A%3AAID-ASI1%3E3.0.CO%3B2-9.

[85] Mikolov T, Chen K, Corrado G, Dean J. Efficient estimation of word representations in vector space. In: Proceedings of Workshop at ICLR, vol. 2013, 2013,

[86] Reimers N, Gurevych I. Sentence-BERT: Sentence embeddings using siamese BERT-networks. In: Inui K, Jiang J, Ng V, Wan X, editors. Proceedings of the 2019 conference on empirical methods in natural language processing and the 9th international joint conference on natural language processing. EMNLP-IJCNLP, Hong Kong, China: Association for Computational Linguistics; 2019, p. 3982–92. http://dx.doi.org/10.18653/v1/D19-1410, URL: https://aclanthology.org/D19-1410/.

[87] Francis SP, Kolil VK, Pavithran V, Ray I, Achuthan K. Exploring gender dynamics in cybersecurity education: A self-determination theory and social cognitive theory perspective. Comput Secur 2024;144:103968. http://dx.doi.org/10.1016/j.cose.2024.103968, URL: https://www.sciencedirect.com/science/article/pii/S0167404824002736.

[88] Heverin T, Lilholt A, Woodward E. Evaluating cybersecurity class activities based on the cognitive continuum theory: An exploratory case study. In: European conference on cyber warfare and security. 2024, http://dx.doi.org/10.34190/eccws.23.1.2371.

[89] Adams N. Bloom's taxonomy of cognitive learning objectives. J Med Libr Assoc : JMLA 2015;103 3:152–3. http://dx.doi.org/10.3163/1536-5050.103.3.010.

[90] Deist FDL, Winterton J. What is competence? Hum Resour Dev Int 2005;8:27–46. http://dx.doi.org/10.1080/1367886042000338227.

[91] Boeren E, Íñiguez Berrozpe T. Unpacking piaac's cognitive skills measurements through engagement with bloom's taxonomy. Stud Educ Eval 2022. http://dx.doi.org/10.1016/j.stueduc.2022.101151.

[92] Zerényi K, Mátrai Z. Taxonomies from a cognitive to a digital revolution, focusing on transferable skills. Andragoske Stud 2022. http://dx.doi.org/10.5937/andstud2202091z.

[93] Raman R, Venkatasubramanian S, Achuthan K, Nedungadi P. Computer science (cs) education in indian schools: Situation analysis using darmstadt model. ACM Trans Comput Educ 2015;15:1–36. http://dx.doi.org/10.1145/2716325.

[94] Klitis C, Makris I, Bouzinis P, Asimopoulos DC, Mallouli W, Kioskli K, Seralidou E, Douligeris C, Christofi L. Nero: Advanced cybersecurity awareness ecosystem for smes. In: Proceedings of the 19th international conference on availability, reliability and security. New York, NY, USA: Association for Computing Machinery; 2024, p. 1–9. http://dx.doi.org/10.1145/3664476.3670447.

[95] Aarjav Jain AJ. An analysis on challenges faced by cyber security on the latest technologies. J Adv Sci Technol 2024;20:71–5. http://dx.doi.org/10.29070/by8v4h97.

[96] Mijwil M, Unogwu OJ, Filali Y, Bala I, Al-Shahwani H. Exploring the top five evolving threats in cybersecurity: An in-depth overview. Mesopotamian J CyberSecurity 2023;2023:57–63. http://dx.doi.org/10.58496/mjcs/2023/010.

[97] Seid E, Popov O, Blix F. An automated adaptive security framework for cyber-physical systems. In: Proceedings of the 10th international conference on information systems security and privacy. SCITEPRESS - Science and Technology Publications; 2024, p. 242–53. http://dx.doi.org/10.5220/0012469100003648.

[98] Repetto M, Striccoli D, Piro G, Carrega A, Boggia G, Bolla R. An autonomous cybersecurity framework for next-generation digital service chains. J Netw Syst Manage 2021;29. http://dx.doi.org/10.1007/s10922-021-09607-7.

[99] Graham CM. Ai skills in cybersecurity: global job trends analysis. Inf Comput Secur 2025;33:673–89. http://dx.doi.org/10.1108/ICS-09-2024-0235, URL: https://www.sciencedirect.com/science/article/pii/S2056496125000182.

[100] Di Mary A Meyer, JMB. Eliciting and Analyzing Expert Judgment. URL: https://epubs.siam.org/doi/abs/10.1137/1.9780898718485.fm. arXiv:https://epubs.siam.org/doi/pdf/10.1137/1.9780898718485.fm. http://dx.doi.org/10.1137/1.9780898718485.fm.

[101] Mosli R. Optimal job role allocation for compliance with nca-ecc controls using the Saudi cybersecurity workforce framework. IEEE Access 2024;12:128235–45. http://dx.doi.org/10.1109/ACCESS.2024.3457025.

[102] Gambo ML, Danasabe A, Binbeshr F, Imam M, Shinwari MW, Mahmoud A. Navigating the cyber landscape: Saudi Arabia's cybersecurity standards and implementation barriers. Arab J Sci Eng 2025. http://dx.doi.org/10.1007/s13369-025-10765-y.

[103] Khadka K, Ullah AB. Human factors in cybersecurity: an interdisciplinary review and framework proposal. Int J Inf Secur 2025;24. http://dx.doi.org/10.1007/s10207-025-01032-0.

[104] Bendler D, Felderer M. Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model. ACM Trans Comput Educ 2023;23:1–33. http://dx.doi.org/10.1145/3573205.

[105] Shokeen B. Skill oriented certification & value-addition courses for employability, sustainability & lifelong learning. Soc Sci Rev A Multidiscip J 2025. http://dx.doi.org/10.70096/tssr.250307005.

[106] Petersen K, Vakkalanka S, Kuzniarz L. Guidelines for conducting systematic mapping studies in software engineering: An update. Inf Softw Technol 2015;64:1–18. http://dx.doi.org/10.1016/j.infsof.2015.03.007, URL: https://www.sciencedirect.com/science/article/pii/S0950584915000646.

[107] Kitchenham B, Brereton P. A systematic review of systematic review process research in software engineering. Inf Softw Technol 2013;55:2049–75. http://dx.doi.org/10.1016/j.infsof.2013.07.010, URL: https://www.sciencedirect.com/science/article/pii/S0950584913001560.

[108] Aguilar AI, Li R. Responsibility assignment matrix in responding to critical outages: A case study of it incident management activity process design. In: Proceedings of the 2023 5th international conference on management science and industrial engineering. New York, NY, USA: Association for Computing Machinery; 2023, p. 1–8. http://dx.doi.org/10.1145/3603955.3603956.

[109] Zubaedah PA, Harliyanto R, Situmeang SMT, Siagian DS, Septaria E. The legal implications of data privacy laws, cybersecurity regulations, and ai ethics in a digital society. J Acad Sci 2024;1. http://dx.doi.org/10.59613/29qypw51, URL: http://dx.doi.org/10.59613/29qypw51.

[110] Cosentino V, Cánovas Izquierdo JL, Cabot J. A systematic mapping study of software development with github. IEEE Access 2017;5:7173–92. http://dx.doi.org/10.1109/ACCESS.2017.2682323.

[111] Ramsoonder NK, Kinnoo S, Griffin AJ, Valli C, Johnson N. Optimizing cyber security education: Implementation of bloom's taxonomy for future cyber security workforce. In: 2020 international conference on computational science and computational intelligence. CSCI, 2020, p. 93–8. http://dx.doi.org/10.1109/csci51800.2020.00023.

[112] Prakash R, Litoriya R. Pedagogical transformation of bloom taxonomy's lots into hots: An investigation in context with it education. Wirel Pers Commun 2021;122:725–36. http://dx.doi.org/10.1007/s11277-021-08921-2.

[113] Ali MK, Ali A, Ali FF, Ali RI, Hasanah A. Membangun kompetensi berpikir tinggi dan keterampilan kerja: Analisis perbandingan taksonomi bloom revisi dan taksonomi simpson/harrow dalam konteks pendidikan sma dan smk. Cognoscere: J Komun Dan Media Pendidik 2025. http://dx.doi.org/10.61292/cognoscere.260.

[114] Ligale LM. Redefining the blooms taxonomy - developing a framework for cognitive competence acquisition. Afr J Tech Vocat Educ Train 2025. http://dx.doi.org/10.69641/afritvet.2025.101176.

[115] Harrow AJ. A taxonomy of the psychomotor domain: A guide for developing behavioral objectives. New York: McKay; 1972.

[116] Simon HA. The architecture of complexity. Boston, MA: Springer US; 1991, p. 457–76. http://dx.doi.org/10.1007/978-1-4899-0718-9_31, chapter 31.

[117] Parnas DL. On the criteria to be used in decomposing systems into modules. Commun ACM 1972;15:1053–8. http://dx.doi.org/10.1145/361598.361623.

[118] Baldwin C. The power of modularity: the financial consequences of computer and code architecture. In: Proceedings of the 5th international conference on aspect-oriented software development. New York, NY, USA: Association for Computing Machinery; 2006, p. 1. http://dx.doi.org/10.1145/1119655.1119657.

[119] Hussain S, Keung J, Khan AA. The effect of gang-of-four design patterns usage on design quality attributes. 2017 IEEE international conference on software quality, reliability and security. QRS, IEEE; 2017, p. 263–73. http://dx.doi.org/10.1109/qrs.2017.37.

[120] Klir GJ, Yuan B. Fuzzy sets and fuzzy logic: Theory and applications. Upper Saddle River, NJ, USA: Prentice-Hall, Inc. 1994.

[121] Karatop B, Kubat C, Uygun O. Talent management in manufacturing system using fuzzy logic approach. Comput Ind Eng 2015;86:127–36. http://dx.doi.org/10.1016/j.cie.2014.09.015.

[122] Luna RP, Rodríguez GG, Guerrero-Ramos LA, Andrade RAE, Rodríguez S, De-León-Gómez V. Smart competence management using business analytics with fuzzy predicates. Axioms 2021;10:280. http://dx.doi.org/10.3390/axioms10040280.

[123] Raman R, Calyam P, Achuthan K. Chatgpt or bard: Who is a better certified ethical hacker? Comput Secur 2024;140:103804. http://dx.doi.org/10.1016/j.cose.2024.103804, URL: https://www.sciencedirect.com/science/article/pii/S0167404824001056.

[124] Tridgell J. Open or closing doors? The influence of 'digital sovereignty' in the EU's Cybersecurity Strategy on cybersecurity of open-source software. Comput Law Secur Rev 2025;56:106078. http://dx.doi.org/10.1016/j.clsr.2024.106078, URL: https://www.sciencedirect.com/science/article/pii/S0267364924001444.

[125] Plevnik M, Gumzej R. Open source as the foundation of safety and security in logistics digital transformation. Systems 2025;13. http://dx.doi.org/10.3390/systems13060424, URL: https://www.mdpi.com/2079-8954/13/6/424.

[126] Zhang X, Yu Y, Gousios G, Rastogi A. Pull request decisions explained: An empirical overview. IEEE Trans Softw Eng 2023;49:849–71. http://dx.doi.org/10.1109/TSE.2022.3165056.

[127] Gruber TR. Toward principles for the design of ontologies used for knowledge sharing? Int J Hum-Comput Stud 1995;43:907–28. http://dx.doi.org/10.1006/ijhc.1995.1081, URL: https://www.sciencedirect.com/science/article/pii/S1071581985710816.

[128] Darlington M, Culley S. Investigating ontology development for engineering design support. Adv Eng Inform 2008;22:112–34. http://dx.doi.org/10.1016/j.aei.2007.04.001, URL: https://www.sciencedirect.com/science/article/pii/S1474034607000237. intelligent computing in engineering and architecture.