SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M8 Frameworks that describe the competencies

Contents

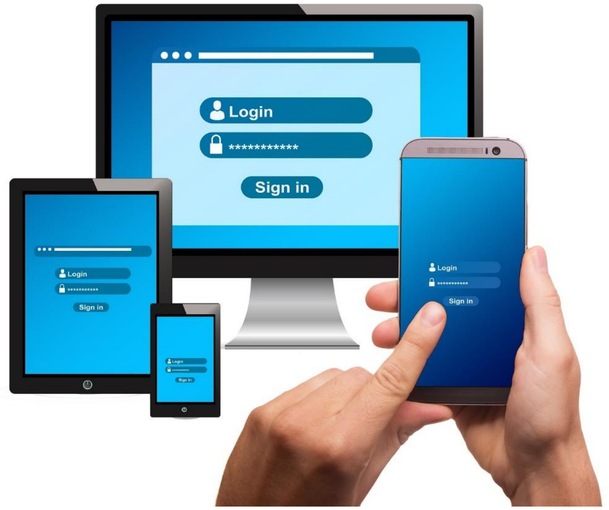
8.1 Frameworks that describe the competencies

- Introduction to the main Frameworks commonly recognized to describe professional profiles within ICT security
- Levels, professional roles, and mapped competencies. European e-Competence Framework (e-CF)
- NICE and AGID Frameworks

Digital world and employment

STANDARDIZATION OF COMPETENCIES

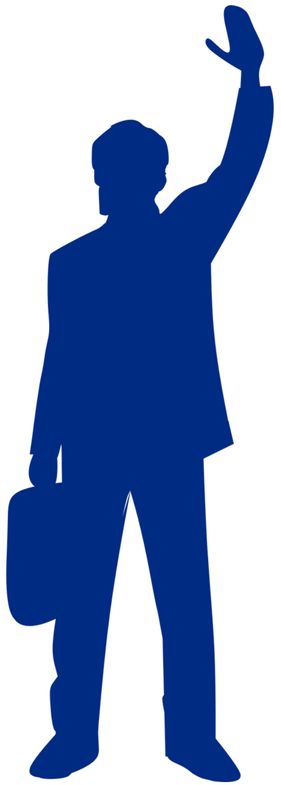
In all advanced economies, work is becoming increasingly **knowledge intensive** both in terms of *specific* knowledge and in terms of more *general* knowledge. The pervasiveness of the use of machines, digital technology and artificial intelligence (AI) requires more and more specific knowledge in the technological field.



ICT Competencies

STANDARDIZATION

This knowledge is now indispensable not only for highly qualified professions, which have always been characterized by a high intensity of knowledge, but also for apparently less qualified professions that actually interact with extremely *sophisticated* and *complex* devices, robots and machines.



ICT Competencies

STANDARDIZATION

The need to observe *social distancing* also in working activities has led to an exponential increase in smart working, an already growing practice but which has now become “**regular**” for many activities. Remote working or real smart working *accentuate even more* the importance of digital skills in the performance of work.

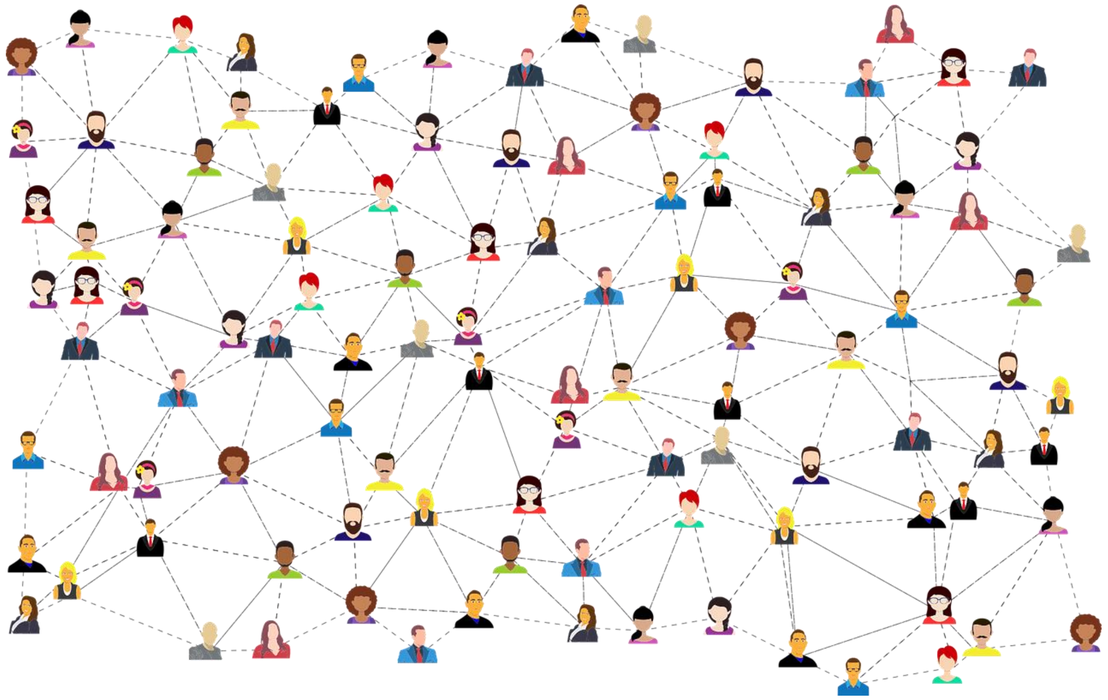
[Source: Unioncamere, Sistema Informativo Excelsior - forecasting of employment and professional needs in Italy in the medium term (2020-2024)]

Common language

TO RESPOND THE GROWING DEMAND

The rapid evolution and expansion of ICT labor markets requires a **common language** to manage the supply and demand for *talents*, which is particularly critical and complex in a scenario of transnational integration such as the European Union.

Models and frameworks are useful tools for this purpose.



Digital world and employment

STANDARDIZATION OF COMPETENCIES

Digital skills frameworks can improve **information security** in many ways, regardless of whether the focus is on cybersecurity (as in the NICE framework).

The more the skills can be typified and composited, *the more* it is possible to search for specific skills in the professional figures that one wants to hire for **certain** jobs, and the workers can test their skills in the same way against the typed criteria.

e-CF

UNI EN 16234-1

European e-Competence Framework (e-CF) is a reference framework of ICT **competences** that can be used used and understood by ICT user and supply **companies**, ICT **practitioners**, **managers** and **Human Resources** (HR) departments, the **public** sector, **educational** and **social partners** across Europe.

e-CF was designed to be an **empowerment** tool for users, and not to define any kind of restrictions and was designed to support understanding, not to make the use of every term used within the framework mandatory

Please note: **Competence** should not be *confused* with **technological** or **process concepts** such as 'Cloud Computing' or 'Big Data'. These concepts represent evolving technologies and, in the context of the e-CF, can be integrated as examples in the description of knowledge and skills.

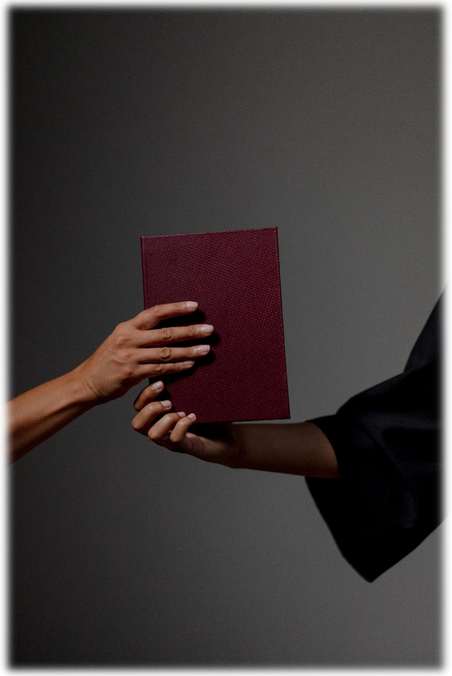
e-CF definitions

UNI EN 16234-1

What is **competence**?

> "*Competence is a demonstrated ability to apply knowledge, skills and attitudes to achieving* ***observable results***"
>
> Consequently, the related e-Competence descriptions embed and integrate knowledge, skills and attitudes.

[Source: User guide for the application of the European e-Competence Framework]



e-CF definitions

UNI EN 16234-1

What is **skill**?

Skill is defined as "*ability to carry out managerial or technical tasks*". Managerial and technical **skills are the components of competences** and specify some core abilities which form a competence.

[Source: User guide for the application of the European e-Competence Framework]

e-CF definitions

UNI EN 16234-1

Let's define **knowledge**

Knowledge represents the "*set of know-what*" (e.g. programming languages, design tools...) and can be described by operational descriptions as well.

[Source: User guide for the application of the European e-Competence Framework]

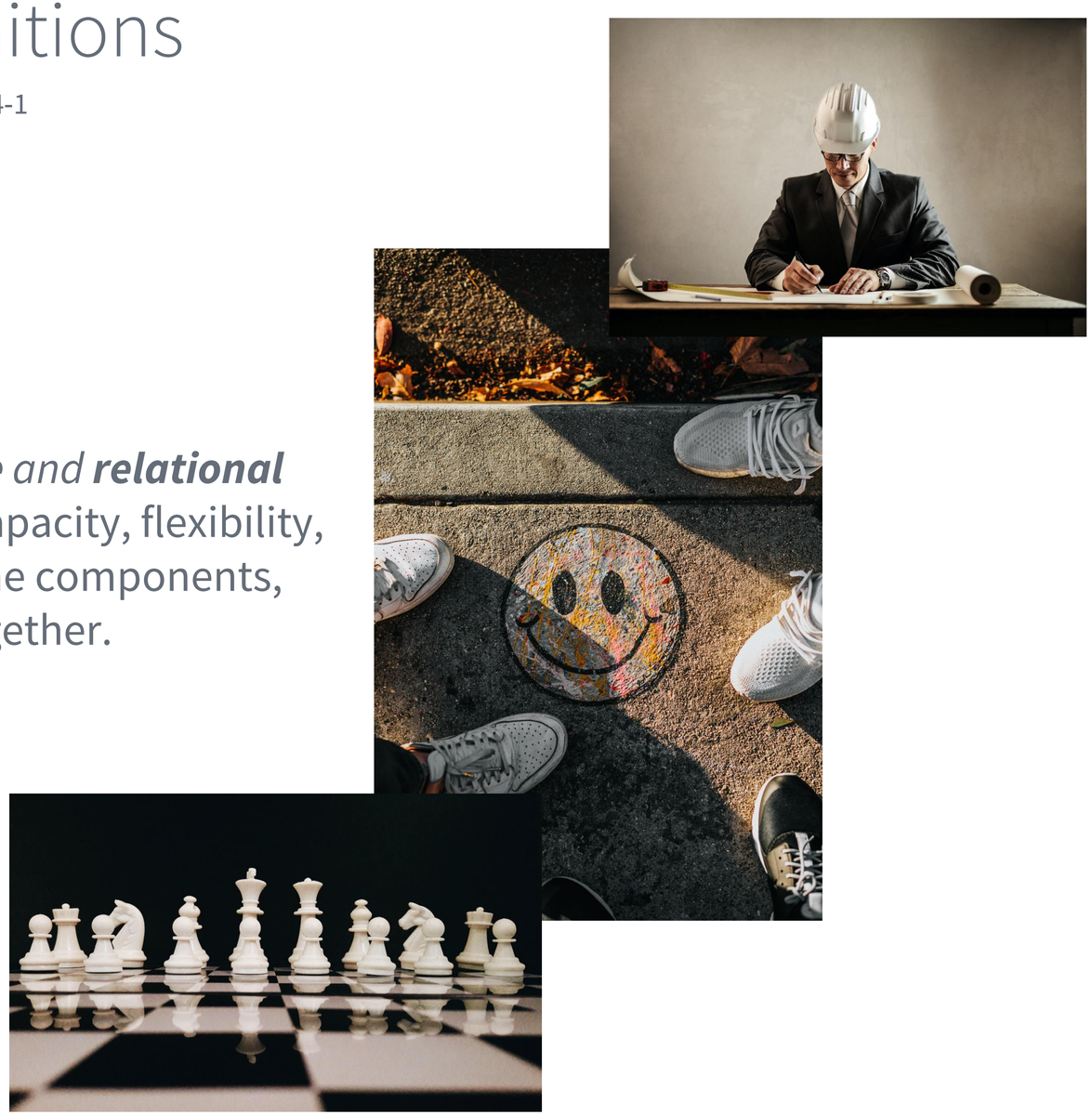
e-CF definitions

UNI EN 16234-1

Let's define **attitude**

Attitude means in this context the "***cognitive*** *and* ***relational*** *capacity*" (e.g. analysis capacity, synthesis capacity, flexibility, pragmatism...). If skills and knowledge are the components, attitudes are the **glue**, which keeps them together.

[Source: User guide for the application of the European e-Competence Framework]



e-CF proficiency levels

UNI EN 16234-1

[Source: User guide for the application of the European e-Competence Framework]

e-Competence proficiency levels "Level" is another basic concept used within the European e-Competence Framework. (It is identified in the e-CF **Dimension 3**).

In the e-CF this concept refers to "*proficiency*" levels instead of "learning" levels in the EQF. This is another reason why e-CF levels are different from the EQF levels, even though strong relationships can be found.
A proficiency level **integrates three facets**, as shown in the e-Competence level table in the Annex:

context complexity, autonomy and behaviour. Hence, the proficiency levels described in Dimension 3 *embed these three components*.

e-CF proficiency levels

UNI EN 16234-1

[Source: User guide for the application of the European e-Competence Framework]

All these dimensions are also present and easily identifiable within the **EQF** definitions and descriptions.
This maintains a uniform relationship between the two frameworks. In particular, in the e-CF, these three dimensions can be summarised as following:

- **Autonomy** ranges between "*Responding to instructions*" and "*Making personal choices*".
- **Context complexity** ranges between "*Structured – Predictable*" situations and "*Unpredictable – Unstructured*" situations.
- **Behaviour** here represents an observable outcome of attitude and ranges between "*the ability to apply*" and "*the ability to conceive*".

e-CF proficiency levels

UNI EN 16234-1

EQF=*European Qualifications Framework*.

Annex 2 of the e-CF compares European e-CF and EQF leves.

[Source: User guide for the application of the European e-Competence Framework]

e-CF Structure and Look

The European e-Competence Framework is structured from **four dimensions**.

These dimensions *reflect* different levels of business and human resource planning requirements in addition to job / work proficiency guidelines and are specified as follows.

e-CF Structure and Look

Dimension 1:
5 e-Competence areas, derived from the ICT business processes PLAN – BUILD – RUN – ENABLE – MANAGE

Dimension 2:
A set of reference e-Competences for each area, with a generic description for each competence. 40 competences identified in total provide the European generic reference definitions of the e-CF 3.0.

Dimension 3:
Proficiency levels of each e-Competence provide European reference level specifications on e-Competence levels e-1 to e-5, which are related to the EQF levels 3 to 8.

Dimension 4:
Samples of knowledge and skills relate to e-Competences in dimension 2. They are provided to add value and context and are not intended to be exhaustive.

e-CF Structure and Look

Whilst competence definitions are explicitly assigned to dimension **2** and **3** and *knowledge* and *skills* samples appear in dimension 4 of the framework, **attitude** is embedded in **all three dimensions**.

e-CF Overview

European e-Competence Framework 3.0 overview

Dimension 1 5 e-CF areas (A – E)	**Dimension 2** 40 e-Competences identified	**Dimension 3** e-Competence proficiency levels e-1 to e-5, related to EQF levels 3–8				
		e-1	**e-2**	**e-3**	**e-4**	**e-5**
A. PLAN	A.1. IS and Business Strategy Alignment				■	■
	A.2. Service Level Management			■	■	
	A.3. Business Plan Development			■	■	■
	A.4. Product/Service Planning		■	■	■	
	A.5. Architecture Design			■	■	■
	A.6. Application Design	■	■	■		
	A.7. Technology Trend Monitoring				■	■
	A.8. Sustainable Development			■	■	
	A.9. Innovating				■	■
B. BUILD	B.1. Application Development	■	■	■		
	B.2. Component Integration		■	■	■	
	B.3. Testing	■	■	■	■	
	B.4. Solution Deployment	■	■	■		
	B.5. Documentation Production	■	■	■		
	B.6. Systems Engineering			■	■	

e-CF Overview

Dimension 1 5 e-CF areas (A – E)	**Dimension 2** 40 e-Competences identified	**Dimension 3** e-Competence proficiency levels e-1 to e-5, related to EQF levels 3–8				
		e-1	**e-2**	**e-3**	**e-4**	**e-5**
C. RUN	C.1. User Support	■	■	■		
	C.2. Change Support		■	■		
	C.3. Service Delivery	■	■	■		
	C.4. Problem Management		■	■	■	
D. ENABLE	D.1. Information Security Strategy Development				■	■
	D.2. ICT Quality Strategy Development				■	■
	D.3. Education and Training Provision		■	■		
	D.4. Purchasing		■	■	■	
	D.5. Sales Proposal Development		■	■		
	D.6. Channel Management			■	■	
	D.7. Sales Management			■	■	■
	D.8. Contract Management		■	■	■	
	D.9. Personnel Development		■	■	■	
	D.10. Information and Knowledge Management			■	■	■
	D.11. Needs Identification			■	■	■
	D.12. Digital Marketing		■	■	■	
E. MANAGE	E.1. Forecast Development			■	■	
	E.2. Project and Portfolio Management		■	■	■	■
	E.3. Risk Management		■	■	■	
	E.4. Relationship Management			■	■	
	E.5. Process Improvement			■	■	
	E.6. ICT Quality Management		■	■	■	
	E.7. Business Change Management			■	■	■
	E.8. Information Security Management		■	■	■	
	E.9. IS Governance				■	■

e-Cf Full version – B.6

Dimension 1 e-Comp. area	**B. BUILD**				
Dimension 2 e-Competence: Title + generic description	**B.6. Systems Engineering** Engineers software and/or hardware components to meet solution requirements such as specifications, costs, quality, time, energy efficiency, information security and data protection. Follows a systematic methodology to analyse and build the required components and interfaces. Builds system structure models and conducts system behavior simulation. Performs unit and system tests to ensure requirements are met.				
Dimension 3 e-Competence proficiency levels e-1 to e-5, related to EQF levels 3 to 8	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
	–	Ensures interoperability of the system components. Exploits wide ranging specialist knowledge to create a complete system that will satisfy the system constraints and meet the customer's expectations.	Handles complexity by developing standard procedures and architectures in support of cohesive product development. Establishes a set of system requirements that will guide the design of the system. Identifies which system requirements should be allocated to which elements of the system.	–	–
Dimension 4 Knowledge examples *Knows/aware of/ familiar with*	K1 appropriate software programs/modules, DBMS and programming languages K2 hardware components, tools and hardware architectures K3 functional & technical designing K4 state of the art technologies K5 programming languages K6 power consumption models of software and/or hardware K7 information Security Basics K8 prototyping				
Skills examples *Is able to*	S1 explain and communicate the design/development to the customer S2 perform and evaluate test results against product specifications S3 apply appropriate software and/or hardware architectures S4 design and develop hardware architecture, user interfaces, business software components and embedded software components S5 manage and guarantee high levels of cohesion and quality in complex software developments S6 use data models S7 apply appropriate development and/or process models, to develop effectively and efficiently				

e-Cf Full version – B.6

Dimension 1 e-Comp. area	**E. MANAGE**				
Dimension 2 e-Competence: Title + generic description	**E.8. Information Security Management** Implements information security policy. Monitors and takes action against intrusion, fraud and security breaches or leaks. Ensures that security risks are analysed and managed with respect to enterprise data and information. Reviews security incidents, makes recommendations for security policy and strategy to ensure continuous improvement of security provision.				
Dimension 3 e-Competence proficiency levels e-1 to e-5, related to EQF levels 3 to 8	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
	–	Systematically scans the environment to identify and define vulnerabilities and threats. Records and escalates non-compliance.	Evaluates security management measures and indicators and decides if compliant to information security policy. Investigates and instigates remedial measures to address any security breaches.	Provides leadership for the integrity, confidentiality and availability of data stored on information systems and complies with all legal requirements.	–
Dimension 4 Knowledge examples *Knows/aware of/ familiar with*	K1 the organisations security management policy and its implications for engagement with customers, suppliers and subcontractors K2 the best practices and standards in information security management K3 the critical risks for information security management K4 the ICT internal audit approach K5 security detection techniques, including mobile and digital K6 cyber attack techniques and counter measures for avoidance K7 computer forensics				
Skills examples *Is able to*	S1 document the information security management policy, linking it to business strategy S2 analyse the company critical assets and identify weaknesses and vulnerability to intrusion or attack S3 establish a risk management plan to feed and produce preventative action plans S4 perform security audits S5 apply monitoring and testing techniques S6 establish the recovery plan S7 implement the recovery plan in case of crisis				

NICE Framework

NIST - WORKFORCE FRAMEWORK FOR CYBERSECURITY

NIST Special Publication 800-181 revision 1, the *Workforce Framework for Cybersecurity (NICE Framework)*, provides a set of **building blocks** for describing the *tasks*, *knowledge*, and *skills* that are **needed to perform cybersecurity work** performed by individuals and teams. Through these building blocks, the NICE Framework enables organizations to develop their *workforces* to perform cybersecurity work, and it helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills.

[Source: nist.gov]

NICE Framework

NIST - WORKFORCE FRAMEWORK FOR CYBERSECURITY

This publication from the National Initiative for Cybersecurity Education (NICE) constitutes a fundamental reference for describing and sharing information about cybersecurity work.

It expresses that work as Task statements and describes Knowledge and Skill statements that provide a foundation for learners including **students**, job **seekers**, and **employees**. The use of these statements helps students to develop skills, job seekers to demonstrate competencies, and employees to accomplish tasks.

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

NIST - WORKFORCE FRAMEWORK FOR CYBERSECURITY

As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent.
The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity *education*, *training*, and *workforce* development.

Keywords for the framework are
Competency; cybersecurity; cyberspace; education; knowledge; role; security; skill; task; team; training; workforce; work role.

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

‘BUILDING BLOCKS’ APPROACH

The “*work*” is what an organization needs to achieve cybersecurity risk management objectives. Every organization executes common tasks as well as some context-unique tasks. For example, every organization has some form of management tasks, whereas only some organizations have tasks to “*deploy bulk energy systems securely*.” The NICE Framework provides organizations a way to describe their work through Task statements that group supporting Knowledge and Skill statements.

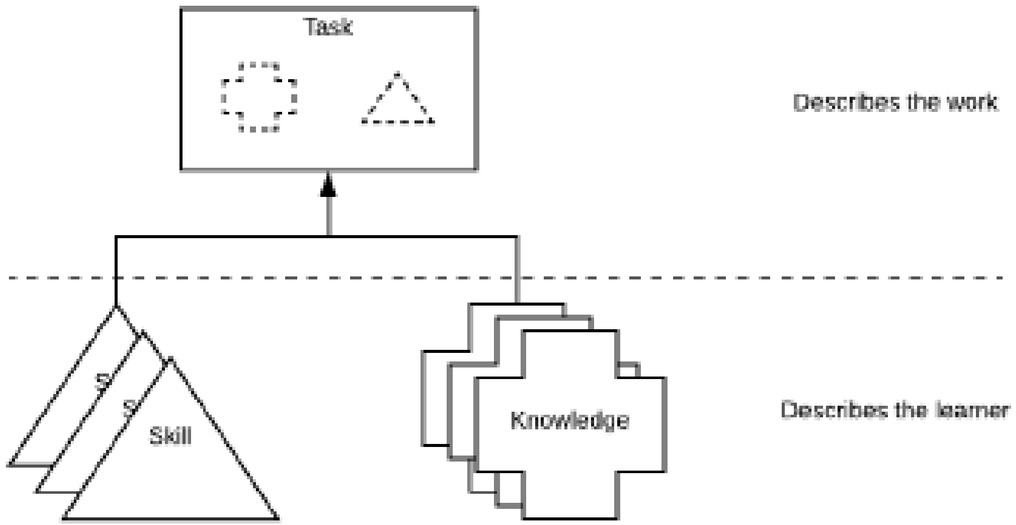


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

‘BUILDING BLOCKS’ APPROACH

The “*learner*” is the person who has knowledge and skills. The term *learner* applies to all people within the scope of this document. A learner can be a student, job seeker, employee, or other people within the workforce. In an organizational context, learners execute tasks. In an educational context, learners acquire new **knowledge** and **skills**.
All individuals are considered learners due to education or training they received prior to entering the workforce, ongoing training, self-learning, or a career progression plan.

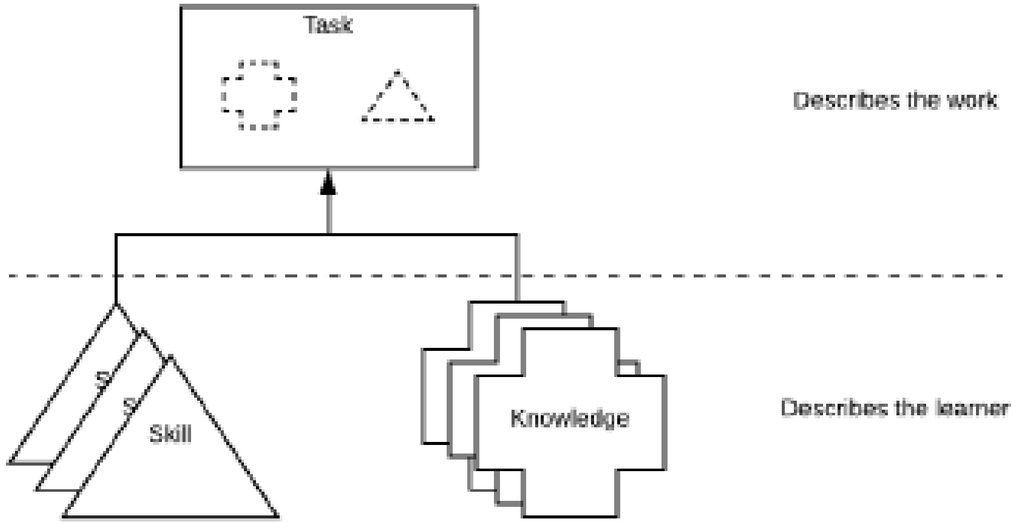


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

‘BUILDING BLOCKS’ APPROACH

The NICE Framework provides organizations with a way to describe learners by associating **Knowledge** and **Skill** statements to an *individual* or group. By using their Knowledge and Skills, learners can complete Tasks *to achieve organizational objectives*. While not all organizations will use every concept pertaining to learners, the NICE Framework provides organizations with a flexible set of building blocks to use as needed by their unique context. The recognition of the role the learner plays in developing capabilities to perform cybersecurity work also reinforces the applicability of the NICE Framework to education and training providers.

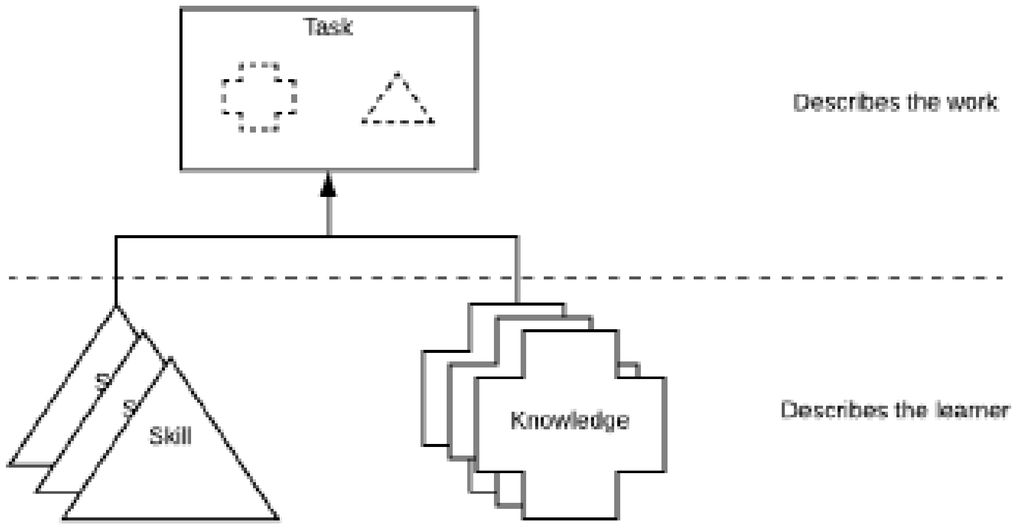


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

‘BUILDING BLOCKS’ APPROACH

By describing both the **work** and the **learner**, the NICE Framework provides organizations a *common language to describe their cybersecurity work and workforce*. Parts of the NICE Framework describe an organizational work context (Tasks), other parts describe a learner context (Knowledge and Skill), and finally, the building block approach of the NICE Framework allows organizations to *link the two contexts together*.

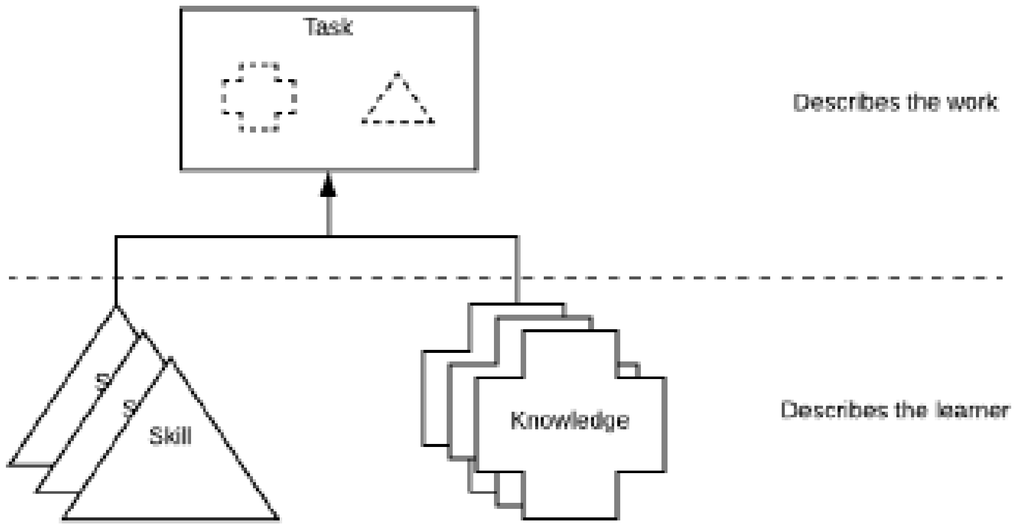


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

‘BUILDING BLOCKS’ APPROACH

Furthermore, the NICE Framework provides a mechanism to communicate across organizations at a **peer** level, **sector** level, **state** level, **national** level, or **international** level using the *same building blocks*. This communication can drive innovative solutions to common challenges, lower barriers to entry for new organizations and individuals, and *facilitate* workforce **mobility**.

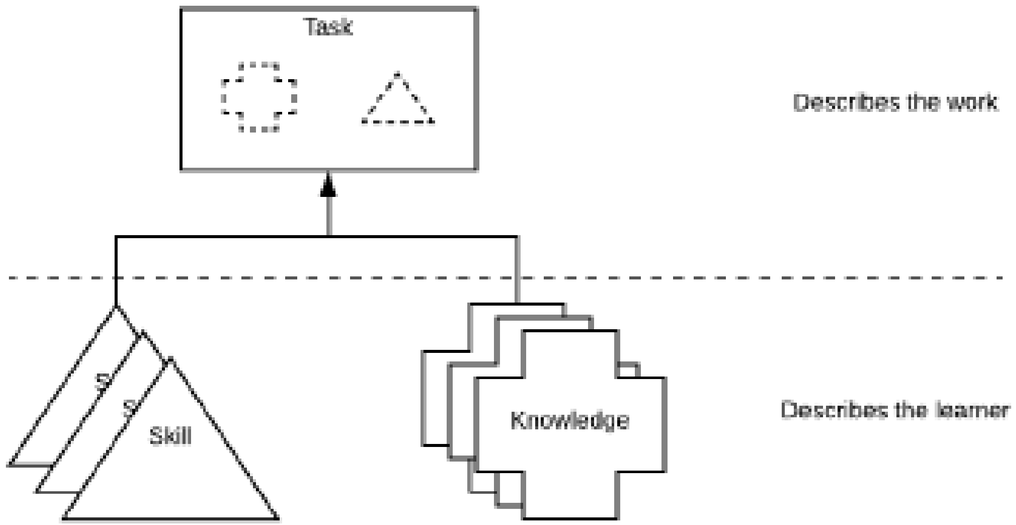


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

ATTRIBUTES

Attributes of the NICE Framework

The NICE Framework is a reference resource for those seeking to describe the cybersecurity work their organization does, the people who will carry out the work, and the ongoing learning that will be needed to do that work effectively. The nature of the work, and consequently, the workforce, can be described using the **TKS building blocks** presented in the following sections.

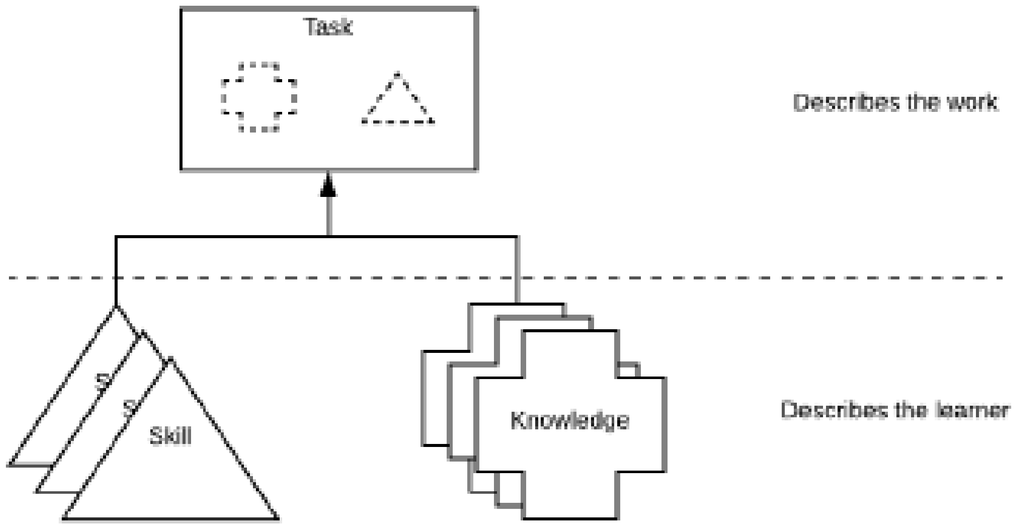


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

ATTRIBUTES

These building blocks *incorporate* the following attributes:

- **Agility—***People*, *processes*, and *technology* mature and must adapt to change. Therefore, the NICE Framework enables organizations to keep pace with a constantly evolving ecosystem.

- **Flexibility—**While every organization faces similar challenges, there is no one-size-fits-all solution to those common challenges. Therefore, the NICE Framework enables organizations to account for the organization's *unique* operating context.

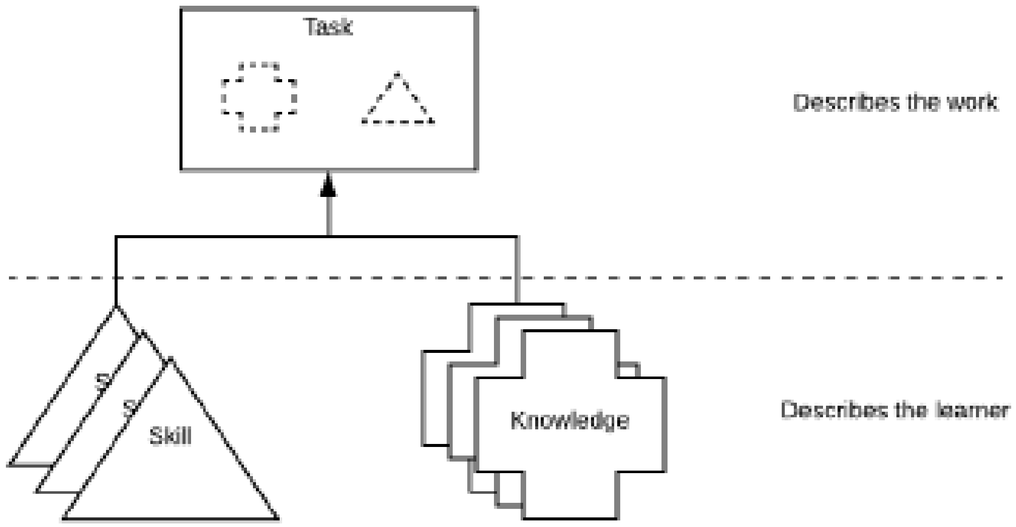


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

ATTRIBUTES

● **Interoperability—**While every solution to common challenges is unique, those solutions must agree upon consistent use of terms. Therefore, the NICE Framework enables organizations to exchange workforce information using a common language.

● **Modularity—**While cybersecurity risk remains the basis of this document, there are other risks that organizations must manage within the enterprise. Therefore, the NICE Framework enables organizations to communicate about other types of workforces within an enterprise and across organizations or sectors (e.g., privacy, risk management, software engineering/development).

[Source: NIST Special Publication 800-181, Revision 1]

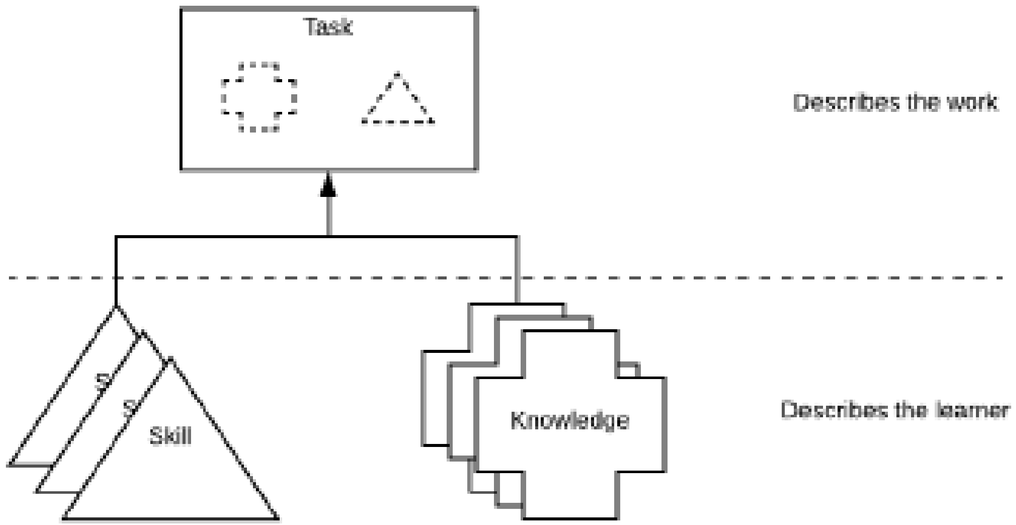


Figure 1 - NICE Framework Building Blocks Approach

NICE Framework

TASK

Task Statements

As depicted in Figure 1, Task statements describe the **work**, *while Knowledge and Skill (K&S) statements describe the* ***learner***. Task statements should focus on the organizational language and communication patterns that provide value to the organization. These statements are designed to describe work to be done and should be aligned with the context of the organization.

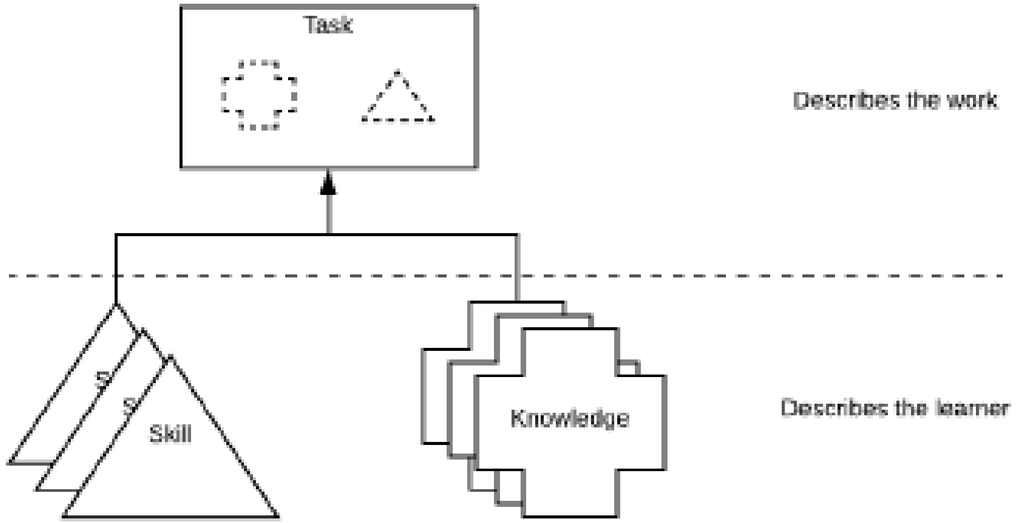


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

TASK

Tasks describe **work** to be completed. A task can be defined as an activity that is directed toward the achievement of organizational objectives, including business objectives, technology objectives, or mission objectives. Task statements should be **straightforward**. While the work encompassed within a Task statement may have many steps, the statement itself is easy to read and understand.

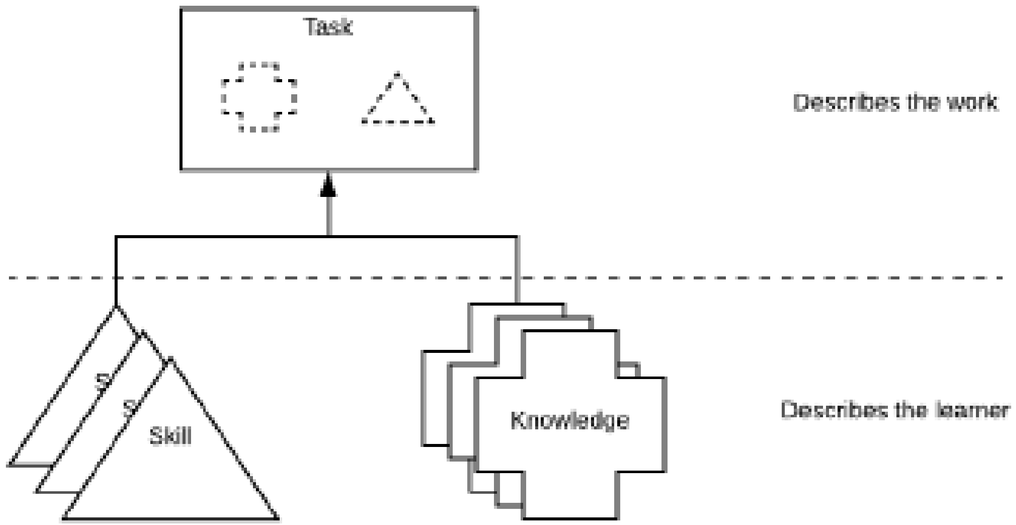


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

KNOWLEDGE

Knowledge Statements
Knowledge statements relate to Task statements in that only with the understanding described by the Knowledge statement will the learner be able to complete the Task. Knowledge is defined as a *retrievable set of concepts within memory*. Knowledge statements may describe either **foundational** or **specific** concepts. Multiple Knowledge statements may be needed to complete a given Task. Likewise, one Knowledge statement may be used to complete many different Tasks.

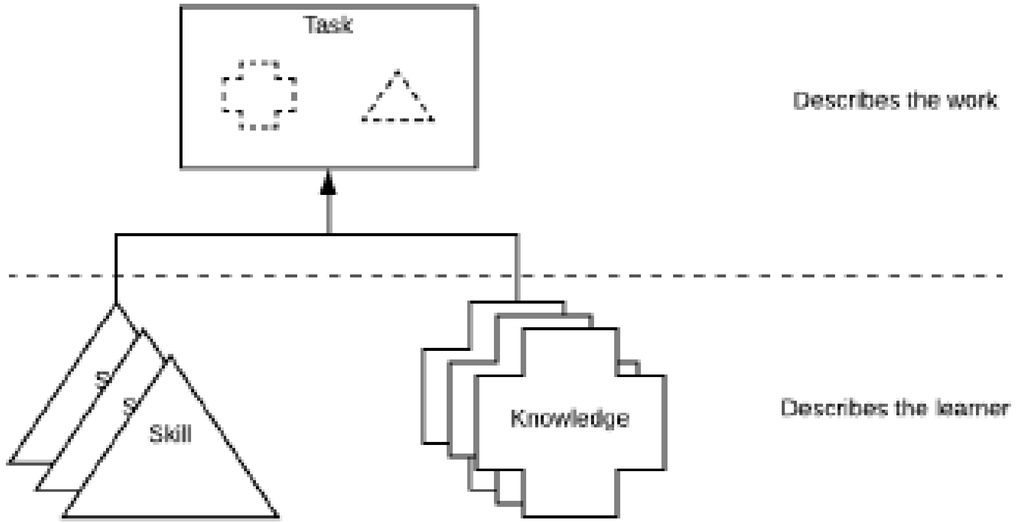


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

SKILL

Skill Statements
Skill statements relate to Task statements in that a learner is demonstrating skills in performing tasks. A learner who is not able to demonstrate the described skill would not be able to complete the Task that relies on that skill. A Skill is defined as the *capacity to perform an observable action*. Skill statements may describe **straightforward** or **complex** skills. Multiple Skill statements may be needed to complete a given Task. Likewise, exercising a Skill may be used to complete more than one Task.

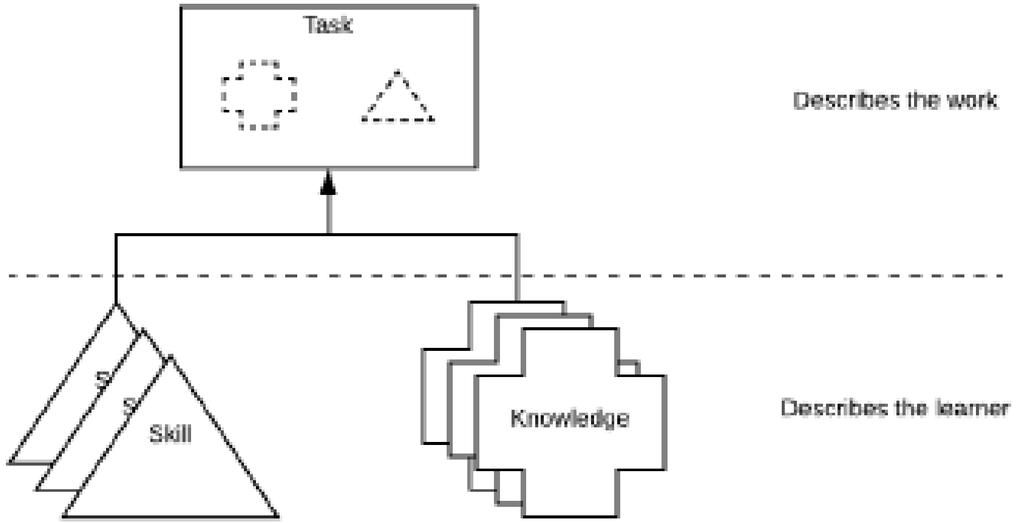


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

SKILL

Users may also create entirely **new** Task, Knowledge, or Skill statements to help tailor the use of the NICE Framework for **local use** within their unique context.

Such additional statements will help support clear and consistent internal discussions regarding learners and their work activities.

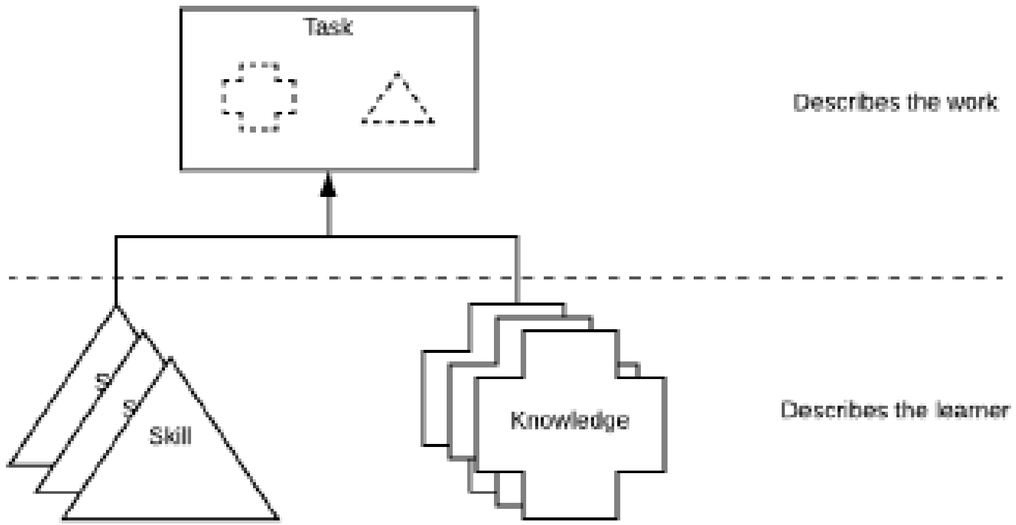


Figure 1 - NICE Framework Building Blocks Approach

[Source: NIST Special Publication 800-181, Revision 1]

NICE Framework

COMPETENCIES

Competencies
Competencies provide a mechanism for organizations to assess learners. Competencies are defined via an *employer-driven* approach that provides insight to an organization's unique context.
Furthermore, Competencies allow education and training providers to be responsive to employer or sector needs by developing learning experiences that help learners develop and demonstrate the Competencies.

Competencies consist of a **name**, **description** of the Competency, **assessment** method, as well as a group of associated **TKS statements**.

[Source: NIST Special Publication 800-181, Revision 1]

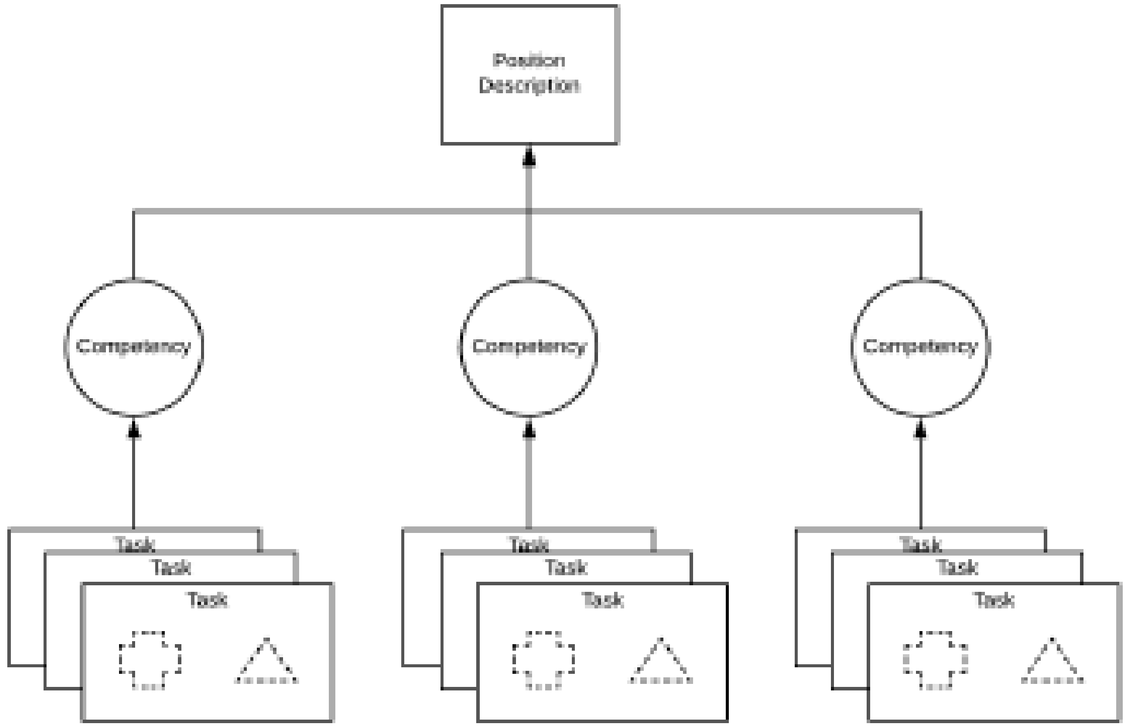


Figure 2. Using Competencies to Assess Learners through a Position Description

NICE Framework

COMPETENCIES

Other organizations could use Competencies to determine **whether a learner has achieved a defined set of Skills and Knowledge**. These organizations could, as depicted in Figure 3, choose to use Competencies as groups of K&S statements. These organizations could then assess the learners for these K&S statements. Assessments could take the form of **tests**, **lab-based demonstration**, or **oral evaluations**.

[Source: NIST Special Publication 800-181, Revision 1]

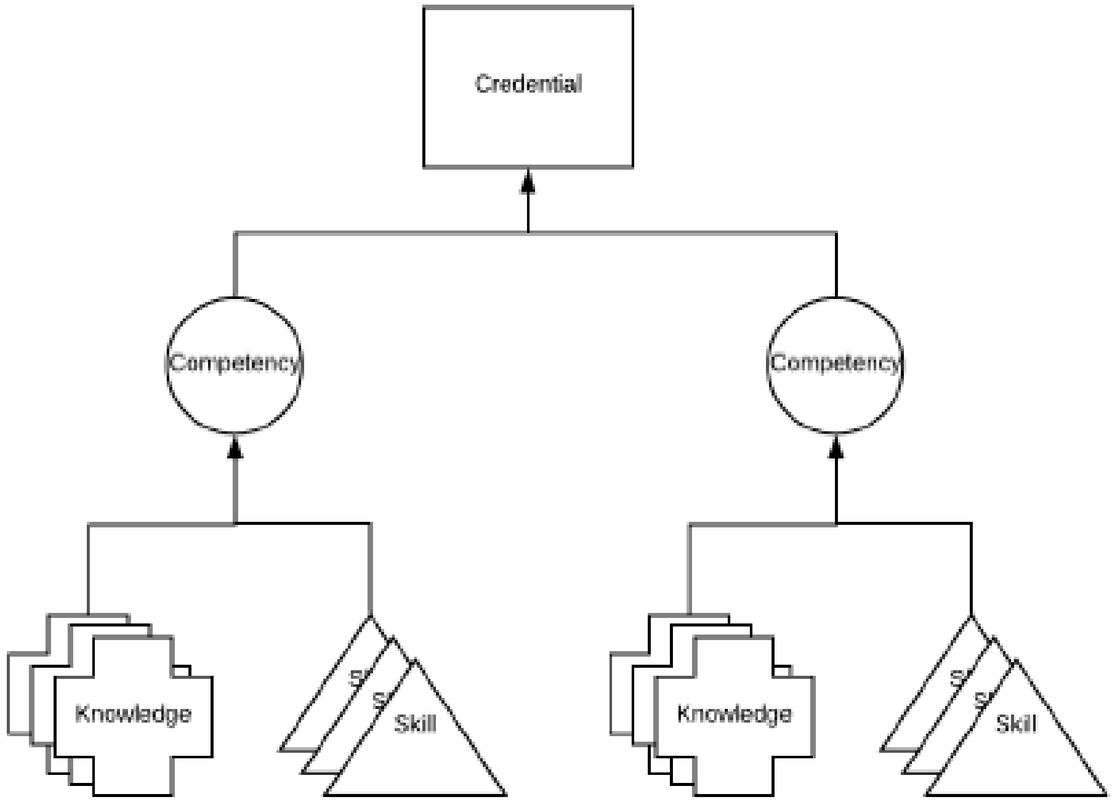


Figure 3. Using Competencies to Assess Learners through a Credential

NICE Framework

WORK ROLES

Work Roles

Work Roles are a *common use case* of the NICE Framework. Work Roles are a way of describing a grouping of work for which someone is responsible or accountable.

While previous workforce frameworks also associated Work Roles with Knowledge, Skill, and Ability specifications, the NICE Framework encourages a more agile approach through Tasks. Work Roles are composed of Tasks that constitute work to be done; Tasks include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks. This transitive approach, illustrated in Figure 3, *supports flexibility and simplifies communication*.

[Source: NIST Special Publication 800-181, Revision 1]

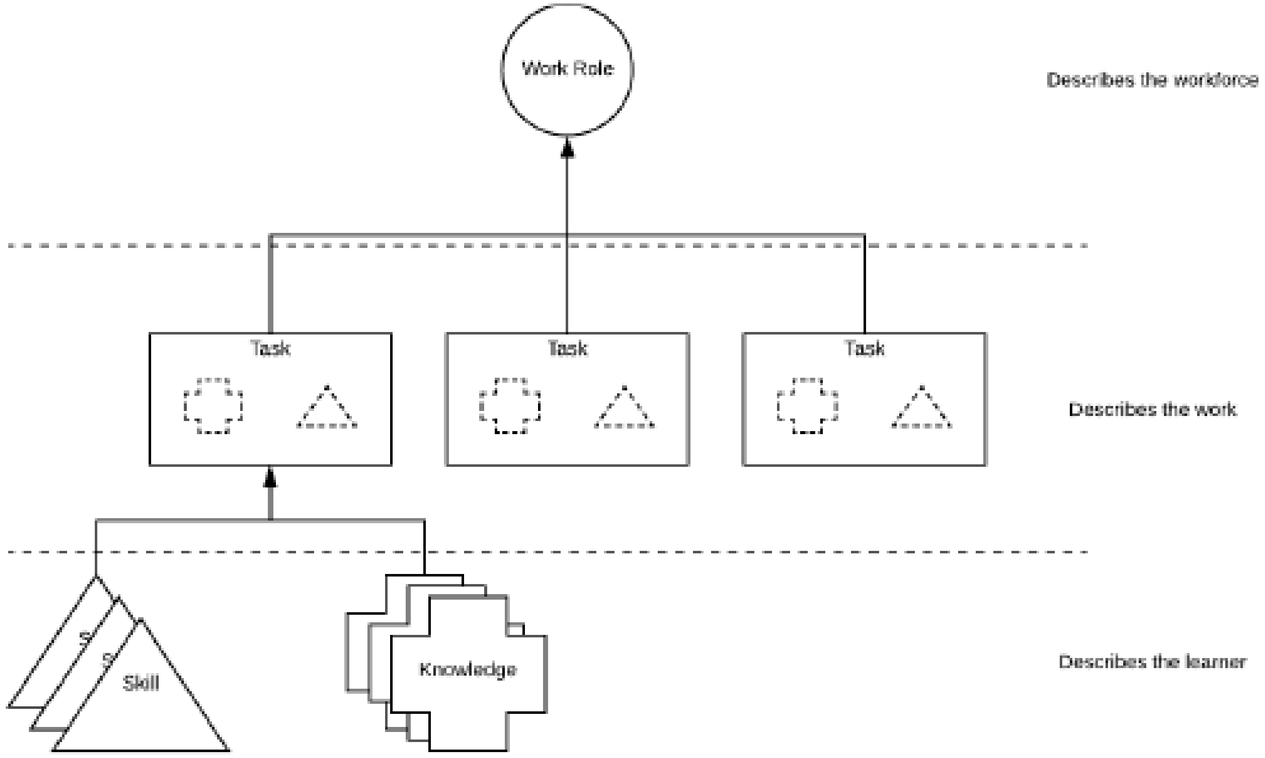


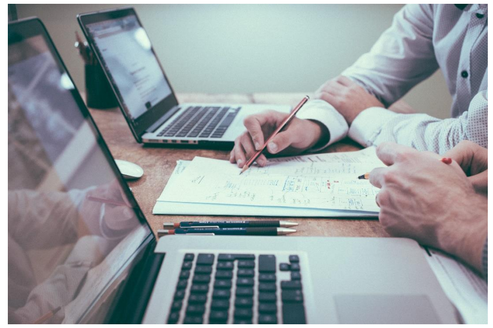
Figure 4 - Work Roles' Relationship to Building Blocks

NICE Framework

BUILDING TEAMS

Building Teams with Work Roles or Competencies

A **Work Role**-centered approach to building teams allows organizations to define what types of Work Roles are needed to achieve defined objectives. Since Work Roles are themselves made up of Competencies, this approach to building teams starts with the work to be completed. This approach may be considered "*top down*."



[Source: NIST Special Publication 800-181, Revision 1]

Teams can also be built using **Competencies**. This approach to building teams recognizes that individual Tasks may be unknown, but the types of Competencies needed to solve the challenge are known. This approach may be considered "*bottom up*." Therefore, teams built this way can help identify learners who may participate in the Team's work in the future. These learners may or may not be associated with a Work Role and simply possess the Competencies needed to help meet organizational objectives.

NICE Framework

CONCLUSIONS

Through the application of the building block approach described by the NICE Framework, users can benefit from a consistent method for *organizing and communicating the work to be done* via Task statements and the Knowledge and Skills of individual learners who support that work. The NICE Framework **helps guide the efforts of employers to describe cybersecurity work**, **education** and **training providers** to prepare cybersecurity workers, *and learners to demonstrate their capabilities to perform cybersecurity work*.

[Source: NIST Special Publication 800-181, Revision 1]

The ability to describe Tasks, Knowledge, and Skills is important to ensure a comprehensive understanding of the work and the workforce. The NICE Framework provides an *extensible* reference resource that can be applied and used by various organizations or sectors *to describe the work to be performed in many areas*.

Agid

‘LINEE GUIDA PER LA QUALITÀ DELLE COMPETENZE DIGITALI NELLE PROFESSIONALITÀ ICT’

AgID, acknowledging the provisions of the "*2014-2020 digital growth strategy* promotes the use of the e-CF 3.0 model and related profiles.

‘*LINEE GUIDA per la qualità delle competenze digitali nelle professionalità ICT*’ ('GUIDELINES for the quality of digital skills in ICT professionals‘) apply the e-CF framework and related concepts to the world of public procurement.

Agid

'LINEE GUIDA PER LA QUALITÀ DELLE COMPETENZE DIGITALI NELLE PROFESSIONALITÀ ICT'

Purpose

- Provide the administrations with indications on **how** to integrate the provision of professional services in the context of ICT service contracts.

- Provide cross-cutting information whenever it is necessary to deal with issues relating to the use of professionals.

- Make it possible to clearly identify the regulated ICT professional profiles with related skills and competences. Give suggestions and create a common lexicon to facilitate and simplify the relationship between public administration and suppliers.

Agid

'LINEE GUIDA PER LA QUALITÀ DELLE COMPETENZE DIGITALI NELLE PROFESSIONALITÀ ICT'

Advantages

An overall reference framework for public procurement of ICT services by administrations.

Quantitative methods to be applied to define quality measures and identify measurement processes, in order to provide concrete, pragmatic, immediately applicable indications, both to contracting administrations and to bidders.

Agid

'LINEE GUIDA PER LA QUALITÀ DELLE COMPETENZE DIGITALI NELLE PROFESSIONALITÀ ICT'

Adequate **clauses**, to be used in the negotiation phase, for the definition of specifications and public contracts for the supply of goods and services in the ICT sector, relating to the description of the activities to be contractually envisaged, to the products that these activities produce (contractual deliverables), quality indicators and measures to refer to both activities and products.

Clauses that are subsequently useful in the implementation phase of ICT contracts, for the necessary management of the contract and the monitoring to verify compliance with contractual requirements in terms of time, costs and work progress, expected quantity and quality of ICT services required.

Evolution and technical **standardization** of profiles according to the needs of the market to ensure the recognition of skills.

Some online resources

e-CF Explorer (interactive tool to explore the competences and the 30 ICT Professional Role Profiles identified by the European Committee for Standardization):

- https://ecfexplorer.itprofessionalism.org/

Workforce Framework for Cybersecurity (NICE Framework) :

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Agid guidelines and resources:

- https://www.agid.gov.it/it/agenzia/competenze-digitali

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
antonio.belli@unipd.it
simone.soderi@unipd.it

Thanks for your attention!

M8 Frameworks that describe the competencies