NIST Special Publication 800-181
Revision 1

Workforce Framework for Cybersecurity (NICE Framework)

Rodney Petersen
Danielle Santos
Matthew C. Smith
Karen A. Wetzel
Greg Witte

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181r1

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-181 Revision 1

Workforce Framework for Cybersecurity (NICE Framework)

Rodney Petersen (Director)
Danielle Santos (Manager of Communications and Operations)
Karen A. Wetzel (Manager of the NICE Framework)
National Initiative for Cybersecurity Education (NICE)
Applied Cybersecurity Division
Information Technology Laboratory

Matthew C. Smith
Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181r1

November 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-181
Natl. Inst. Stand. Technol. Spec. Publ. 800-181 Rev. 1, 27 pages (November 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181r1

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: NICEFramework@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

Abstract

This publication from the National Initiative for Cybersecurity Education (NICE) describes the Workforce Framework for Cybersecurity (NICE Framework), 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. 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

Competency; cybersecurity; cyberspace; education; knowledge; role; security; skill; task; team; training; workforce; work role.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Document Conventions

The terms "shall" and "shall not" indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted. The terms "should" and "should not" indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms "may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical or causal.

Throughout the NICE Framework, those performing cybersecurity work—including students, job seekers, and employees—are referenced as Learners. This moniker highlights that each member of the workforce is also a lifelong learner.

Acknowledgments

The NICE Framework was developed by a Core Authoring Team that includes representatives from numerous departments and agencies in the United States federal government. The National Institute of Standards and Technology wishes to acknowledge and thank these team members whose dedicated efforts contributed significantly to the publication:

William Newhouse, National Institute of Standards and Technology
Pam Frugoli, Department of Labor
Lisa Dorr, Department of Homeland Security
Kenneth Vrooman, Cybersecurity and Infrastructure Security Agency
Bobbie Sanders, Department of Defense
Patrick Johnson, Department of Defense
Matt Isnor, Department of Defense
Stephanie Shively, Department of Defense
Ryan Farr, Department of Defense

The authors and the Core Authoring Team gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. The authors particularly appreciate the many helpful responses to the NICE Framework Request for Comments and to the public comment draft of this publication.

Additionally, the team appreciates and acknowledges the contributions of those who established previous editions of national cybersecurity workforce frameworks as described at the History page of the NICE Framework Resource Center. [1]

Note to Readers

Welcome to the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework), Revision 1. The NICE Program Office staff have received significant feedback from the community, including many responses to a recent request for general comments regarding the NICE Framework and also responses to the public draft of this publication. In light of that feedback and the fast-paced and connected ecosystem of cybersecurity, the authoring team decided to adopt and promote attributes of agility, flexibility, interoperability, and modularity. These attributes led to a refactoring of the NICE Framework to provide a streamlined approach for developing a workforce to manage cybersecurity risk. Below is a summary of changes:

- Organizing constructs in Revision 1 have been simplified by deprecating Categories (e.g., securely provision, oversee and govern, protect and defend, analyze, etc.) and Specialty Areas (e.g., incident response, threat analysis, cybersecurity management, etc.). In order to simplify an approach that offers agility, flexibility, interoperability, and modularity for organizations, Revision 1 presents a streamlined set of "building blocks" comprised of Tasks, Knowledge, and Skills. Organizations that find value in the former Categories and Specialty Areas can continue to use them or create teams around those concepts and align them with this version of the NICE Framework (see Section 3.4).
- Revision 1 describes several uses of Tasks, Knowledge, and Skills, including methods of applying those in the creation of Work Roles. Users of the Work Roles described in the original NIST SP 800-181 may continue to use those; updates to those may be published by NICE in the future. [2]

The relationships among Tasks, Knowledge, Skills, and Abilities have changed. Skill and Ability statements from the previous version have been refactored for simplicity into Skill statements, which focus on the action of the learner. This revision describes methods for associating Knowledge and Skill statements with Task statements for various outcomes. The lists of Tasks, Knowledge, Skills, and Work Roles that were previously available in Appendices A and B of the 2017 Framework have been removed from this version in order to simplify the maintenance of the NICE Framework and to ease updates to those lists. The Task, Knowledge, and Skills (TKS) statements and corresponding Competencies and Work Roles will be maintained as separate artifacts and will be subject to ongoing review and updates with a defined change process and indication of version control to manage and communicate changes. Until those updates occur, the earlier versions of these lists will remain available to users in the NICE Framework Resource Center. In support of interoperability and modularity, future updates will ensure that the statements match the final definitions of TKS statements noted here.

- For readers interested in mapping standards, references, or resources to the NICE Framework, NICE is working with the Online Informative Reference (OLIR) Program to develop templates for these mappings. The OLIR Program, managed by NIST, provides a process for aligning references to NIST documents. Additionally, the program provides a catalog of those references. [3]

Executive Summary

Each of us—individually and organizationally—performs important work that provides a contribution to society. However, as information and technology, including many evolving types of operational technology, grow increasingly complex and interconnected it can be difficult to clearly describe the work that is being performed or that we desire to accomplish, in these areas in particular. The National Initiative for Cybersecurity Education (NICE) recognizes that those performing cybersecurity work—including students, job seekers, and employees— are lifelong learners throughout their efforts to emphasize and address cybersecurity implications across many domains. This segment of people is referenced in this document both as "Learners" and at times as the "cybersecurity workforce", though the latter is not meant to imply that the work roles and content included in the NICE Framework apply only to those fully embedded in the cybersecurity domain. The tasks that these learners perform are further referenced here as "cybersecurity work", and the Framework provides a means to describing that work with precision to support learner education or training and in the recruitment, hiring, development, and retention of employees. The NICE Framework has been developed to help provide a reference taxonomy—that is, a common language—of the cybersecurity work and of the individuals who carry out that work. The NICE Framework supports the NICE mission to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development. The 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. This development, in turn, benefits employers and employees through the identification of career pathways that document how to prepare for cybersecurity work using the data of Task, Knowledge, and Skill (TKS) statements bundled into Work Roles and Competencies.

The use of common terms and language helps to organize and communicate the work to be done and the attributes of those that are qualified to perform that work. In this way, the NICE Framework helps to simplify communications and provide focus on the tasks at hand. Finally, use of the NICE Framework improves clarity and consistency at all organizational levels—from an individual to a technology system to a program, organization, sector, state, or nation.

Table of Contents

1 Background

Technology continues to evolve at an ever-increasing pace. Specifically, the technology which facilitates the ability to access and process information quickly and efficiently is dramatically changing. The work required to design, build, secure, and implement these data, networks, and systems increases in complexity. Furthermore, describing this work and those who can perform the work remains a challenge. Compounding this problem, organizations use varying and self-created methods to attempt to solve the challenge.

This publication from the National Initiative for Cybersecurity Education (NICE) describes the Workforce Framework for Cybersecurity (NICE Framework). The NICE Framework helps organizations overcome the barrier of describing their workforce to multiple stakeholders by presenting a building block approach. Through the use of conceptual building blocks, the NICE Framework presents a common language for organizations to use internally and with others. This approach allows organizations to tailor and implement the NICE Framework to their unique operating context. Furthermore, by creating a common language, the NICE Framework lowers the barrier to entry for organizations seeking to enter and interoperate with other organizations.

Figure 1, below, depicts a high-level view of the NICE Framework. The main building blocks of the NICE Framework are Tasks, Knowledge, and Skills (TKS) statements (explained in Section 2) that are shown alongside the concepts they describe. Figure 1 shows that there are two main types of concepts being described: “the work” and “the learner.” Notably, those who are (or will be) performing work (e.g., students, current employees, or job seekers) are continually learning and achieving objectives and can be found in any part of the learning lifecycle. The NICE Framework attempts to describe both “the work” and “the learner” in generic terms that can be applied to all organizations.

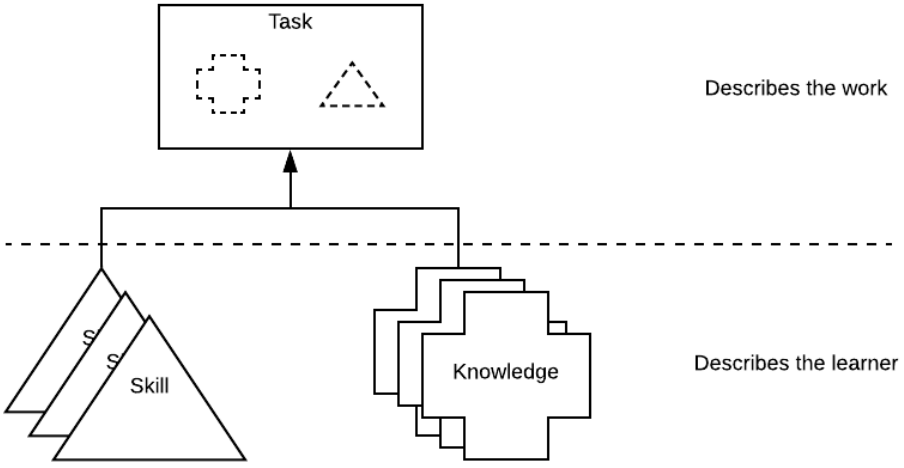

Figure 1 - NICE Framework Building Blocks Approach

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.

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.

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.

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.

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.

1.1 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. 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.

- **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).

1.2 Purpose and Applicability

Organizations manage many different business functions (such as operations, finance, legal, and human resources) as part of their overall enterprise. Each of these business functions has associated risks. As technology has become an enabling factor in managing an enterprise, the risks associated with cybersecurity have also become more prominent. The NICE Framework assists organizations with managing cybersecurity risks by providing a way to discuss the work and learners associated with cybersecurity. These cybersecurity risks are an important input into enterprise risk decisions as described in NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. [4]

This document serves as a potential guide for other business functions that are considering the creation of workforce frameworks. Organizations can increase efficiency by using the same building blocks across various business functions. Therefore, any organization can leverage this document.

1.3 Audience

The topic of managing a workforce for cybersecurity involves many different types of positions, as well as many different types of organizations. The audience of this document includes public sector agencies, private and not-for-profit organizations, education and training providers, curriculum developers, credential providers, human resource professionals, hiring managers, line managers, workforce planners, recruiters, and all learners.

1.4 Organization of this Publication

The remainder of this Special Publication is organized as follows:

- Section 2, NICE Framework Building Blocks: Defines the TKS building block components of the NICE Framework
- Section 3, Using the NICE Framework: Describes common approaches to using the NICE Framework
- Section 4, Conclusion
- References: A list of related publications referenced in this paper
- Appendix A, Acronyms: A list of acronyms and abbreviations used in this publication

2 NICE Framework Building Blocks

The Workforce Framework for Cybersecurity (NICE Framework) is built upon a set of discrete building blocks that describe the work to be done (in the form of Tasks) and what is required to perform that work (through Knowledge and Skills). These building blocks are organizing constructs that support the usability and implementation of the NICE Framework. They provide a mechanism by which both organizations and individuals can understand the scope and content of the NICE Framework. These building blocks are meant to be guidelines that can be used to enhance comprehension rather than rigid structures.

2.1 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.

Task
An activity that is directed toward the achievement of organizational objectives.

Task Statements

- Easy to read and understand
- Begin with the activity being executed
- Do not contain the task objective

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, as with the example below, the statement itself is easy to read and understand.

A Task statement begins with the activity being executed.

> Example: **Troubleshoot** system hardware and software.

A Task statement does not contain the objective within the statement, as objective may vary based on mission drivers and organizational needs.

> Example: Conduct interactive training exercises.

In the above example, the purpose of these exercises may be to create an effective learning environment, but that goal is not included in the Task statement itself.

As Figure 1 shows, Tasks are related to K&S statements. A learner will demonstrate that they possess the knowledge and skills to complete a Task (or will be challenged to gain the knowledge and learn the skill to prepare to complete the task.) The complexity within a Task is explained by the associated K&S statements. In the troubleshooting example above, in order to effectively troubleshoot any piece of software or hardware, the learner should be familiar with and understand the related Knowledge statements. The same can be said for Skill statements.

2.2 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.

Knowledge
A retrievable set of concepts within memory.

Knowledge Statements

- Describe foundational or specific Knowledge
- Multiple statements may be needed to complete a Task
- A single statement may be used to complete many different Tasks

Knowledge statements can be foundational.

> Example: Knowledge of cyberspace threats and vulnerabilities.

Knowledge statements can be specific.

> Example: Knowledge of vulnerability information dissemination sources (e.g., vendor alerts, government advisories, product literature errata, and sector bulletins).

Organizations developing Knowledge statements should consider the learners' different levels of knowledge and expertise. An example of these various levels is described in Bloom's Taxonomy (Revised) which uses language that facilitates observability and assessment of the learner. [5]

2.3 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.

Skill
The capacity to perform an observable action.

Skill Statements

- Describe straightforward or complex skills
- Multiple Skill statements may be needed to complete a Task
- A single Skill statement may be used to complete more than one Task

Skill statements can be simple.

> Example: Skill in recognizing the alerts of an Intrusion Detection System

Skill statements can be complex.

> Example: Skill in generating a hypothesis as to how a threat actor circumvented the Intrusion Detection System.

As depicted in Figure 1, Skill statements describe what the learner can do, and Task statements describe the work to be done. Therefore, it is important to separate the language used between Skill statements and Task statements and to use terms that facilitate observability and assessment of the learner.

3 Using the NICE Framework

Notably, while the Workforce Framework for Cybersecurity (NICE Framework) is intended to provide a common set of building blocks from which many can draw, some organizations will find the need to tailor the model to align more closely with their unique context. For example, a manufacturer may have sector- or organization-specific Tasks that are not described in the NICE Framework. Others may find that the Tasks are applicable but need to adjust or develop specific K&S statements in order to increase the likelihood that the Tasks can be completed as defined by their unique context. As such, these building blocks are not intended to be rigid; instead, they are meant to provide a common language for organizations or sectors to use in ways that are beneficial to a given context.

Finally, example uses of the NICE Framework building blocks provided below are notional or conceptual in nature; an organization may use the building blocks in any number of ways to best meet local needs. These examples here are meant to illustrate potential practical approaches to the NICE Framework that have been shown to help achieve common organizational objectives. They provide guidance to organizations or sectors seeking a place to start rather than a singular way to use the NICE Framework.

3.1 Using Existing Task, Knowledge, and Skill (TKS) Statements

Users of the NICE Framework reference one or more Task, Knowledge, and Skill statements (TKS statements), as described in Section 2, to describe both work and learners. Task statements are used to describe the work. Task statements have associated K&S statements. Although a Task statement may have a recommended set of associated K&S statements, users may include other existing K&S statements to tailor Tasks for their unique context. K&S statements are used to describe learners. K&S statements can be used in many ways to manage the cybersecurity workforce. They can be used in part, all together, or not at all, depending on the implementing organization’s unique context. The notional examples of use below demonstrate areas where TKS statements might be implemented:

- Employee Skill tracking program to determine promotion qualifications
- Required Knowledge for completion of a course
- Weekly Task list for completion at an organization

TKS statements and examples can be found in the NICE Framework Resource Center and will be updated, as needed, to keep pace with changes resulting from evolving business missions, risks, or emerging technologies. [1]

3.2 Creating New TKS Statements

Users are cautioned against modifying the text in existing NICE Framework TKS statements. The statements are intended to support interoperability so changing their content may result in subsequent misalignment when using outside sources. If different wording is needed in a TKS statement to support a user’s unique context a new statement can be created.

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.

3.3 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.

Competency
A mechanism for organizations to assess learners.

Competencies are
- Defined via an employer-driven approach
- Learner-focused
- Observable and measurable

Competencies offer flexibility by allowing organizations to group together various TKS statements into an overarching category that defines a broad need. While an individual Task and its associated Knowledge and Skill statements may not change, the more broadly defined Competency may introduce new Tasks or even individual Knowledge and Skills — or remove existing ones — in response to shifting needs in a changing cybersecurity ecosystem.

There are various ways that Competencies could be used. For example, as depicted in Figure 2, an organization could use Competencies as part of the hiring process aimed at fulfilling specific organizational goals. In this case, the Competencies could be defined as a group of related Tasks statements. The organization could then use these Competencies to assess whether a candidate can perform those Tasks. This assessment could take the form of an interview, pre-employment test, or work-based learning observation.

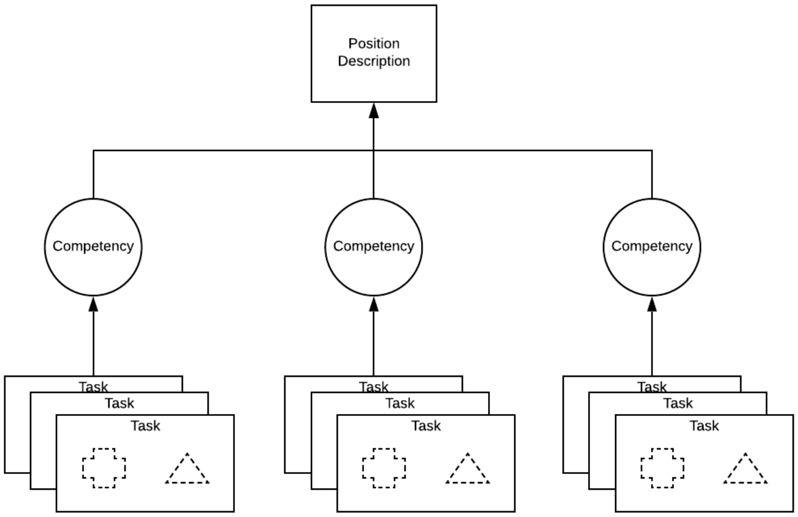

Figure 2. Using Competencies to Assess Learners through a Position Description

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.

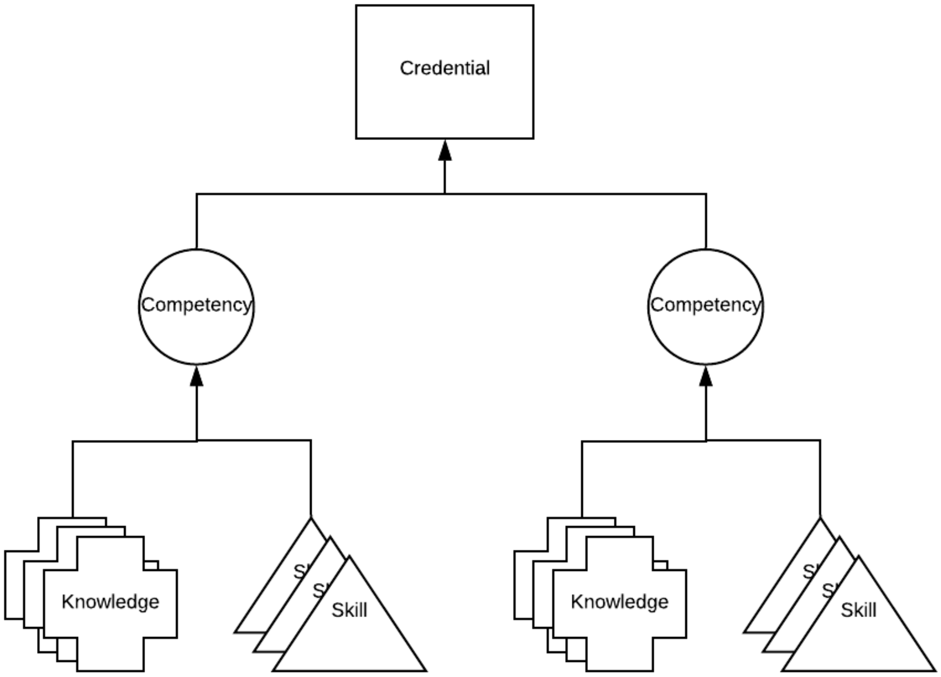

Figure 3. Using Competencies to Assess Learners through a Credential

The above examples are meant to be notional. They can be used in part, all together, or not at all, depending on the implementing organization's unique context.

3.3.1 Using Existing Competencies

The NICE Framework Competencies are a way for organizations to align with the NICE Framework at a high level without delving into the details of TKS statements. Competencies are a way to describe the assessment of a learner. By enabling organization-defined groups of TKS statements, Competencies enable organizations to succinctly communicate and effectively organize their cybersecurity work in order to provide a streamlined view of the workforce. Other potential uses of Competencies include to:

- Describe types of Tasks within a given position
- Track workforce capabilities
- Describe team requirements
- Demonstrate learner capabilities

Although a Competency has a recommended set of associated TKS statements, users could add or remove existing statements to tailor Competencies for their unique context. However, users are cautioned against modifying the title or description of an existing NICE Framework Competency. Competencies are intended to support interoperability so changing their content may result in subsequent misalignment when using outside sources. If different wording is needed in a Competency to support a user's unique context a new Competency can be created as described below (see Section 3.3.2).

3.3.2 Creating New Competencies

Some organizations may need to describe a Competency for the specific context of their cybersecurity work. The NICE Framework, developed with the principle of agility, allows organizations to describe a Competency to meet a changing cybersecurity ecosystem. This could be done by altering an existing Competency to meet local needs or creating an entirely new competency.

Two notional examples are provided below to explain potential processes for using Competencies. The two examples focus on Data Analysis to show that the same Competency can be utilized through different approaches. Additionally, these examples elaborate on Figure 2 and Figure 3 to ground the reader in a potential implementation. These examples use a table structure to communicate the Competency. This tabular approach is one of many that could be used by an organization seeking to implement Competencies.

Data Analysis Example 1

Table 1, below, is informative and provides a starting point for building a Competency. The Data Analysis Example 1 Competency has a name and a description that quickly allows the organization to identify a Competency as one that has value to their organizational structure and context. Using the assessment method of "lab-based demonstration" the organization is assessing a learner by providing a simulated work environment to complete the Tasks which meet their business objectives. (Note that Table 1 uses Tasks from the 2017 version of the NICE Framework. [2])

Table 1 – Example of Creating A New Data Analysis Competency with Existing NICE Framework 2017 Tasks

Competency Name: Data Analysis Example 1
Competency Description: The collecting, synthesizing, or analyzing qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence.
Assessment Method: Lab-based demonstration
Task Statements
T0007 | Analyze and define data requirements and specifications.

T0405 | Utilize open source language such as R and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line).

In the example described in Table 1, an organization may give a learner a computer loaded with a particular data set and connected to the lab network. The learner is then given time to demonstrate their ability to use open source languages to apply quantitative techniques to the data. A key portion of this assessment may be to analyze the data set to ensure the data meets a specific data specification before completing the analysis. Through this assessment the learner demonstrates the Competency of "Data Analysis Example 1" as defined by the employer.

A fully detailed Competency of Data Analysis could be much larger. By enumerating the Task statements within the Competency the organization can specify the desired scope of the Competency. For ease of use, Tasks are referenced with their NICE Framework 2017 Task IDs.

Data Analysis Example 2

Table 2, below, demonstrates another starting point for creating a Competency. The example is informative; the description is the same as Table 1, however, this example uses Knowledge and Skill statements to build the Competency.

Table 2 - Example of Creating A New Data Analysis Competency With Additional Tasks

Competency Name: Data Analysis Example 2
Competency Description: The collecting, synthesizing, or analyzing of qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence.
Assessment Method: Test
K&S Statements
S0013 |Skill in conducting queries and developing algorithms to analyze data structures.
S0021 | Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data).
S0091 | Skill in analyzing volatile data.
K0020 | Knowledge of data administration and data standardization policies.
K0338 | Knowledge of data mining techniques.

In this example, Table 2 represents a Data Analysis Competency. This Competency could be created by a certification body that provides a test to assess learners. The test could be administered in paper form or computer-based format. By passing the test, the learner demonstrates the Competency of "Data Analysis Example 2" as defined by the certification body.

(Note that Table 2 uses K&S statements from the 2017 version of the NICE Framework. [2])

3.4 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.

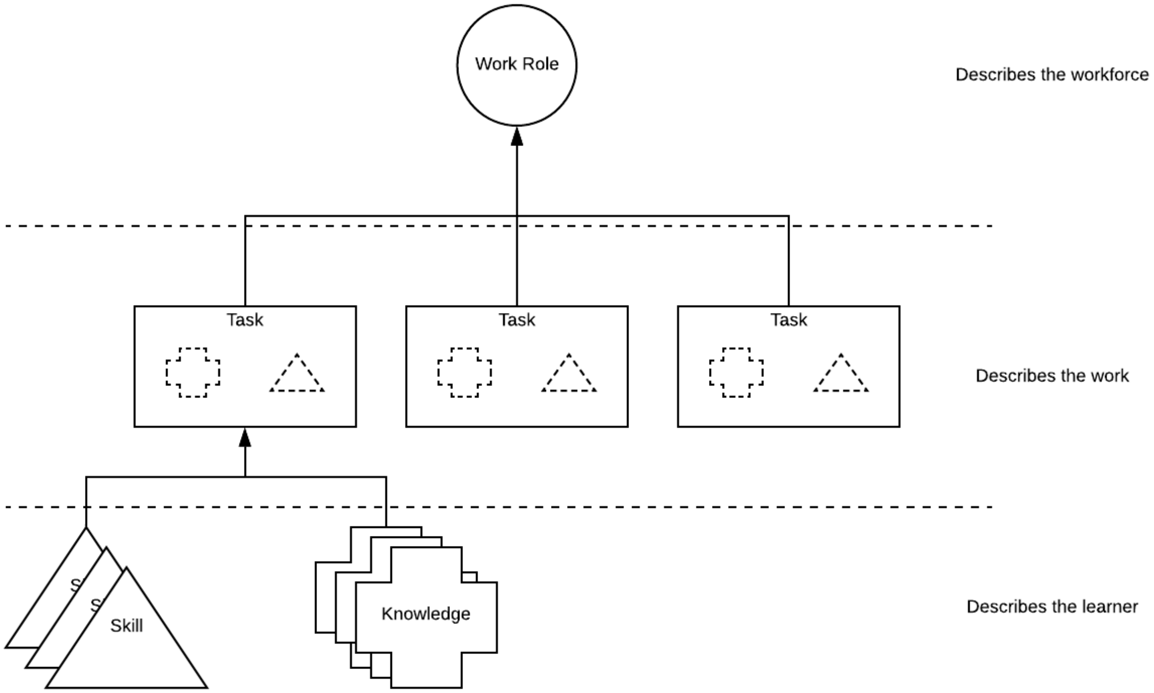

Figure 4 - Work Roles' Relationship to Building Blocks

Work Role names are not synonymous with job titles. Some Work Roles may coincide with a job title depending on an organization's use of job titles. Additionally, Work Roles are not synonymous with occupations.

A single Work Role (e.g., Software Developer) may apply to those with many varying job titles (e.g., software engineer, coder, application developer). Conversely, multiple roles could be combined to create a particular job. This additive approach supports improved modularity and illustrates the fact that all learners in the workforce perform numerous tasks in various roles, regardless of their job titles. Similarly, the NICE Framework does not define proficiency levels (e.g., Basic, Intermediate, Advanced). Such attributes, and those regarding the proficiency with which a learner performs Tasks, are left to other models or resources.

3.4.1 Using Existing Work Roles

Each Work Role is intended to support the achievement of objectives through Tasks. Although a Work Role may have a predetermined set of associated Tasks, users may include other existing Tasks to tailor Work Roles for their unique context. Similarly, a user may wish to draw from the listed Work Roles or add additional ones to support additional objectives. The current set of NICE Framework components is available from the NICE Framework Resource Center. [1]

Users are cautioned against internally modifying the name and description of an existing Work Role. The Work Roles are intended to support interoperability so changing their content may result in subsequent misalignment. If different wording is needed, a new Work Role can be created as described below.

3.4.2 Creating a New Work Role

Users may also create new Work Roles to help tailor the use of the NICE Framework for their unique context. Such additional Work Roles will help support clear and consistent internal discussions regarding the cybersecurity work.

3.5 Teams

Many organizations use teams to collectively tackle complex challenges by bringing together individuals with complementary skills and experience. By utilizing different resources and perspectives, teams allow organizations to manage risks holistically. Teams take advantage of each member's specialization of knowledge and processes to effectively distribute work. Teams can be defined using Work Roles or Competencies.

3.5.1 Building Teams with Work Roles

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."

Table 3 - Example of a Secure Software Development Team Using the NICE Framework 2017 Work Roles

Lifecycle Phase	Work Role
Design	SP-ARC-002 | Security Architect
Build	SP-DEV-001 | Software Developer
Deploy	OM-NET-001 | Network Operations Specialist
Operate	OM-STS-001 | Technical Support Specialist
Maintain	OM-DTA-001 | Database Administrator
Decommission	OV-LGA-001 | Cyber Legal Advisor

Table 3, above, demonstrates a way of creating a secure software development Team. The Work Roles are referenced using the 2017 version of the NICE Framework Work Role IDs. Teams built this way begin with the identification of the work that needs to be accomplished. In this example, the secure software development team is organized by lifecycle phase. The first row illustrates that the team would consider objectives of the Design phase including planning, and thus would need a Security Architect. Table 3 is an informative example and does not cover all the Work Roles that may be present or needed for a given Team. For more information, see NIST's *Secure Software Development Framework*. [6]

Table 4 - Example Creating A Cybersecurity Team Using NICE Framework 2017 Work Roles and New Work Roles

Cybersecurity Framework Function	Work Role
Identify	NewWorkRole1 | Risk Manager
Protect	SP-RSK-002 | Security Control Assessor
Detect	PR-CDA-001 | Cyber Defense Analyst
Respond	PR-CIR-001|Cyber Defense Incident Responder
Recover	NewWorkRole2 | Communications Specialist

Table 4 describes an example cybersecurity Team. Similar to the secure software development team, the example team is built with a work-centered approach. By using the Core of the *Framework for Improving Critical Infrastructure Cybersecurity* (*Cybersecurity Framework*), cybersecurity objectives are selected, Tasks are identified to achieve those objectives, and Work Roles are selected to define the roles necessary to support those objectives. [7] Table 4 is an informative example and does not cover all Work Roles which may be present or required for a given Team. Two new Work Roles are added to show a mixed approach of using existing Work Roles (Section 3.4.1) and creating new Work Roles (Section 3.4.2). By creating new Work Roles the example demonstrates a flexible and agile approach to the tailoring of the NICE Framework.

3.5.2 Building Teams with Competencies

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.

For example, a defensive cybersecurity team that uses its skills to imitate adversaries' attack techniques (i.e., a "Red Team") may be composed of the following notional Competencies:

- Engagement Planning
- Rules of Engagement
- Pen Testing
- Data Collection
- Vulnerability Exploitation

By creating teams or other TKS groupings, each organization can tailor the NICE Framework in ways that best help to apply and communicate about the learners (and the work that those learners will perform) to enable achievement of mission objectives.

4 Conclusion

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.

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. The benefits to these organizations support the NICE mission of energizing, promoting, and coordinating a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

References

[1] National Initiative for Cybersecurity Education (2020) *NICE Framework Resource Center*. Available at https://www.nist.gov/nice/framework

[2] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

[3] National Institute of Standards and Technology (2020) *National Online Informative References Program*. Available at https://csrc.nist.gov/projects/olir

[4] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[5] Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory Into Practice*, 41(4), 212-218. Available at https://www.depauw.edu/files/resources/krathwohl.pdf

[6] Dodson DF, Souppaya MP, Scarfone KA (2020) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.04232020

[7] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
ITL	NIST Information Technology Laboratory
K&S	Knowledge and Skill statement(s)
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OLIR	Online Informative Reference
OMB	Office of Management and Budget
SSDF	Secure Software Development Framework
TKS	Task, Knowledge, and Skill statements

Appendix B—Glossary

For a complete glossary, please visit https://csrc.nist.gov/glossary.

Competency A mechanism for organizations to assess learners.

Knowledge A retrievable set of concepts within memory.

Skill The capacity to perform an observable action.

Task An activity that is directed toward the achievement of organizational objectives.