Draft NIST Special Publication 800-181
Revision 1

Workforce Framework for Cybersecurity (NICE Framework)

Rodney Petersen
Danielle Santos
Matthew Smith
Greg Witte

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

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

Draft NIST Special Publication 800-181 Revision 1

Workforce Framework for Cybersecurity (NICE Framework)

Rodney Petersen (Director)
Danielle Santos (Program Manager)
National Initiative for Cybersecurity Education (NICE)
Applied Cybersecurity Division
Information Technology Laboratory

Matthew 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-draft

July 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, 23 pages (July 2020)
CODEN: NSPUE2

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

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.

Public comment period: July 15, 2020 through August 28, 2020

Email: NICEFramework@nist.gov

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

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication 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 defines Work Roles that perform those tasks. It also describes Knowledge and Skill statements that provide the foundation for lifelong learners to accomplish tasks. Additionally, Competencies are introduced as a way to further describe learners (employees, job seekers, and students) by grouping sets of knowledge and skills. 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.

Supplemental Content

A Reference Spreadsheet for the original NICE Framework is available at https://www.nist.gov/file/372581.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: NICEFramework@nist.gov

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.

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
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. Additionally, the authors would like to acknowledge the work of the authors of the original SP 800-181 Cybersecurity Workforce Framework: William Newhouse of NIST; Stephanie Keith of the U.S. Department of Defense; and Benjamin Scribner of the U.S. Department of Homeland Security.

The first NICE Framework was posted for public comment in September 2012 and published as final in April 2013 as the National Cybersecurity Workforce Framework version 1.0 [1]. The authors recognize Dr. Jane Homeyer, Anne Quigley, Rex Min, Noel Kyle, Maya Yankelevich, and Peggy Maxson for leading its development, along with Montana Williams and Roy Burgess for their leadership in the development of National Cybersecurity Workforce Framework version 2.0 which was posted in April 2014 [2].

Note to Reviewers

Welcome to the National Initiative for Cybersecurity (NICE) Workforce Framework for Cybersecurity (NICE Framework), Revision 1 draft. The NICE Program Office staff have received significant feedback from the community including through many responses to a recent Request for Comments. 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 managing the workforce. 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 Knowledge, Skills, and Tasks as well as Work Roles. Organizations that find value in the former Categories and Specialty areas can create "Teams" around those concepts and align them with this version of the NICE Framework (See Section 3.4).
- The relationships among Knowledge, Skill, and Abilities and Tasks 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. Knowledge and Skill statements can then associate with Task Statements.
- The "lists" of Knowledge, Skill, Task, and Work Roles have been removed from the document. This helps to separate the maintenance of the NICE Framework from the content itself. In support of agility and flexibility, the Task, Knowledge, and Skill (TKS) Statements and list of Work Roles are currently under development. NICE expects to provide an additional resource in the future, possibly to include some options for grouping of Work Roles, and will request public comment at that time.
- Many of the resources (e.g., the supplemental spreadsheet, KSAs, Work Roles, Online Informative Reference catalog entries) from the original NICE Cybersecurity Workforce Framework are being updated based on feedback received and other lessons learned. In support of interoperability and modularity, forthcoming work will update these statements to match the final definitions of TKS Statements noted here.

Questions to the Reviewer:

- Users may want "NICE approved" TKS, Work Roles, and Competencies. What is a recommended way to develop and manage such a list? Does it make sense that NICE could prescribe aspects of the NICE Framework without knowing an organization's structure and mission?
- The current definition of Competency within the NICE Framework is one of many used in the community. Does this definition and formulation help clarify and specify workforce management?
- The current draft does not address "proficiency" in a Work Role (e.g., Entry-, Intermediate-, or Advanced-Level). Is this concept needed in the NICE Framework or best left to users or to be explored in a corresponding publication (e.g., NISTIR)?

Executive Summary

Each of us—individually and organizationally—performs important work that provides a contribution to society. However, it is often difficult, to clearly describe the work that one is performing or desires to accomplish. Information and technology, including many evolving types of operational technology, grow increasingly complex and interconnected every day. The National Initiative for Cybersecurity Education (NICE) recognizes that the participants in that evolution are lifelong learners, from their first day in a classroom to long after their retirement party, and that there is a segment of learners that are responsible for maintaining confidentiality, integrity, and availability objectives. In this publication, that segment is referenced as the cybersecurity workforce and the tasks that they perform are referenced as the cybersecurity work. There is value in describing that work with precision when recruiting, hiring, developing, and retaining employees or contractors.

The NICE Framework has been developed by to help provide a reference taxonomy of the cybersecurity work and of the individuals who carry out that work. The NICE Framework supports the NICE mission to energize and promote a robust network and an 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 helps learners to explore cybersecurity work and to connect with initiatives 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 TKS Statements bundled into Work Roles and Competencies.

There are numerous benefits to both individuals and organizational entities from applying such a framework. 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, such as for cybersecurity work to be accomplished. 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 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 help solve this definition challenge. Thus, communication among organizations regarding security initiatives and the people who perform them remains difficult.

The Workforce Framework for Cybersecurity (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, Skills (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.” The NICE Framework attempts to describe both of these in generic terms that can be applied to all organizations.

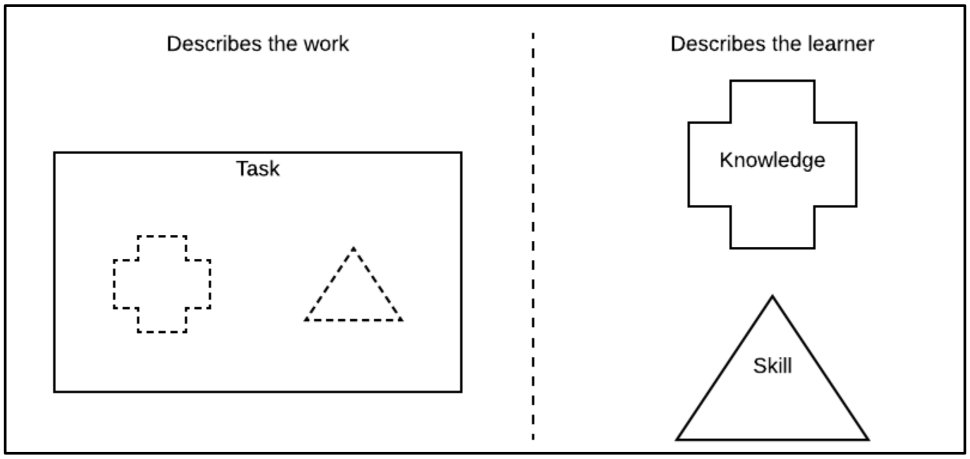

Figure 1 - NICE Framework Approach

The “work” is what an organization executes on a daily basis. 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 carries out the Task. It is important to remember that all people are constantly learning and achieving objectives. These objectives can be better management skills, more in-depth technical knowledge, or other Knowledge or Skills. Therefore, “learners” can be any part of the learning lifecycle such as students, current employees, or job seekers. The NICE Framework provides organizations a way to describe "learners" by associating Knowledge and Skill statements that enable task completion.

By describing both the "work" and the "learner," the NICE Framework provides organizations a common language to describe their cybersecurity work. Furthermore, the NICE Framework provides a mechanism to communicate across organizations at a peer level, sector 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 that will carry out the work, and the ongoing learning that will be needed. The nature of the work, and consequently the workforce, can be described using the 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, Artificial Intelligence).

1.2 Purpose and Applicability

Organizations manage many different business functions such as operations, finance, legal, human resources, etc., 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)*. [3]

This document serves as a potential guideline for other business functions that are considering the creation of Workforce Frameworks. By using the same building blocks across various business functions, organizations can increase efficiency. 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 is: public sector agencies, private companies, academia, hiring managers, line managers, workforce planners, curriculum developers, credential providers, recruiters, and all learners.

1.4 Organization of this Publication

The remainder of this special publication is organized as follows:

- Chapter 2 defines the building block components (Tasks, Knowledge, and Skills) of the NICE Framework,
- Chapter 3 describes common uses of the NICE Framework,
- A list of References to publications related to this publication is included after Chapter 3, and
- Appendix A provides a list of abbreviations and acronyms used in this publication.

2 NICE Framework Components

The Workforce Framework for Cybersecurity (NICE Framework) is built upon a set of discrete components that describe the work to be done (in the form of Tasks) and the learners who perform that work (through Knowledge and Skills).

2.1 Task Statements

Task: an activity that is directed toward the achievement of objectives.

As depicted in Figure 1, Task statements describe the work, and Skill statements describe the learner. Therefore, it is important to distinguish the language used between Skill statements and Task statements. 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.

Tasks describe work to be completed. The objectives of this work can be 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 Task statement.

> Example: Conduct interactive training exercises ~~to create an effective learning environment.~~

As Figure 1 depicts, Tasks are related to Knowledge and Skill (K&S) statements. A learner will demonstrate that they possess the knowledge and skill to complete a task or 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&Ss. 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: a retrievable set of concepts within memory.

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).

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. There may be multiple Knowledge statements that are needed to complete a given Task. Likewise, one Knowledge statement may be used to complete many different Tasks.

2.3 Skill Statements

Skill: the capacity to perform an observable action.

Skill statements can be straightforward.

> Example: Recognize the alerts of an Intrusion Detection System

Skill statements can be complex.

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

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. There may be multiple Skill statements that are needed to complete a given Task. Likewise, exercising a skill may be used to complete more than one Task.

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. Skill statements should use language such as that which is outlined in Bloom's Taxonomy (Revised) because it facilitates observability and assessment of the learner. [4]

3 Using the NICE Framework Building Blocks

3.1 Applying 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, many 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 that increase the likelihood that the tasks can be completed as defined by the unique context of the organization.

3.1.1 Using Existing TKS Statements

Each Knowledge and Skill statement is intended to support various tasks, and the Task statements may support one or more Work Roles. Although a Task statement may have a predetermined set of associated K&S statements, users may include other existing Ks and Ss to tailor Tasks for their unique context. Similarly, a user may wish to draw from the listed Tasks and add additional ones to those supporting a Work Role. The current set of NICE Framework components is available from the NICE Framework Resource Center.

Users are cautioned against internally modifying the text in an existing NICE Framework Component. The statements are intended to support interoperability, so changing their content may result in subsequent misalignment. If different wording is needed in a TKS statement, a new statement can be created as described below.

3.1.2 Creating New TKS Statements

Users may also create new Task, Knowledge, or Skill statements to help tailor the use of the NICE Framework for their unique context. Such additional statements will help support clear and consistent internal discussions regarding learners and their work activities. Any internally developed statements should follow the guidance to be provided in the future.

3.2 Work Roles

A key building block of the NICE Framework is described by Work Roles. Work Roles are a way of describing a grouping of work for which someone is responsible or accountable. Each Work Role is associated with a given set of Task statements, thereby describing a "work-centered" view of workforce management.

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 Task statements that constitute the work to be done; Task statements, as described above, include associated Knowledge and Skill statements that represent learners' potential to perform those tasks. This transitive approach, illustrated in Figure 2, supports flexibility and simplifies communication.

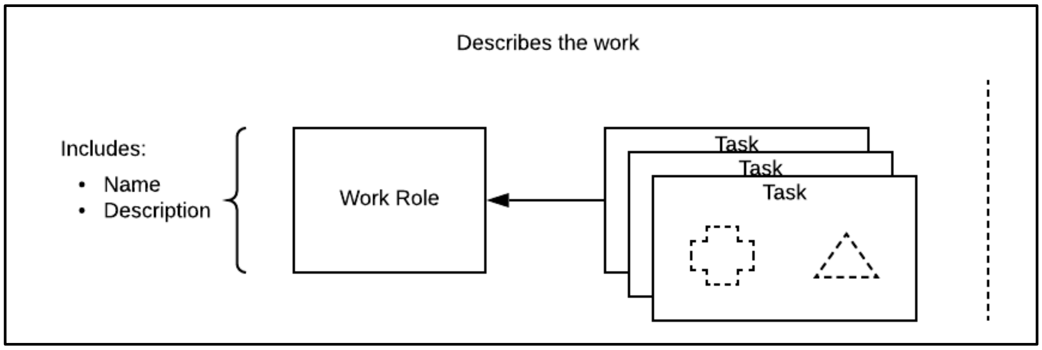

Figure 2 - Work Roles' Relationship to Task Statements

Work Role names are not synonymous with job titles, though some Work Roles may coincide with a job title. Similarly, a single Work Role (e.g., Software Developer) may apply to those with many varying job titles (e.g., software engineer, coder, application developer.) This method supports improved modularity and illustrates the fact that all in the workforce perform numerous tasks in various roles, regardless of their job titles. Similarly, the NICE Framework does not provide for attribution of adjectives such as Entry-, Intermediate-, or Advanced-level. Such attributes, and those regarding the proficiency with which a learner performs tasks, are left to other models or resources.

3.2.1 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.

Users are cautioned against internally modifying the text in an existing NICE Framework Component. 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.

3.2.2 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. Any internally developed Work Roles should follow the guidance to be provided in the future.

3.3 Competencies

Competency: an observable group of related Knowledge and Skills statements.

Competencies are a way to further describe learners. Figure 3 depicts a grouping of K&S statements. By grouping sets of Knowledge and Skills, Competencies allow learners to succinctly communicate and effectively demonstrate that they have the requisite Knowledge and

Skills to perform cybersecurity work. The underlying Knowledge and Skills do not change; however, the grouping provided by Competencies provides a streamlined view of a learner. As such, Competencies are a "learner-centered" view of workforce management. The flexibility of Competencies allows organizations and learners to adapt to the changing cybersecurity ecosystem.

3.3.1 Using Existing Competencies

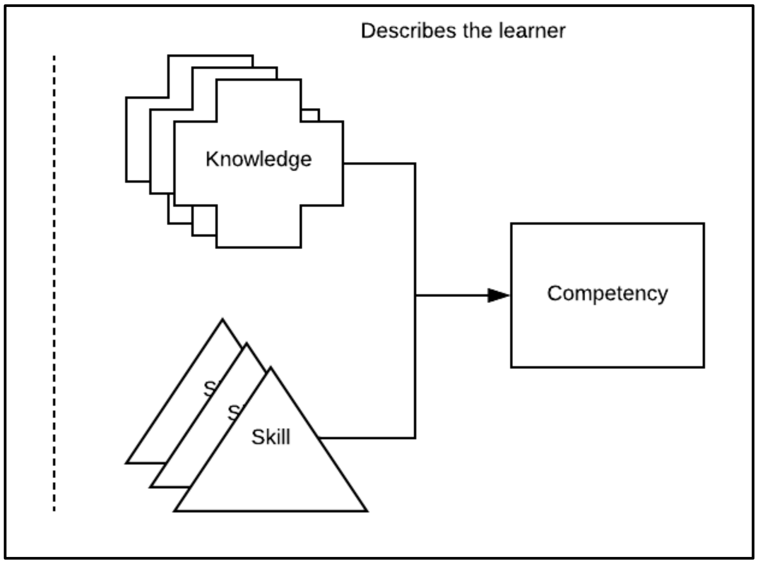

Figure 3 - How Competencies Relate to Knowledge and Skills Statements

Organizations have provided examples of Competencies within their industries. NIST is developing a set of these in the forthcoming Draft Special Publication (SP) 800-16 Revision 2, *Cybersecurity Role Profiles for Training*. [5] These concepts can be adapted to fit within the Competency component provided above. By mapping the Competency into its constituent K&S statements, the Competency is then aligned to the NICE Framework.

As mentioned in section 3.1.2, it is possible to tailor the NICE Framework. Existing Competencies may highlight the need for new K&S statements. By creating these new K&S statements, the user of the NICE Framework can tailor the NICE Framework to meet their unique requirements. Using the Competency concept allows organizations to practice interoperability between frameworks by using a common language and building blocks.

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. Creating or identifying relevant competencies is a flexibility offered by mapping Ks and Ss that are valued by subject matter experts who wish to use a competency to support conversations between managers and employees, for example.

Additionally, if an organization wanted to create a Competency for Data Analysis, it could look like the following:

Table 1 - Creating a Data Analysis Competency

Competency Name: Data Analysis	
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.	
Knowledge Statements	**Skill Statements**
Knowledge of statistical primitives	Evaluates information for reliability, validity, and relevance
Knowledge of data structures	Analyzes meaning across data sets
Knowledge of analytic tools and techniques for language, voice, and/or graphic material.	Performs sensitivity analysis

Table 1 demonstrates a way of creating Competencies. The example presented in Table 1 is informative and provides a starting point for building a Competency. A fully detailed Competency of Data Analysis would be much larger. The Data Analysis Competency has a name and a description that quickly allows the learner or the organization allows the learner to identify a competency as one they possess or aspire to achieve. By enumerating the K&S statements within the Competency, the learner or the organization can specify the desired scope of the Competency.

3.4 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.

3.4.1 Building Teams with Work Roles

Teams can be built from a work-centered approach using Work Roles. A work-centered approach to building teams allows organizations to define what types of Work Roles are appropriate for achieving objectives. Consequently, these Work Roles execute the Tasks needed to achieve the objectives. Since Work Roles are made up of Tasks, this approach to building teams starts with the work.

Table 2 - Example of a Secure Software Development Team

Lifecycle Phase	Work Role
Design	Security Architect
Build	Software Developer
Deploy	Network Operations Specialist
Operate	Customer Support Specialist
Maintain	Database Administrator
Decommission	Communications Specialist

Table 2, above, describes an example Secure Software Development team. Teams built using Work Roles begin with the identification of the work which needs to be accomplished. Secure software development has lifecycle phases designed to achieve objectives of security and quality of software. These objectives are linked to Tasks, and thus, Work Roles. Table 2 is an informative example and does not cover all Work Roles which may be present. For more information, see NIST's Secure Software Development Framework. [6]

Table 3 - Example of a Cybersecurity Team

Cybersecurity Framework Function	Work Role
Identify	Risk Manager
Protect	Controls Assessor
Detect	Cyber Defense Analyst
Respond	Incident Responder
Recover	Communications Specialist

Table 3 describes an example Cybersecurity Team. Similar to the Secure Software Development team, the example Cybersecurity 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. Table 3 is an informative example and does not cover all Work Roles which may be present. For more information, see NIST's Cybersecurity Framework. [7]

3.4.2 Building Teams with Competencies

Teams can also be built using Competencies through a learner-centered approach. This approach to building teams recognizes that the individual Tasks may be unknown, but the types of Competencies needed to solve the challenge are known. Therefore, teams can be built by using a group of Competencies to identify learners who might help with work in the future. Since Competencies are made up of K&S statements, this approach to building teams starts with the learners.

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 competencies:

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

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 (e.g., through Task statements) and the knowledge and skills of individual learners that support that work.

The ability to describe 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 to describe the work to be performed in many areas. The benefits to these organizations support the NICE mission of energizing and promoting a robust ecosystem of cybersecurity education, training, and workforce development.

References

[1] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 1.0*, https://www.nist.gov/file/359276

[2] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 2.0*, https://www.nist.gov/file/359261

[3] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), Second Draft NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286-draft2

[4] Anderson LW (ed.), Krathwohl DR (ed.), Airasian PW, Cruikshank KA, Mayer RE, Pintrich PR, Raths J, Wittrock, MC (2001) A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. (Addison Wesley Longman, Inc., New York, NY).

[5] Newhouse W, Sanchez-Cherry K, Williams C, Van Duyn L (Forthcoming) Cybersecurity Role Profiles for Training. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-16, Rev. 2.

[6] Dodson D, Souppaya M, Scarfone K (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
OMB	Office of Management and Budget
SSDF	Secure Software Development Framework
TKS	Task, Knowledge, and Skill statements