https://easy-peasy.ai/ai-image-generator/images/futuristic-website-security-surfersparadise-web3

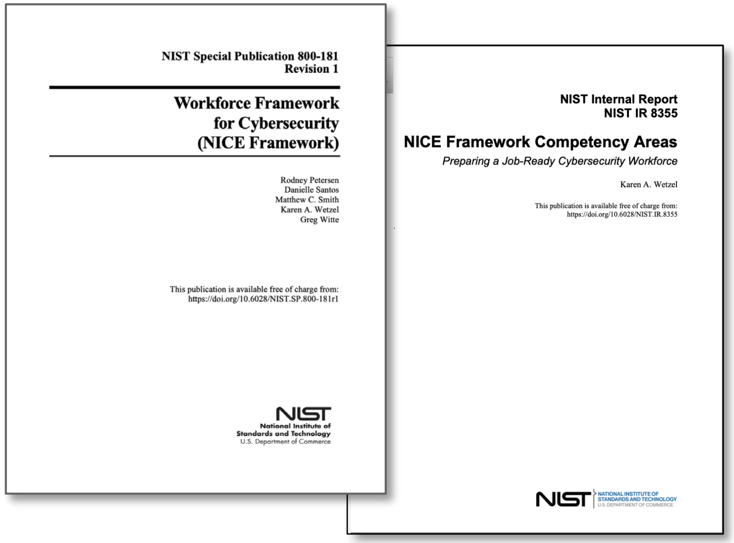
The NICE Framework:
A tool for cybersecurity workforce planning and development

Karen Wetzel and Mike Prebil, NICE
National Institute of Standards and Technology
U.S. Department of Commerce

NCyTE Monthly Membership Meeting | April 19, 2024

Workforce Framework for Cybersecurity (NICE Framework)

NIST SP 800-181r1 (2020) | Components v1.0.0 (March 2024)



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

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

NIST Internal Report
NIST IR 8355

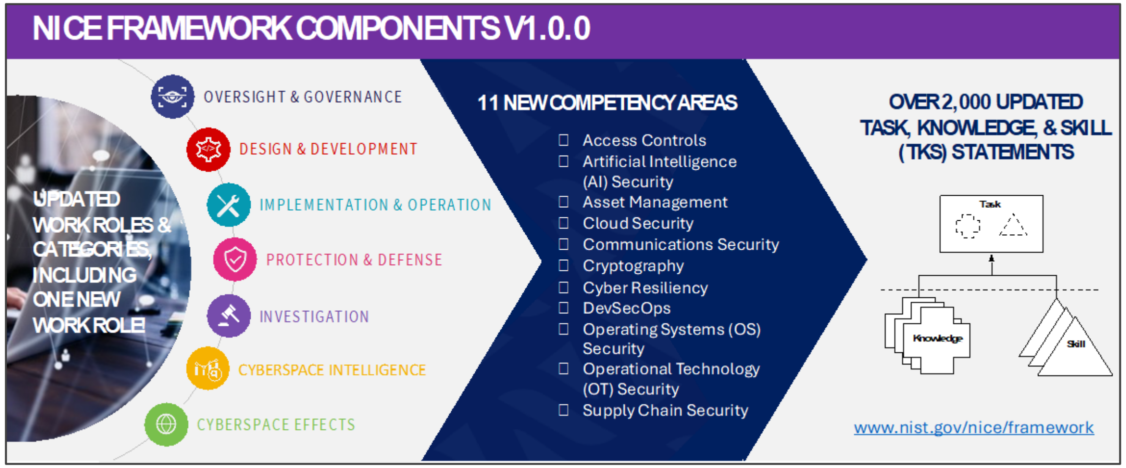
NICE Framework Competency Areas

Preparing a Job-Ready Cybersecurity Workforce

Karen A. Wetzel

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8355

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



NICE FRAMEWORK COMPONENTS V1.0.0

UPDATED WORK ROLES & CATEGORIES, INCLUDING ONE NEW WORK ROLE!

- OVERSIGHT & GOVERNANCE
- DESIGN & DEVELOPMENT
- IMPLEMENTATION & OPERATION
- PROTECTION & DEFENSE
- INVESTIGATION
- CYBERSPACE INTELLIGENCE
- CYBERSPACE EFFECTS

11 NEW COMPETENCY AREAS

- ☐ Access Controls
- ☐ Artificial Intelligence (AI) Security
- ☐ Asset Management
- ☐ Cloud Security
- ☐ Communications Security
- ☐ Cryptography
- ☐ Cyber Resiliency
- ☐ DevSecOps
- ☐ Operating Systems (OS) Security
- ☐ Operational Technology (OT) Security
- ☐ Supply Chain Security

OVER 2,000 UPDATED TASK, KNOWLEDGE, & SKILL (TKS) STATEMENTS

www.nist.gov/nice/framework

- ✓ A **common language** to clearly share about what a workforce needs to know
- ✓ A **modular, building-blocks approach** based on Task, Knowledge, and Skill (TKS) statements
- ✓ Defined **Work Roles** and **Competency Areas** for use in:
  - Career discovery
  - Education and training
  - Workforce planning and assessment
  - Hiring and career development

NIST | NICE

www.nist.gov/nice/framework

Value for...

EMPLOYERS

- Broaden pipeline and increase diversity
- Create job descriptions and assess candidate skills
- Track and plan workforce capabilities
- Develop employees through role-based training

LEARNERS

- Discover and plan for cybersecurity careers
- Knowledge and skills development
- Demonstrate capability and evidence competency

EDUCATORS

- Develop learning courses and programs that address employer needs
- Align learning experiences with the NICE Framework
- Conduct performance-based assessments

Resource: Resources by Audience

NIST NICE

GOVERNMENT • INDUSTRY • ACADEMIA

March 5, 2024

NICE FRAMEWORK COMPONENTS V1.0.0

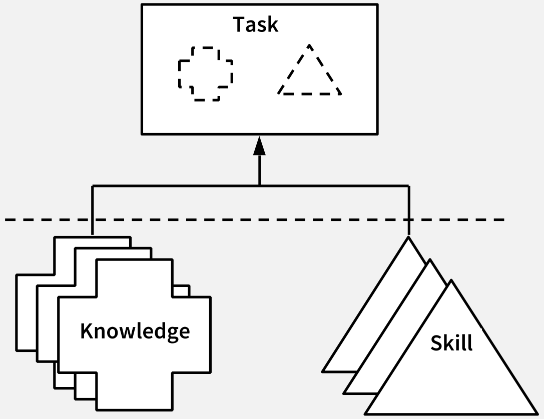
UPDATED WORK ROLES & CATEGORIES, INCLUDING ONE NEW WORK ROLE!

- OVERSIGHT & GOVERNANCE
- DESIGN & DEVELOPMENT
- IMPLEMENTATION & OPERATION
- PROTECTION & DEFENSE
- INVESTIGATION
- CYBERSPACE INTELLIGENCE
- CYBERSPACE EFFECTS

11 NEW COMPETENCY AREAS

- Access Controls
- Artificial Intelligence (AI) Security
- Asset Management
- Cloud Security
- Communications Security
- Cryptography
- Cyber Resiliency
- DevSecOps
- Operating Systems (OS) Security
- Operational Technology (OT) Security
- Supply Chain Security

OVER 2,000 UPDATED TASK, KNOWLEDGE, & SKILL (TKS) STATEMENTS



www.nist.gov/nice/framework

Resource: NICE Framework Resource Center

Walkthrough of v1.0.0 Components

v1.0.0 Components: Content (1)

Updates reflected in the v1.0.0 Components include:

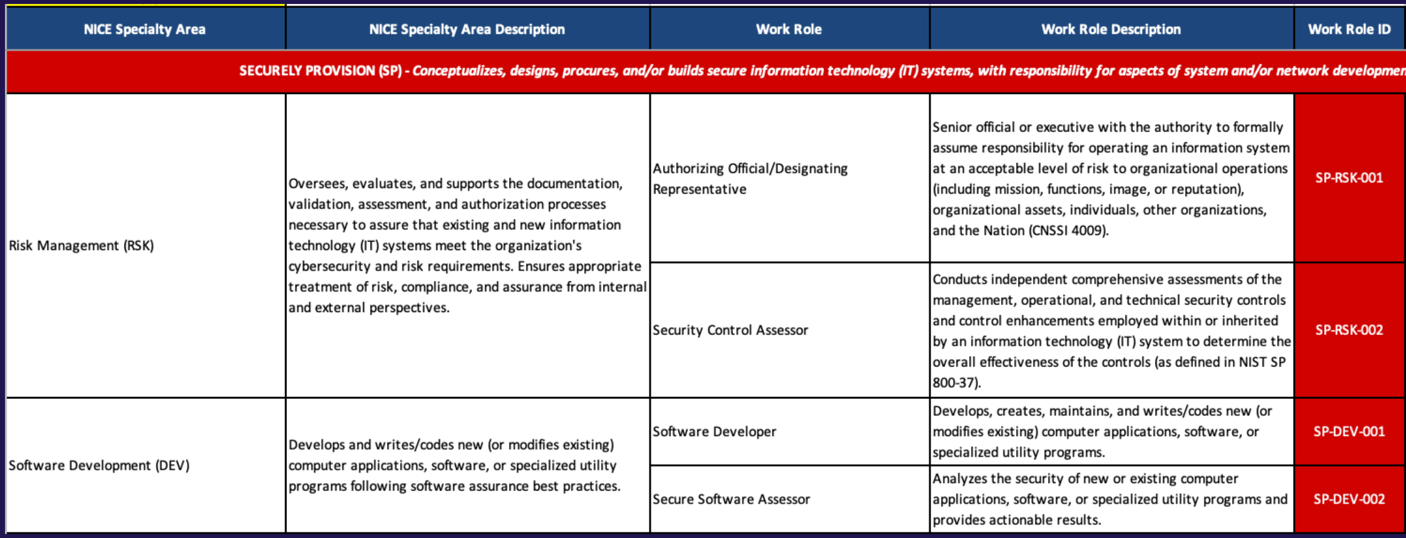
- SP 800-181 Revision 1 (structural changes, Nov. 2020)
- Abilities and K&S refactorings (Dec. 2021, Apr. 2022)
- Updates to Work Roles & WR Categories (comment period beginning April 2023)
- Updates to Competency Areas (June 2023)
- Updates to Task statements (comment period Nov. 2023)

v1.0.0 Components: Content (2)

Structural changes reflected in v1.0.0 Components:

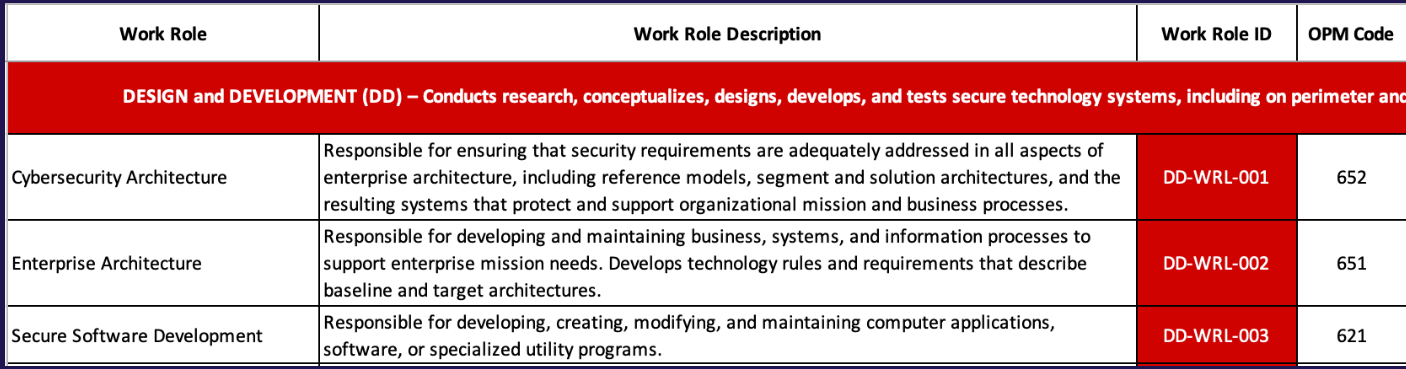
- Work Role Categories
    - ~~Specialty Areas~~
        - Work Roles
            - Tasks
            - Knowledge
            - Skills
            - ~~Abilities~~
- Competency Areas

2017



NICE Specialty Area	NICE Specialty Area Description	Work Role	Work Role Description	Work Role ID
SECURELY PROVISION (SP) - ***Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network developmen***				
Risk Management (RSK)	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.	Authorizing Official/Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).	SP-RSK-001
		Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).	SP-RSK-002
Software Development (DEV)	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.	Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.	SP-DEV-001
		Secure Software Assessor	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.	SP-DEV-002

v1.0.0



Work Role	Work Role Description	Work Role ID	OPM Code
DESIGN and DEVELOPMENT (DD) – Conducts research, conceptualizes, designs, develops, and tests secure technology systems, including on perimeter anc			
Cybersecurity Architecture	Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes.	DD-WRL-001	652
Enterprise Architecture	Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules and requirements that describe baseline and target architectures.	DD-WRL-002	651
Secure Software Development	Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs.	DD-WRL-003	621

v1.0.0 Components: Content (3)

Common changes to elements in the v1.0.0 Components:

- Updated names (“Securely Provision” Category renamed to “Design and Development”)
- Updated identifiers (“DD” replaces “SP”)
- Updated descriptions

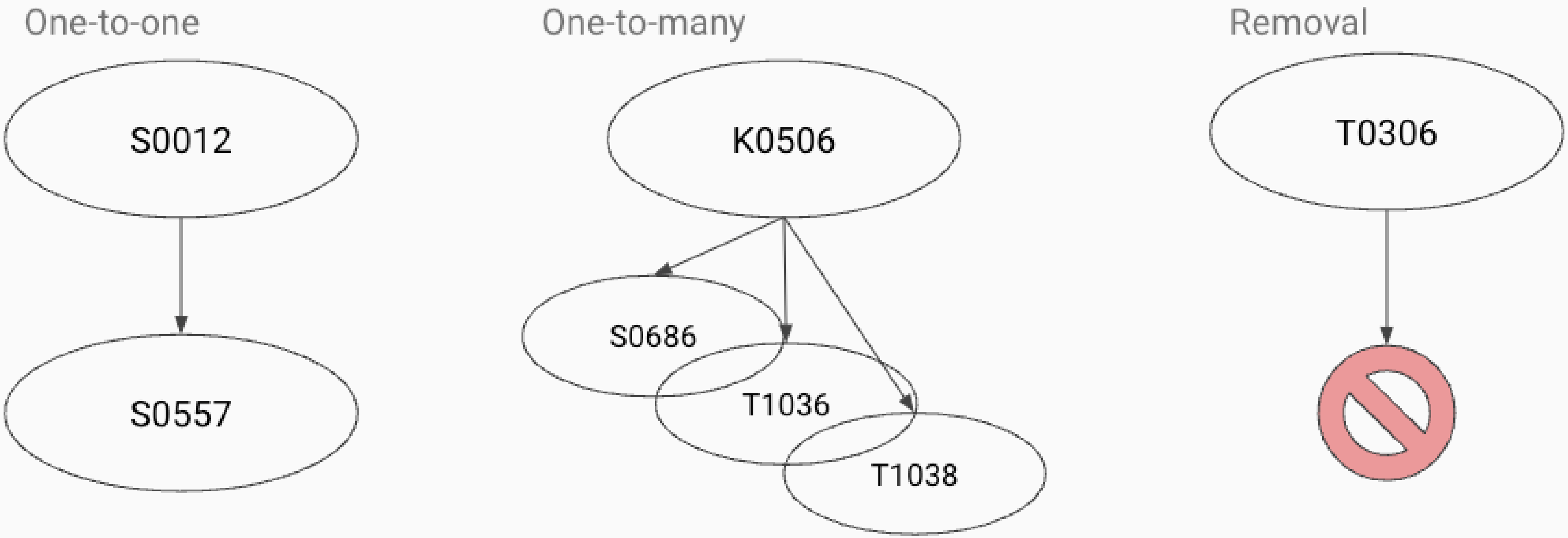
New elements have also been added: 11 Competency Areas; one new Work Role; 2141 new TKS statements.

v1.0.0 Components: Content (TKS updates 1)

Most elements of the NICE Framework have changed. E.g., TKS Statements:

	2017	Retained	Withdrawn	New	v1.0.0
Abilities	177	0	177	0	0
Tasks	1006	91	915	993	1084
Knowledge	634	15	619	625	640
Skills	377	33	344	523	556
Total	2194	139	2055	2141	2280

v1.0.0 Components: Contents (TKS updates 2)



S0012 is withdrawn; new S0057.

K0506 is withdrawn; new S0686, T1036, T1038

T0306 is withdrawn.

v1.0.0 Components: Formats

The v1.0.0 Components are available in two formats:

- Excel spreadsheets (best for browsing & searching)
- JSON files (best for updating NF-enabled applications)

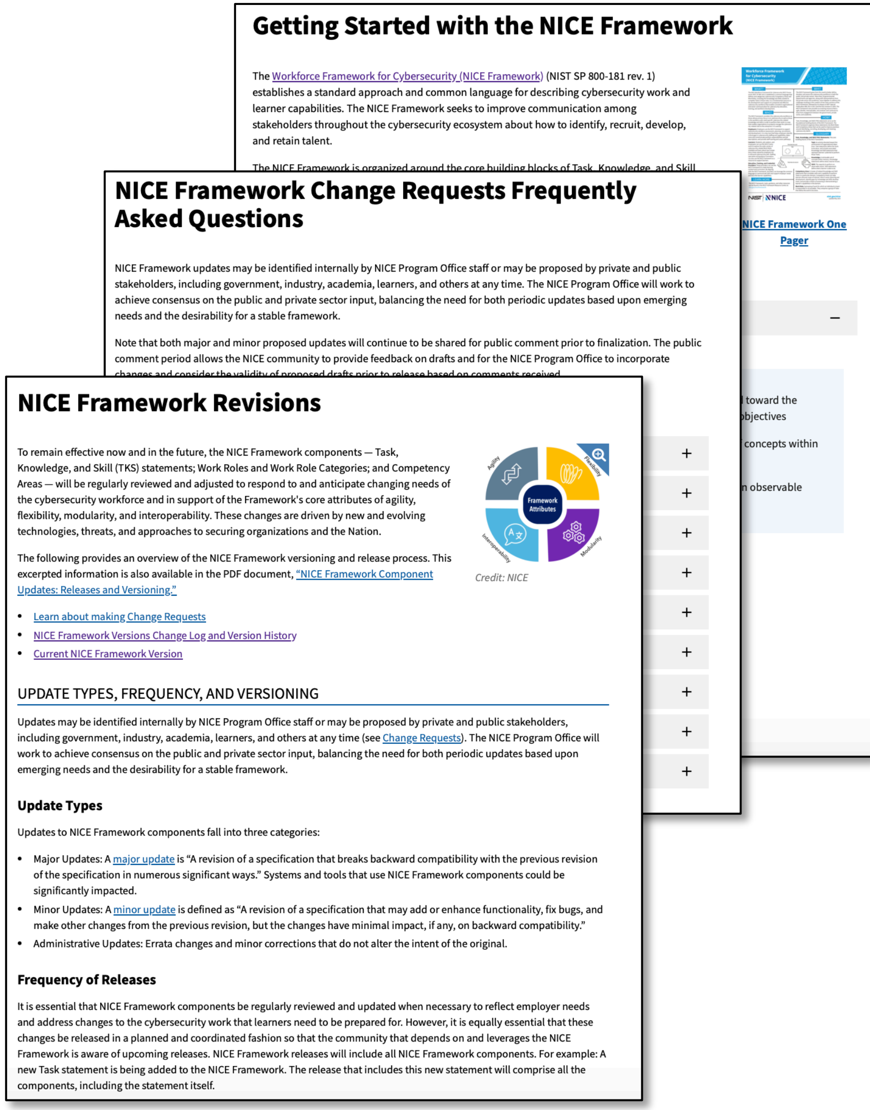
For each format, you'll encounter two types of document:

- Current Components (v1.0.0): all current elements of the NICE Framework
- Mapping documents: connections between 2017 and v1.0.0 Components.

Both data formats are available on the NICE Framework Resource Center.

NICE Framework Resource Center: New and Updated Content

- Getting Started with the NICE Framework
- NICE Framework Current Version
- NICE Framework History & Change Logs
- Revisions: Update Types, Frequency, and Versioning
- NICE Framework Change Requests FAQ
- NICE Framework FAQ



Getting Started with the NICE Framework

The Workforce Framework for Cybersecurity (NICE Framework) (NIST SP 800-181 rev. 1) establishes a standard approach and common language for describing cybersecurity work and learner capabilities. The NICE Framework seeks to improve communication among stakeholders throughout the cybersecurity ecosystem about how to identify, recruit, develop, and retain talent.

The NICE Framework is organized around the core building blocks of Task, Knowledge, and Skill

NICE Framework One Pager

NICE Framework Change Requests Frequently Asked Questions

NICE Framework updates may be identified internally by NICE Program Office staff or may be proposed by private and public stakeholders, including government, industry, academia, learners, and others at any time. The NICE Program Office will work to achieve consensus on the public and private sector input, balancing the need for both periodic updates based upon emerging needs and the desirability for a stable framework.

Note that both major and minor proposed updates will continue to be shared for public comment prior to finalization. The public comment period allows the NICE community to provide feedback on drafts and for the NICE Program Office to incorporate changes and consider the validity of proposed drafts prior to release based on comments received.

NICE Framework Revisions

To remain effective now and in the future, the NICE Framework components — Task, Knowledge, and Skill (TKS) statements; Work Roles and Work Role Categories; and Competency Areas — will be regularly reviewed and adjusted to respond to and anticipate changing needs of the cybersecurity workforce and in support of the Framework's core attributes of agility, flexibility, modularity, and interoperability. These changes are driven by new and evolving technologies, threats, and approaches to securing organizations and the Nation.

Credit: NICE

The following provides an overview of the NICE Framework versioning and release process. This excerpted information is also available in the PDF document, "NICE Framework Component Updates: Releases and Versioning."

- Learn about making Change Requests
- NICE Framework Versions Change Log and Version History
- Current NICE Framework Version

UPDATE TYPES, FREQUENCY, AND VERSIONING

Updates may be identified internally by NICE Program Office staff or may be proposed by private and public stakeholders, including government, industry, academia, learners, and others at any time (see Change Requests). The NICE Program Office will work to achieve consensus on the public and private sector input, balancing the need for both periodic updates based upon emerging needs and the desirability for a stable framework.

Update Types

Updates to NICE Framework components fall into three categories:

- Major Updates: A major update is "A revision of a specification that breaks backward compatibility with the previous revision of the specification in numerous significant ways." Systems and tools that use NICE Framework components could be significantly impacted.
- Minor Updates: A minor update is defined as "A revision of a specification that may add or enhance functionality, fix bugs, and make other changes from the previous revision, but the changes have minimal impact, if any, on backward compatibility."
- Administrative Updates: Errata changes and minor corrections that do not alter the intent of the original.

Frequency of Releases

It is essential that NICE Framework components be regularly reviewed and updated when necessary to reflect employer needs and address changes to the cybersecurity work that learners need to be prepared for. However, it is equally essential that these changes be released in a planned and coordinated fashion so that the community that depends on and leverages the NICE Framework is aware of upcoming releases. NICE Framework releases will include all NICE Framework components. For example: A new Task statement is being added to the NICE Framework. The release that includes this new statement will comprise all the components, including the statement itself.

Resource: www.nist.gov/nice/framework

Get Involved

- NICE Working Groups
- NICE Communities of Interest
- NICE Framework Users Group
- Events and Workshops
- NICE Publications
- Direct Feedback

Resource: Ways to Engage

NICE | Conference & Expo 2024

REGISTER TODAY!

SHERATON DALLAS
JUNE 3 - 5, 2024
niceconference.org

NICE

This event is supported by NICE, a program of the National Institute of Standards and Technology in the U.S. Department of Commerce, under NIST Financial Assistance. Award number: 70NANB23H004

FIU | FLORIDA INTERNATIONAL UNIVERSITY

NEW AMERICA