The NICE Workforce Framework for Cybersecurity (NICE Framework) is a fundamental resource to help in the development and support of a workforce capable of meeting an organization's cybersecurity needs. It establishes a common language to describe cybersecurity work and what someone needs to know or be able to do to complete that work. By doing so, it enables consistent organizational and sector communication for cybersecurity education, training, and workforce development.

**Why?**

The NICE Framework supports a variety of audiences:

- **Employers**: Helps with cybersecurity workforce assessment and planning, including supporting the identification of critical gaps in cybersecurity staffing and capabilities; in hiring, when determining position responsibilities and creating job descriptions consistent with national language; and in development, providing staff training and career development.

- **Learners**: Students, job-seekers, and employees can use the NICE Framework to explore the wide variety of cybersecurity-related Work Roles available and learn about top Competency Areas valued by employers for in-demand cybersecurity jobs. Staffing specialists and guidance counselors can also use the NICE Framework as a resource to support learners.

- **Education, Training, and Credential Providers**: The NICE Framework provides direct information about what a workforce needs to know, providing clear, consistent language to support learning content and curriculum development and the creation of certificates, badging, and other verification techniques to describe learner capabilities.

**Purpose**

Task, Knowledge, and Skill (TKS) statements serve as the foundational building blocks of the NICE Framework. The NICE Framework further organizes these statements into common cybersecurity Work Roles and Competency Areas that can be used to improve practices around identifying, recruiting, developing, and retaining cybersecurity talent, including those whose primary focus is on cybersecurity as well as those who need specific cybersecurity-related knowledge and skills in order to manage risks to the enterprise.

**Development**

The concept for the NICE Framework grew from a recognized need to better define and assess the cybersecurity workforce in both the public and private sectors. To address this challenge, more than 20 governmental departments and agencies along with representatives from the private sector and academia came together to determine how to provide a common understanding of cybersecurity work. This resulted in the creation of two early versions of the NICE Framework, followed by its release as NIST Special Publication 800-181 in 2017 and the first revision in 2020. The evolution of the NICE Framework now provides a resource that is agile, flexible, interoperable, and modular and continues to draw from engagement between the government, private sector, and academia.

**Definitions**

- **Task, Knowledge, and Skill (TKS) Statements**: The core building blocks of the NICE Framework.
- **Task**: An activity directed toward the achievement of organizational objectives. Tasks include associated Knowledge and Skill statements that represent learners’ potential to perform those Tasks.
- **Knowledge**: A retrievable set of concepts within memory.
- **Skill**: The capacity to perform an observable action.
- **Competency Area**: A measurable cluster of related Task, Knowledge, or Skill (TKS) statements that correlates with performance on the job and can be improved through education, training (including on-the-job and via apprenticeships), or other learning experiences.

**Learn More**

nist.gov/nice/framework