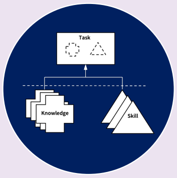
# WHAT IS THE NICE FRAMEWORK?

The NICE Workforce Framework for Cybersecurity (NICE Framework) is a structure and language for describing cybersecurity work, skills, and knowledge.

Learn more at www.nist.gov/nice/framework

942
TASKS



631
KNOWLEDGE

538
SKILLS

## TASK, KNOWLEDGE, AND SKILLS

TKS Statements are the building blocks of the NICE Framework. Tasks describe the work to be done, while Knowledge and Skills are what someone needs to know or be able to do to complete the work. They are used to define Work Roles and Competency Areas.

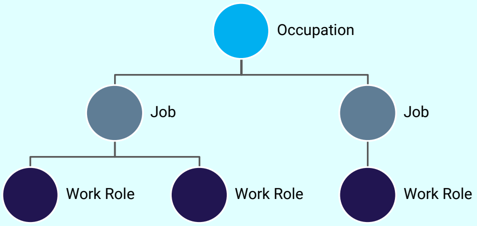
2111

5

## WORK ROLE CATEGORIES

These categories show the broad range of cybersecurity responsibilities across an organization, from oversight and governance to incorporating cybersecurity in design and implementations, in addition to the more specialized cybersecurity roles.

- OVERSIGHT & GOVERNANCE
- DESIGN & DEVELOPMENT
- IMPLEMENTATION & OPERATION
- PROTECTION & DEFENSE
- INVESTIGATION



## WORK ROLES

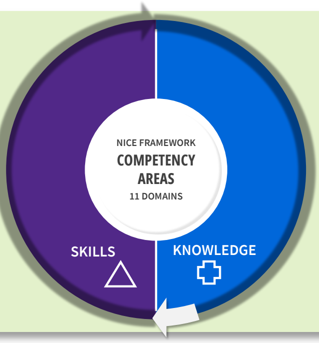
Work Roles group together TKS statements into areas of responsibility so you can learn about the kind of work that a role performs. All sorts of jobs can have cybersecurity responsibility, from legal advisors to project managers, systems developers, database administrators, incident responders, cybercrime analysts, and more.

41

11

## COMPETENCY AREAS

Competency Areas focus on a learner's capabilities in particular domains. These can be used in conjunction with Work Roles or on their own and represent emerging areas and other topics such as AI Cybersecurity, Cyber Resiliency, Operational Technology Security, and Supply Chain Security.



NICE | workforce framework for cybersecurity

*Updated March 2025*