الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Alignment Guide for the Saudi Cybersecurity Workforce Framework «SCyWF»

Issue Date: Oct 2020 version: 1

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red – Personal, Confidential and for Intended Recipient Only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization.

Amber – Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green – Sharing within the Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

White – No Restriction

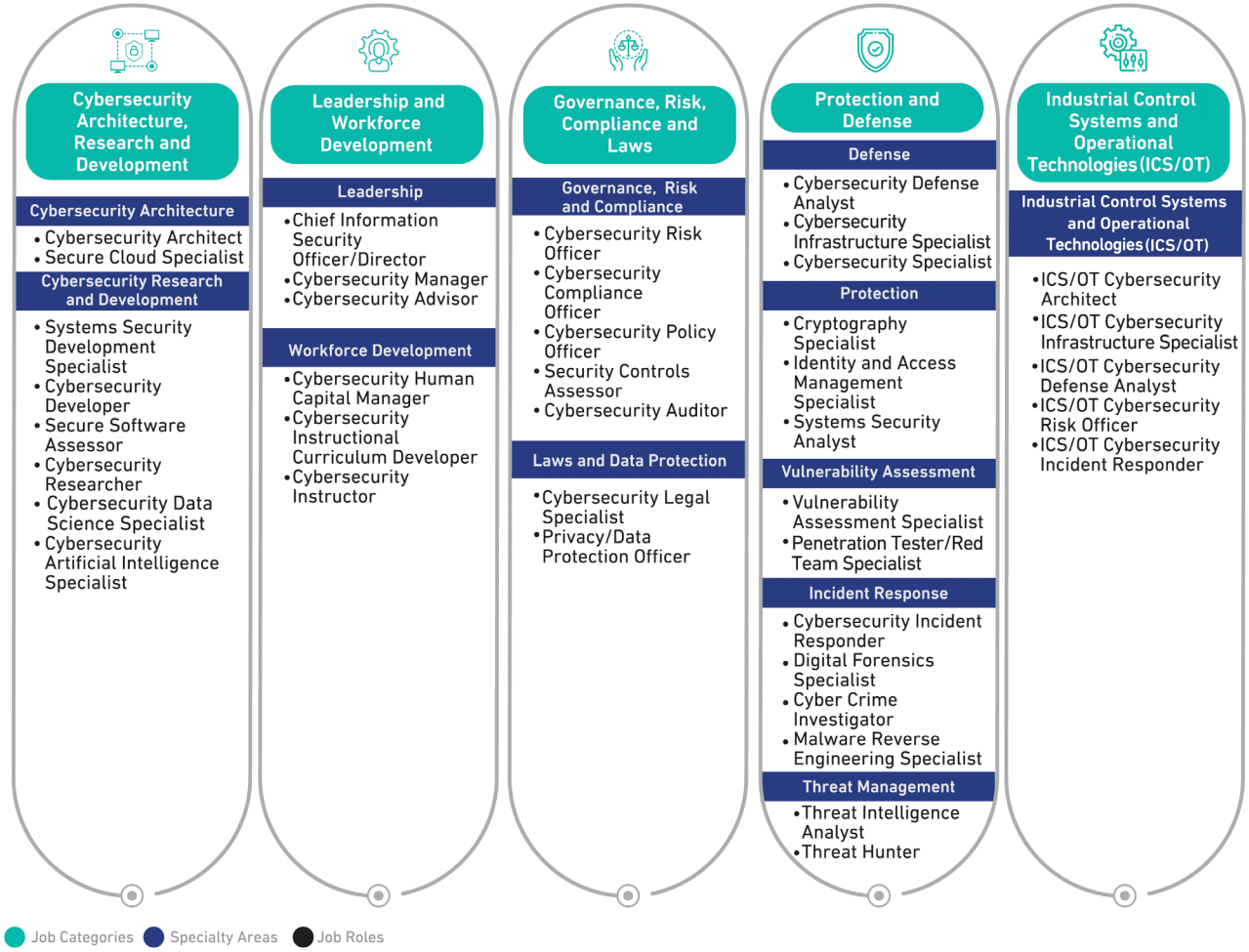
Introduction

The Saudi Cybersecurity Workforce Framework (SCyWF) categorizes cybersecurity work in Saudi Arabia, defines the job roles within each category and sets the requirements for each job role in terms of tasks, knowledge, skills and abilities (TKSAs).

Organizations are recommended to adopt and use this framework so they can align their cybersecurity workforce structures and activities with the national frameworks and guidelines. However, they can customize the framework to address their requirements.

The required cybersecurity job roles are determined according to the organization needs to satisfy its cybersecurity requirements and that depends on the organization's size and business nature.

The job roles specified in this framework have been included in the Saudi Standard Classification of Occupations which was approved by the Cabinet Resolution No. (660), dated 10/24/1441 AH.



What are the Objectives of "SCyWF"?

To serve as a reference model and a guideline for preparing, developing, recruiting, promoting and managing the cybersecurity workforce

To provide a common lexicon that improves communication between managers and Human Recourses personnel for attracting, retaining and training specialized talents in cybersecurity

To help in mapping learning outcomes of education and training programs to the knowledge, skills and abilities (KSAs) required for different cybersecurity job roles

Why do we need to link all cybersecurity job titles at the entity to "SCyWF" job roles?

1. To accurately identify the knowledge, skills and abilities required for the various cybersecurity job roles.
2. To determine the number of qualified employees for each job role at the organization level, at the sector level and at the national level; and to determine the workforce demand for each job role.

"SCyWF" Framework Alignment Mechanism

LIST

Listing the job roles within "SCyWF" framework that exist at the organization according to the tasks assigned:

- Review cybersecurity job roles in "SCyWF" framework.
- Determine the job roles (from "SCyWF" framework) that represent the cybersecurity jobs at the organization based on the tasks of the job roles within "SCyWF" framework and the nature of the organizations' cybersecurity work, regardless of the structure of the cybersecurity department and units in the organization.

LINK

Linking the listed job roles to the existing jobs at the organization:

- Examine the organization's job titles that relate to cybersecurity tasks and link them to the corresponding job roles within "SCyWF" framework.
- Update the job titles at the organization according to the corresponding job roles within "SCyWF" framework based on the tasks related to the job.

HANDLE

Handling special cases, including:

- When a proper justification exists, two or more job roles within "SCyWF" framework can be mapped to one job at the organization, provided that the job title reflects the tasks associated with these job roles.
- When a proper justification exists, a job role within "SCyWF" framework can be mapped to two or more cybersecurity jobs at the organization, provided that the job titles reflect the tasks associated with them.
- The jobs of the cybersecurity managers at the organization are related to different specialty areas and job roles within "SCyWF" framework (e.g., the Incident Response Manager). In these cases, the administrative position at the organization can be mapped to two job roles within "SCyWF" framework, one of them is "Cyberseurity Manager" and the other role depends on the specialty of the administrative unit associated with the cybersecurity job.

DOCUMENT

Document the alignment process:

Preparing an internal document to be approved by the organization's authority holder. The document should include the mapping between the identified cybersecurity job roles within "SCyWF" framework and the existing cybersecurity jobs at the organization. In addition, it should include the documentation of any special cases that were addressed as in the previous step.

Examples of mapping job titles in the organization with the relevant job roles in "SCyWF" framework

Example 1: Linking a job in the organization with one job role in "SCyWF" framework with the same job title:

Job Title in the Organization Before the Alignment	Information Security Risk Officer
"SCyWF" Job Roles Linked to the Job in the Organization	Cybersecurity Risk Officer
Job Title in the Organization After the Alignment	Cybersecurity Risk Officer

Example 2: Linking a job in the organization with one job role in "SCyWF" framework with a different job title:

Job Title in the Organization Before the Alignment	Cybersecurity Operations Analyst
"SCyWF" Job Roles Linked to the Job in the Organization	Cybersecurity Defense Analyst
Job Title in the Organization After the Alignment	Cybersecurity Defense Analyst

Example 3: Linking a job in the organization with two jobs roles in "SCyWF" framework:

Job Title in the Organization Before the Alignment	Cybersecurity Operation Center Manager
"SCyWF" Job Roles Linked to the Job in the Organization	• Cybersecurity Manager • Cybersecurity Defense Analyst
Job Title in the Organization After the Alignment	Cybersecurity Operation Center Manager

Example 4: Linking two jobs in the organization with one job role in "SCyWF" framework:

Job Title in the Organization Before the Alignment	• Cybersecurity Incident Response Analyst • Cybersecurity Incident Response Coordinator
"SCyWF" Job Roles Linked to the Job in the Organization	Cybersecurity Incident Responder
Job Title in the Organization After the Alignment	• Cybersecurity Incident Response Analyst • Cybersecurity Incident Response Coordinator

Note: The alignment involves modifying the job title as in Examples 1 and 2 or linking job titles to job roles in the "SCyWF" framework as in Examples 3 and 4.

What is the relationship between Human Resources Programs and "SCyWF" Framework?

Organizational Structure

"SCyWF" framework does not define the organizational structure of the cybersecurity department and units in the organization, but it can help in designing the organizational structure of cybersecurity departments by understanding the tasks of the job roles, categories, and specialty areas included in the framework. However, there are other cybersecurity controls and guidelines issued by NCA related to the organizational structure of cybersecurity departments.

Job Descriptions

"SCyWF" framework facilitates the process of creating, updating and standardizing job descriptions in the field of cybersecurity within national entities as each role has a job description that includes a description of the tasks, knowledge, skills and abilities required for each job role.

Recruitment

"SCyWF" framework enables human resources personnel to understand the tasks and requirements of cybersecurity jobs, hence facilitating the process of searching and selection of suitable qualified talents.

Competencies

"SCyWF" framework enables human resource personnel to benefit from the knowledge, skill and abilities of each job role in the framework through the process of creating or updating the technical and behavioral competencies framework of cybersecurity jobs.

Learning and Development

"SCyWF" framework assists human resources personnel in preparing training and development plans based on the knowledge, skills and abilities required for each job role.

Career Paths

Currently NCA is working on preparing an appendix of "career paths" for "SCyWF" framework, which clarifies the levels of each job role in terms of the minimum qualifications, tasks, knowledge and skills required as a benchmark for career progression, as well as the possible transfers between job roles and their levels.

For your questions and inquiries about the alignment with "SCyWF" framework, please contact us at: scywf@nca.gov.sa

الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority