الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

The Saudi Cybersecurity Workforce Framework

(SCyWF – 1.5: 2026)

TLP: Clear

Document Classification: Public

Disclaimer: Please refer to the National Cybersecurity Authority's website (https://nca.gov.sa), to obtain the latest version of this document

عام

In The Name Of Allah,
The Most Gracious,
The Most Merciful

Disclaimer: The following framework will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.

Traffic Light Protocol (TLP):

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

Red (Personal, Confidential, and for the Intended Recipient Only)

The recipient has no right to share the information classified in red with any person outside the defined range of recipients, either inside or outside the entity, beyond the scope specified for receipt.

Amber+ Strict (Sharing within the entity)

The recipient may share the information only with the intended recipients inside the entity.

Amber (Restricted Sharing)

The recipient may share the information only with the intended recipients inside the entity or with recipients who are required to take action related to the shared information.

Green (Sharing within the Same Community)

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

Clear (No Restrictions)

Table of Contents

List of Figures

List of Tables

1. Introduction

The Saudi National Cybersecurity Authority (NCA) is leading the national effort to protect the country's cyber space. This mission requires a qualified national cybersecurity workforce capable of carrying out all types of cybersecurity work. The NCA's mandate was issued by Royal Order number 6801, dated October 31, 2017. It includes building national capacities in cybersecurity, participating in the preparation of educational and training programs, setting professional standards and frameworks, and developing and implementing relevant professional standardized tests and measurements. The NCA has developed the Saudi Cybersecurity Workforce Framework (SCyWF) as a foundational step towards carrying out that mandate.

1.1 Overview

The 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 and skills (TKSs). The main objective of the SCyWF is to serve as a reference model and a guideline for preparing, developing, recruiting, promoting and managing the cybersecurity workforce. It provides a common lexicon that improves communication and content development for talent management activities. It also helps in mapping learning outcomes of education and training programs to the knowledge and skills (KSs) required for different cybersecurity job roles.

Organizations are recommended to adopt 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, provided that the core structure of the framework remains intact.

Since cybersecurity is a highly dynamic discipline, the content of this framework will be reviewed and updated periodically.

1.2 Methodology and Structure

The SCyWF was developed based on global best practices and recognized international standards, in a manner that enhance its effectiveness and quality in implementation and fits the needs of cybersecurity workforce in Saudi Arabia. The SCyWF organizes its cybersecurity framework in a hierarchical structure composed of categories, specialty areas, and job roles. The job roles, specialty areas, and categories are defined as follows:

A job role: is a set of cybersecurity tasks that need to be performed in a cybersecurity job. A job role is defined by a set of tasks to be performed within that job role and a list of knowledge and Skills (KSs) required to perform those tasks. All SCyWF job roles are listed in Appendix A.

A specialty area: is a group of job roles that serve a cybersecurity function and share common TKSs.

A category: is a group of specialty areas, and the job roles associated with them, that serve related cybersecurity functions.

This framework only covers job roles that are specific to cybersecurity. There are non-cybersecurity job roles that have some cybersecurity responsibilities or require some cybersecurity KSs. Most of these non-cybersecurity job roles are IT job roles, and they are outside the scope of this framework. In addition, all employees and IT users are expected to have some awareness of cybersecurity risks and good practice.

Figure 1 illustrates the structure of the SCyWF

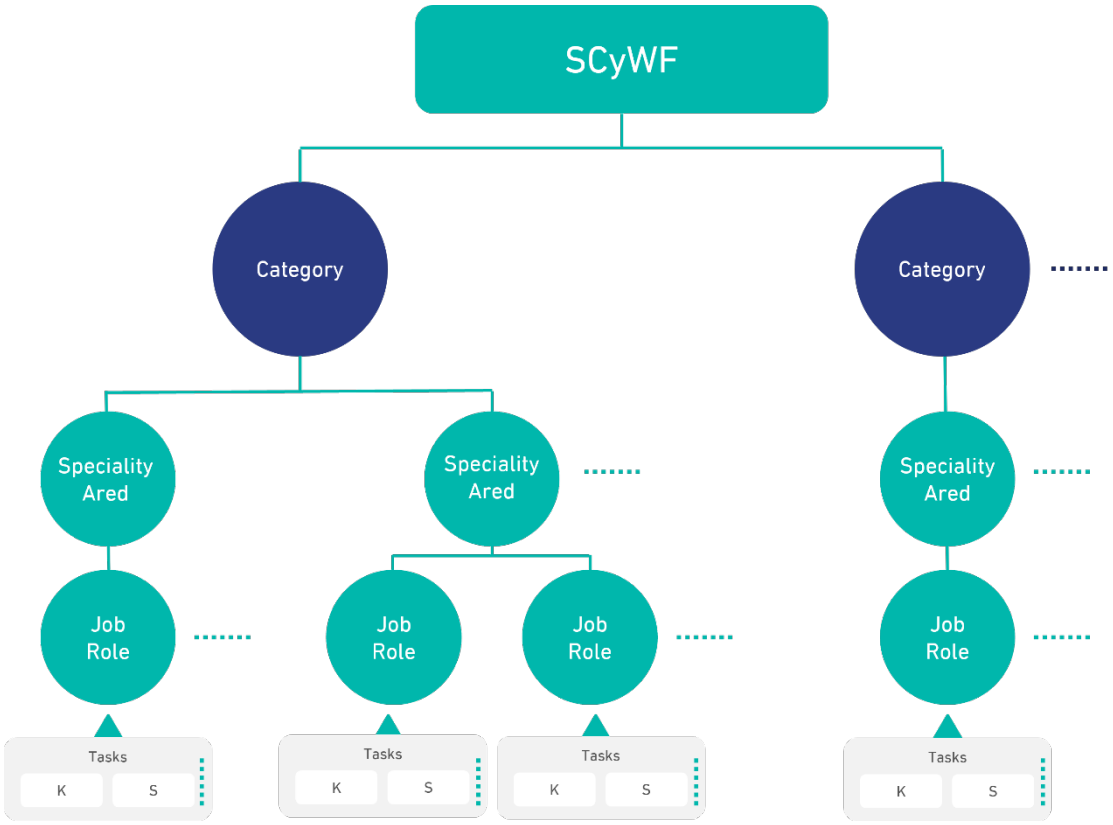

FIGURE 1: SCYWF FRAMEWORK STRUCTURE

2. The Saudi Cybersecurity Workforce Framework

2.1 Taxonomy

SCyWF Categories and specialty areas

The Saudi Cybersecurity Workforce Framework (SCyWF) organizes cybersecurity work into five categories, twelve specialty areas, and forty job roles. This taxonomy ensures a structured and consistent approach to defining and managing cybersecurity functions across diverse domains. Each category and specialty area represents a grouping of related cybersecurity responsibilities and functions designed to align job roles with specific organizational and national cybersecurity needs.

Figure 2 shows the full SCyWF taxonomy and how categories, specialty areas and job roles relate.

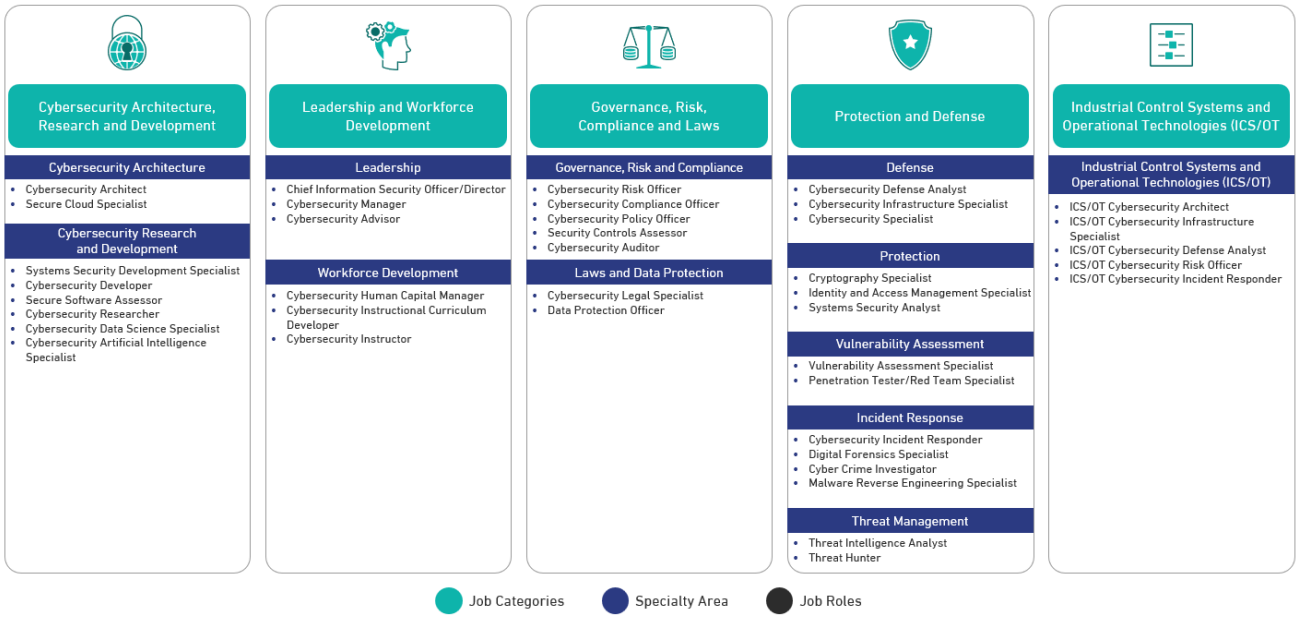

FIGURE 2: THE SCYWF TAXONOMY

Table 1 describes the SCyWF categories. Each category has a unique identifier (ID) composed of the first characters of the category's name (e.g. PD for Protection and Defense). This forms part of the full job role ID for the job roles under each category as described in Appendix A.

Category	Descriptions
Cybersecurity Architecture, Research and Development (**CARD**)	Conducts cybersecurity design, architecture, research and development activities.
Leadership and Workforce Development (**LWD**)	Leads cybersecurity teams and work. Develops cybersecurity human capital.
Governance, Risk, Compliance and Laws (**GRCL**)	Develops organizational cybersecurity policies. Governs cybersecurity structures and processes, manages cyber risks and assures compliance with the organization's cybersecurity, risk management and related legal requirements.
Protection and Defense (**PD**)	Identifies, analyzes, monitors, mitigates and manages threats and vulnerabilities to IT systems and networks. Uses defensive measures and multi-source information to report events and respond to incidents.
Industrial Control Systems and Operational Technologies (**ICS/OT**)	Conducts cybersecurity tasks for Industrial Control Systems and Operational Technologies (ICS/OT).

TABLE 1: SCYWF CATEGORIES

Table 2 describes the SCyWF specialty areas and the categories to which they belong. Each specialty area has a unique ID composed of the first characters of the specialty area's name (e.g. VA for Vulnerability Assessment). This is used alongside the category ID when creating job role IDs for the jobs under each specialty area, as described in Appendix A.

Category	Specialty Area	Description
Cybersecurity Architecture, Research and Development **(CARD)**	Cybersecurity Architecture **(CA)**	Designs and oversees the development and implementation of cybersecurity systems and/or the cybersecurity components of IT systems and networks.
	Cybersecurity Research and Development **(CRD)**	Conducts cybersecurity research and development.
Leadership and Workforce Development **(LWD)**	Leadership **(L)**	Supervises, manages and leads cybersecurity teams and work.
	Workforce Development **(WD)**	Applies knowledge and skills of cybersecurity, human resources development and teaching methodologies to develop, manage, retain and improve the skills of the cybersecurity workforce.
Governance, Risk, Compliance and Laws **(GRCL)**	Governance, Risk and Compliance **(GRC)**	Governs cybersecurity structures and processes. Manages cyber risks and assures IT systems against the organization's cybersecurity and risk management requirements. Develops and updates the organization's cybersecurity policies.
	Laws and Data Protection **(LDP)**	Ensures the organization complies with cybersecurity and data protection laws and regulations.
Protection and Defense **(PD)**	Defense **(D)**	Uses monitoring and analysis tools to identify and analyze events and to detect incidents.
	Protection **(P)**	Uses cybersecurity tools to protect information, systems and networks from cyber threats.
	Vulnerability Assessment **(VA)**	Tests IT systems and networks and assesses their threats and vulnerabilities.
	Incident Response **(IR)**	Investigates, analyzes and responds to cyber incidents.
	Threat Management **(TM)**	Collects and analyzes information about threats, searches for undetected threats and provides actionable insights to support cybersecurity decision-making.
Industrial Control Systems and Operational Technologies **(ICS/OT)**	Industrial Control Systems and Operational Technologies **(ICS/OT)**	Performs work related to cybersecurity governance, risk management and compliance; design and development; operations and administration; protection and defense for OT systems such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

TABLE 2: SCYWF SPECIALTY AREAS

2.2 SCyWF Tasks, Knowledge, Skills (TKS) and Competency Areas

The framework defines the core elements of each job role in terms of Tasks, Knowledge, and Skills:

- **Task**: A set of activities that need to be completed as part of a particular job role.
- **Knowledge**: The set of data, facts, information, theories, concepts, and issues related to a particular subject.
- **Skill**: The capability to apply knowledge and to use tools and methods to carry out a task.

The TKS statements in the SCyWF were developed based on global best practices and refined to meet the cybersecurity workforce needs of Saudi Arabia. Appendix B provides a complete list of the SCyWF TKS statements.

Moreover, this version of the SCyWF introduces competency areas to enhance the framework by addressing critical cybersecurity domains.

- **Competency Area**: A group of related Knowledge and Skill statements that reflect the capability to perform Tasks within a specific domain.

These areas focus on aligning workforce capabilities with real-world challenges, ensuring organizations and professionals can respond effectively to evolving cybersecurity needs. Competency Areas will help organizations to:

- Focus on specialized domains to address unique cybersecurity challenges.
- Align workforce training and certifications with industry requirements.
- Support career development by offering structured pathways for professional growth.

While Competency Areas enrich the SCyWF taxonomy, it is not necessary for professionals to fully master all details within every Competency Area linked to their roles. Instead, these areas act as a guiding framework to focus on relevant expertise. A detailed description of Competency Areas and their associated job roles can be found in Appendix C.

2.3 Cybersecurity Architecture, Research and Development (CARD) Job Roles

Table 3 describes the job roles in the Cybersecurity Architecture, Research and Development category.

No	Specialty Area	Job Role	Job Role ID	Description
1	Cybersecurity Architecture (CA)	Cybersecurity Architect	CARD-CA-001	Designs and oversees the development, implementation and configuration of cybersecurity systems and networks.
2		Secure Cloud Specialist	CARD-CA-002	Designs, implements and operates secure cloud computing systems and develops secure cloud policies.
3	Cybersecurity Research and Development (CRD)	Systems Security Development Specialist	CARD-CRD-001	Designs, develops, tests and evaluates security of information systems throughout the development life-cycle.
4		Cybersecurity Developer	CARD-CRD-002	Develops cybersecurity software, applications, systems and products.
5		Secure Software Assessor	CARD-CRD-003	Assesses the security of computer applications, software, code or programs and provides actionable results.
6		Cybersecurity Researcher	CARD-CRD-004	Conducts scientific research in the cybersecurity field.
7		Cybersecurity Data Science Specialist	CARD-CRD-005	Uses mathematical models and scientific methods and processes to design and implement algorithms and systems that extract cybersecurity insights and knowledge from multiple large-scale data sets.
8		Cybersecurity Artificial Intelligence Specialist	CARD-CRD-006	Uses artificial intelligence models and techniques (including machine learning ones) to design and implement algorithms and systems that automate and improve the efficiency and effectiveness of cybersecurity tasks.

TABLE 3: CYBERSECURITY ARCHITECTURE, RESEARCH AND DEVELOPMENT (CARD) JOB ROLES

2.4 Leadership and Workforce Development (LWD) Job Roles

Table 4 describes the job roles in the Leadership and Workforce Development category.

No	Specialty Area	Job Role	Job Role ID	Description
9	Leadership (L)	Chief Information Security Officer/ Director	LWD-L-001	Directs cybersecurity work within an organization, establishes vision and direction for its cybersecurity and related strategies, resources and activities and advises the leadership on the effective management of the organization's cyber risks.
10		Cybersecurity Manager	LWD-L-002	Manages the security of information systems and functions within an organization. Leads a cybersecurity team, unit and/or enterprise level function.
11		Cybersecurity Advisor	LWD-L-003	Provides expert consultancy and advice on cybersecurity topics to an organization's leadership and to its cybersecurity leadership and teams.
12	Workforce Development (WD)	Cybersecurity Human Capital Manager	LWD-WD-001	Develops plans, strategies and guidance within an organization to support the development and management of the cybersecurity workforce.
13		Cybersecurity Instructional Curriculum Developer	LWD-WD-002	Develops, plans, coordinates and evaluates cybersecurity training, awareness, and education programs, courses, contents, methods and techniques based on instructional needs.
14		Cybersecurity Instructor	LWD-WD-003	Teaches, trains, develops and tests people in cybersecurity topics and awareness to encourage secure behaviors.

TABLE 4: LEADERSHIP AND WORKFORCE DEVELOPMENT (LWD) JOB ROLES

2.5 Governance, Risk, Compliance and Laws (GRCL) Job Roles

Table 5 describes the job roles in the Governance, Risk, Compliance and Laws category.

No	Specialty Area	Job Role	Job Role ID	Description
15	Governance, Risk and Compliance (GRC)	Cybersecurity Risk Officer	GRCL-GRC-001	Identifies, assesses and manages an organization's cybersecurity risks to protect its information and technology assets in line with organizational policies and procedures and related laws and regulations.
16		Cybersecurity Compliance Officer	GRCL-GRC-002	Ensures an organization's cybersecurity program complies with applicable requirements, policies and standards.
17		Cybersecurity Policy Officer	GRCL-GRC-003	Develops, updates and maintains cybersecurity policies to support and align with an organization's cybersecurity requirements.
18		Security Controls Assessor	GRCL-GRC-004	Analyzes cybersecurity controls and assesses their effectiveness.
19		Cybersecurity Auditor	GRCL-GRC-005	Designs, performs and manages cybersecurity audits to assess an organization's compliance with applicable requirements, policies, standards and controls. Prepares audit reports and communicates them to authorized parties.
20	Laws and Data Protection (LDP)	Cybersecurity Legal Specialist	GRCL-LDP-001	Provides legal services on topics related to cyber laws and regulations.
21		Data Protection Officer	GRCL-LDP-002	Analyzes data protection risks and ensures compliance with applicable laws. Oversees the implementation of data protection policies and procedures. Supports organizational response to data protection incidents.

TABLE 5: GOVERNANCE, RISK, COMPLIANCE AND LAWS (GRCL) JOB ROLES

2.6 Protection and Defense (PD) Job Roles

Table 6 describes the job roles in the Protection and Defense category.

No	Specialty Area	Job Role	Job Role ID	Description
22	Defense (D)	Cybersecurity Defense Analyst	PD-D-001	Uses data collected from cyber defense tools to analyze events that occur within their organization to detect and mitigate cyber threats.
23		Cybersecurity Infrastructure Specialist	PD-D-002	Tests, implements, deploys, maintains and administers hardware and software that protect and defend systems and networks against cybersecurity threats.
24		Cybersecurity Specialist	PD-D-003	Provides general cybersecurity support. Assists in cybersecurity tasks.
25	Protection (P)	Cryptography Specialist	PD-P-001	Develops, evaluates, analyzes and identifies weaknesses of, and improvements to, cryptography systems and algorithms, including quantum techniques.
26		Identity and Access Management Specialist	PD-P-002	Manages individuals and entities identities and access to resources through applying identification, authentication and authorization systems and processes.
27		Systems Security Analyst	PD-P-003	Develops, tests and maintains systems' security. Analyzes security of operations and integrated systems.
28	Vulnerability Assessment (VA)	Vulnerability Assessment Specialist	PD-VA-001	Performs vulnerability assessments of systems and networks. Identifies where they deviate from acceptable configurations or applicable policies. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
29		Penetration Tester/Red Team Specialist	PD-VA-002	Conducts authorized attempts to penetrate computer systems or networks and physical premises, using realistic threat techniques, to evaluate their security and detect potential vulnerabilities.
30	Incident Response (IR)	Cybersecurity Incident Responder	PD-IR-001	Investigates, analyzes and responds to cybersecurity incidents.
31		Digital Forensics Specialist	PD-IR-002	Collects and analyzes digital evidence, investigates cybersecurity incidents to derive useful information to mitigate system and network vulnerabilities.
32		Cyber Crime Investigator	PD-IR-003	Identifies, collects, examines and preserves evidence using controlled and documented analytical and investigative techniques.
33		Malware Reverse Engineering Specialist	PD-IR-004	Analyzes (by disassembling and/or decompiling) malicious software, understands how it works, its impact and intent and recommends mitigation techniques and incident response actions.

34	Threat Management (TM)	Threat Intelligence Analyst	PD-TM-001	Collects and analyzes multi-source information about cybersecurity threats to develop deep understanding and awareness of cyber threats and actors' Tactics, Techniques and Procedures (TTPs), to derive and report indicators that help organizations detect and predict cyber incidents and protect systems and networks from cyber threats.
35		Threat Hunter	PD-TM-002	Proactively searches for undetected threats in networks and systems, identifies their Indicators of Compromise (IOCs) and recommends mitigation plans.

TABLE 6: PROTECTION AND DEFENSE (PD) JOB ROLES

2.7 Industrial Control Systems and Operational Technologies (ICS/OT) Job Roles

Table 7 describes the job roles in the Industrial Control Systems and Operational Technologies category.

No	Specialty Area	Job Role	Job Role ID	Description
36	Industrial Control Systems and Operational Technologies (ICS/OT)	ICS/OT Cybersecurity Architect	ICSOT-ICSOT-001	Designs and oversees the development, implementation and configuration of cybersecurity systems and networks in ICS/OT environments.
37		ICS/OT Cybersecurity Infrastructure Specialist	ICSOT-ICSOT-002	Tests, implements, deploys, maintains and administers hardware and software that protect and defend systems and networks against cybersecurity threat in ICS/OT environments.
38		ICS/OT Cybersecurity Defense Analyst	ICSOT-ICSOT-003	Uses data collected from a variety of cybersecurity tools to analyze events that occur within ICS/OT environments to detect and mitigate cybersecurity threats.
39		ICS/OT Cybersecurity Risk Officer	ICSOT-ICSOT-004	Identifies, assesses and manages cybersecurity risks within ICS/OT environments. Evaluates and analyzes the effectiveness of existing cybersecurity controls and provides feedback and recommendations based on assessments.
40		ICS/OT Cybersecurity Incident Responder	ICSOT-ICSOT-005	Investigates, analyzes and responds to cybersecurity incidents within ICS/OT environments.

TABLE 7: INDUSTRIAL CONTROL SYSTEMS AND OPERATIONAL TECHNOLOGIES (ICS/OT) JOB ROLES

For the KSs required for each job role and the tasks associated with it, see Appendix A

3. Appendices

3.1 Appendix A: Job Role Details

3.1.1 Category Group: Cybersecurity Architecture, Research and Development (CARD)

Job Role Details	
Job Role Name	Cybersecurity Architect
Job Role ID	CARD-CA-001
Category	Cybersecurity Architecture, Research and Development
Specialty Area	Cybersecurity Architecture
Job Role Description	Designs and oversees the development, implementation and configuration of cybersecurity systems and networks.
Competency Areas	Cybersecurity Design and Architecture (CA017)
Tasks	T0036, T0037, T0043, T0134, T0507, T0508, T0511, T0512, T0514, T0515, T0516, T0517, T0518, T0519, T0520, T0523, T0524, T0525, T0526, T0527, T0529, T0530, T0534, T0535, T0536, T0537, T0538, T0539, T0540, T0541, T1052, T2511, T4502
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0016, K0017, K0020, K0021, K0022, K0025, K0027, K0028, K0034, K0035, K0042, K0044, K0045, K0046, K0048, K0053, K0057, K0058, K0062, K0074, K0093, K0101, K0109, K0111, K0112, K0120, K0121, K0124, K0125, K0126, K0129, K0133, K0146, K0149, K0175, K0176, K0177, K0185, K0186, K0187, K0188, K0189, K0190, K0191, K0192, K0193, K0209, K0210, K0503, K0504, K0507, K0509, K0510, K0512, K0513, K0514, K0516, K0517, K0518, K1015, K1036, K1505, K4000, K4030, K5503
Skills	S0001, S0003, S0008, S0016, S0021, S0023, S0027, S0038, S0039, S0040, S0051, S0058, S0061, S0064, S0071, S0072, S0074, S0075, S0082, S0092, S0501, S0503, S0504, S0505, S0507, S0508, S0509, S0510, S0511, S1004, S1008, S1034, S1046, S1060, S1504, S1506, S2010, S2501, S2556

Job Role Details	
Job Role Name	Secure Cloud Specialist
Job Role ID	CARD-CA-002
Category	Cybersecurity Architecture, Research and Development
Specialty Area	Cybersecurity Architecture
Job Role Description	Designs, implements and operates secure cloud computing systems and develops secure cloud policies.
Competency Areas	Identity and Access Management (CA001), Cloud Security (CA002), Communications Security (CA003), Operating Systems Security (CA005), Data Security and Administration (CA007)
Tasks	T0003, T0004, T0005, T0011, T0013, T0014, T0015, T0040, T0103, T0107, T0134, T0139, T0500, T0502, T0503, T0504, T0505, T0511, T0524, T0526, T0527, T0532, T0533, T0536, T0542, T0543, T1007, T1016, T1017, T1049, T1050, T1112, T1529, T4011, T4509
Knowledge	K0001, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0019, K0025, K0035, K0042, K0044, K0045, K0046, K0048, K0054, K0056, K0061, K0062, K0069, K0074, K0070, K0080, K0084, K0085, K0106, K0113, K0121, K0124, K0126, K0128, K0132, K0136, K0178, K0180, K0182, K0183, K0185, K0186, K0187, K0188, K0189, K0190, K0191, K0207, K0208, K0500, K0516, K0517, K0518, K0519, K0521, K1011, K1047, K1052, K1504, K1514, K2001, K2511, K3008, K3009, K5524, K5532
Skills	S0003, S0004, S0012, S0018, S0019, S0021, S0039, S0040, S0055, S0058, S0060, S0061, S0062, S0064, S0065, S0071, S0073, S0077, S0078, S0085, S0086, S0088, S0106, S0504, S0505, S0508, S1004, S1007, S1504, S2010, S2501, S2512, S2533, S2546, S2550

Job Role Details	
Job Role Name	Systems Security Development Specialist
Job Role ID	CARD-CRD-001
Category	Cybersecurity Architecture, Research and Development
Specialty Area	Cybersecurity Research and Development
Job Role Description	Designs, develops, tests and evaluates security of information systems throughout the development life-cycle.
Competency Areas	Secure Software Development (CA014), Cybersecurity Testing (CA024)
Tasks	T0004, T0013, T0014, T0022, T0040, T0089, T0096, T0103, T0107, T0138, T0158, T0507, T0508, T0511, T0524, T0526, T0527, T0534, T0536, T1004, T1007, T1008, T1015, T1016, T1017, T1018, T1021, T1022, T1026, T1027, T1029, T1031, T1033, T1034, T1038, T1042, T1044, T1048, T1049, T1050, T1051, T1052, T1053, T1058, T1062, T1063, T1079, T1081, T1087, T1088, T1089, T1090, T1091, T1102, T1104, T1105, T1111, T1112, T1113, T1114, T1117, T1120, T1122, T1123, T1126
Knowledge	K0001, K0002, K0003, K0004, K0005, K0014, K0016, K0020, K0022, K0024, K0027, K0035, K0042, K0045, K0046, K0048, K0049, K0054, K0056, K0057, K0058, K0061, K0062, K0063, K0069, K0073, K0074, K0076, K0080, K0092, K0093, K0095, K0097, K0100, K0101, K0111, K0113, K0124, K0125, K0126, K0128, K0133, K0136, K0146, K0149, K0170, K0172, K0173, K0176, K0178, K0180, K0182, K0183, K0185, K0186, K0187, K0188, K0189, K0193, K0194, K0197, K0205, K0210, K0516, K0517, K0518, K0520, K1005, K1006, K1007, K1008, K1009, K1011, K1014, K1015, K1017, K1024, K1036, K1041, K1047, K1048, K1050, K1051, K1052, K1053, K1057, K1064, K1068, K1504, K1514, K2511, K3008, K3009, K3508, K4008, K4027, K5012, K5040, K5503, K5524, K5536, K6012
Skills	S0001, S0003, S0004, S0008, S0012, S0018, S0023, S0028, S0039, S0040, S0053, S0055, S0058, S0061, S0062, S0064, S0065, S0066, S0068, S0070, S0071, S0072, S0073, S0074, S0075, S0077, S0078, S0082, S0083, S0084, S0086, S0091, S0092, S0106, S0504, S0505, S0508, S0509, S1000, S1004, S1007, S1008, S1010, S1016, S1034, S1039, S1040, S1041, S1049, S1052, S1053, S1060, S1504, S2010, S2512, S2533, S2546, S2550, S5503

Job Role Details	
Job Role Name	Cybersecurity Developer
Job Role ID	CARD-CRD-002
Category	Cybersecurity Architecture, Research and Development
Specialty Area	Cybersecurity Research and Development
Job Role Description	Develops cybersecurity software, applications, systems and products.
Competency Areas	Secure Software Development (CA014)
Tasks	T0013, T0014, T0035, T0039, T0040, T0089, T0091, T0107, T0511, T0527, T0536, T1002, T1003, T1005, T1006, T1009, T1010, T1011, T1013, T1014, T1015, T1023, T1029, T1031, T1035, T1036, T1040, T1043, T1049, T1050, T1051, T1052, T1054, T1055, T1058, T1062, T1071, T1075, T1078, T1081, T1085, T1091, T1092, T1102, T1104, T1105, T1108, T1109, T1110, T1115, T1116, T1123, T1124, T1125, T1127, T1132, T5060
Knowledge	K0001, K0002, K0003, K0004, K0005, K0015, K0022, K0024, K0030, K0035, K0039, K0042, K0045, K0051, K0054, K0056, K0063, K0069, K0074, K0076, K0080, K0083, K0093, K0095, K0097, K0100, K0112, K0113, K0124, K0125, K0126, K0128, K0136, K0146, K0147, K0170, K0171, K0172, K0173, K0174, K0175, K0178, K0180, K0182, K0183, K0185, K0186, K0187, K0188, K0189, K0194, K0205, K0212, K0516, K0517, K0518, K1000, K1005, K1008, K1011, K1012, K1013, K1014, K1015, K1017, K1021, K1023, K1024, K1039, K1040, K1041, K1047, K1048, K1050, K1053, K1057, K1059, K1064, K1068, K1504, K1514, K3008, K3009, K3508, K4008, K4027, K5012, K5040, K5503, K6012
Skills	S0001, S0003, S0004, S0017, S0018, S0036, S0038, S0039, S0040, S0045, S0047, S0048, S0053, S0055, S0058, S0061, S0064, S0065, S0066, S0067, S0068, S0070, S0073, S0077, S0078, S0082, S0086, S0092, S0106, S0504, S0505, S0508, S1000, S1001, S1002, S1003, S1004, S1007, S1008, S1010, S1016, S1026, S1031, S1034, S1039, S1040, S1041, S1047, S1052, S1055, S1056, S1057, S1059, S1060, S1504, S2010, S2018, S2533, S2546, S2550

Job Role Details	
Job Role Name	Secure Software Assessor
Job Role ID	CARD-CRD-003
Category	Cybersecurity Architecture, Research and Development
Specialty Area	Cybersecurity Research and Development
Job Role Description	Assesses the security of computer applications, software, code or programs and provides actionable results.
Competency Areas	Identity and Access Management (CA001), Secure Software Development (CA014), Cybersecurity Testing (CA024)
Tasks	T0013, T0014, T0039, T0040, T0107, T0138, T0511, T0527, T0536, T1005, T1006, T1009, T1012, T1013, T1016, T1024, T1025, T1029, T1031, T1035, T1040, T1041, T1043, T1046, T1049, T1050, T1054, T1055, T1076, T1078, T1081, T1092, T1104, T1105, T1115, T1116, T1123, T1127, T1131, T1133, T1134, T4011
Knowledge	K0003, K0004, K0005, K0015, K0022, K0030, K0035, K0039, K0042, K0045, K0051, K0054, K0056, K0062, K0069, K0074, K0076, K0080, K0083, K0093, K0100, K0112, K0113, K0117, K0124, K0125, K0126, K0128, K0136, K0146, K0153, K0171, K0175, K0186, K0187, K0188, K0189, K0205, K0213, K0214, K1000, K1008, K1011, K1012, K1013, K1014, K1015, K1017, K1021, K1023, K1024, K1037, K1047, K1048, K1050, K1057, K1064, K1068, K1504, K1514, K3008, K3009, K5503
Skills	S0001, S0003, S0004, S0018, S0036, S0038, S0040, S0047, S0048, S0055, S0058, S0061, S0062, S0065, S0066, S0067, S0068, S0070, S0073, S0077, S0078, S0082, S0086, S0091, S0092, S0106, S0504, S0505, S1004, S1007, S1008, S1010, S1039, S1053, S1056, S1057, S1504, S2010, S2512, S2533, S2546, S2547, S2549, S2550, S5526

Job Role Details	
Job Role Name	Cybersecurity Researcher
Job Role ID	CARD-CRD-004
Category	Cybersecurity Architecture, Research and Development
Specialty Area	Cybersecurity Research and Development
Job Role Description	Conducts scientific research in the cybersecurity field.
Competency Areas	All competencies relevant to the fields of research.
Tasks	T0009, T0013, T0040, T0052, T0068, T0089, T0090, T0103, T0107, T0163, T0164, T0529, T1007, T1016, T1019, T1045, T1050, T1051, T1057, T1058, T1073, T1074, T1091, T1093, T1099, T1118, T1119, T1121, T1128, T1129, T1135, T5500, T6006, T6010
Knowledge	K0003, K0004, K0005, K0009, K0017, K0035, K0042, K0044, K0054, K0056, K0069, K0073, K0074, K0080, K0092, K0093, K0094, K0095, K0096, K0097, K0098, K0100, K0112, K0113, K0114, K0124, K0128, K0135, K0136, K0153, K0159, K0170, K0174, K0175, K0181, K0185, K0186, K0187, K0188, K0189, K0192, K0204, K0205, K0213, K0214, K1030, K1031, K1032, K1034, K1035, K1038, K1047, K1058, K1060, K1062, K1063, K1504, K1514, K3008, K3009, K5524
Skills	S0001, S0003, S0004, S0018, S0039, S0040, S0045, S0049, S0051, S0055, S0058, S0061, S0068, S0077, S0078, S0082, S0086, S0090, S0092, S0504, S1002, S1007, S1024, S1028, S1035, S1055, S1056, S1057, S1502, S1504, S2010, S2512, S2533, S2546, S2550, S5500

Job Role Details	
Job Role Name	Cybersecurity Data Science Specialist
Job Role ID	CARD-CRD-005
Category	Cybersecurity Architecture, Research and Development
Specialty Area	Cybersecurity Research and Development
Job Role Description	Uses mathematical models and scientific methods and processes to design and implement algorithms and systems that extract cybersecurity insights and knowledge from multiple large-scale data sets.
Competency Areas	Data Security and Administration (CA007), Artificial Intelligence Security (CA015)
Tasks	T0009, T0068, T0080, T0083, T0084, T1000, T1001, T1020, T1034, T1039, T1059, T1060, T1061, T1062, T1064, T1066, T1069, T1070, T1071, T1072, T1083, T1098, T1100, T1101, T1106, T1502, T5031
Knowledge	K0003, K0004, K0005, K0014, K0015, K0018, K0019, K0020, K0035, K0039, K0042, K0045, K0049, K0051, K0054, K0059, K0069, K0074, K0075, K0076, K0080, K0105, K0107, K0108, K0113, K0124, K0126, K0133, K0156, K0169, K0170, K0186, K0187, K0188, K0189, K0193, K0197, K1000, K1001, K1002, K1003, K1005, K1010, K1016, K1021, K1025, K1027, K1028, K1036, K1045, K1047, K1049, K1052, K1054, K1064, K1065, K1066, K1067, K1069, K1511, K3000, K3001, K3008, K3009, K3010, K3011, K3012, K4009, K4011, K4012, K5008, K5017, K5034, K5503
Skills	S0017, S0018, S0026, S0029, S0030, S0031, S0032, S0045, S0055, S0058, S0066, S0067, S0069, S0070, S0077, S0078, S0086, S0091, S0100, S1000, S1002, S1005, S1006, S1009, S1012, S1013, S1014, S1015, S1016, S1017, S1018, S1019, S1020, S1021, S1022, S1023, S1029, S1030, S1034, S1042, S1043, S1044, S1045, S1046, S1047, S1048, S1050, S1051, S1053, S1054, S1055, S1056, S1057, S1058, S1060, S1504, S2522, S2525, S2541, S2546, S2550, S2554, S3501, S4006, S5503, S5516, S5517, S5525, S5527

Job Role Details	
Job Role Name	Cybersecurity Artificial Intelligence Specialist
Job Role ID	CARD-CRD-006
Category	Cybersecurity Architecture, Research and Development
Specialty Area	Cybersecurity Research and Development
Job Role Description	Uses artificial intelligence models and techniques (including machine learning ones) to design and implement algorithms and systems that automate and improve the efficiency and effectiveness of cybersecurity tasks.
Competency Areas	Artificial Intelligence Security (CA015)
Tasks	T0083, T0134, T1060, T1061, T1064, T1071, T1072, T1094, T1096, T1098, T1099, T1100, T1101, T1130, T3033
Knowledge	K0001, K0002, K0003, K0004, K0005, K0014, K0015, K0018, K0030, K0035, K0051, K0059, K0074, K0119, K0186, K0187, K0188, K0189, K1021, K1028, K1039, K1040, K1041, K1043, K1045, K1047, K1055, K1056, K1058, K3009, K3010, K5503
Skills	S0017, S0058, S0066, S0067, S1000, S1002, S1020, S1023, S1031, S1032, S1034, S1035, S1036, S1055, S1059, S1060

3.1.2 Category Group: Leadership and Workforce Development (LWD)

Job Role Details	
Job Role Name	Chief Information Security Officer/Director
Job Role ID	LWD-L-001
Category	Leadership and Workforce Development
Specialty Area	Leadership
Job Role Description	Directs cybersecurity work within an organization, establishes vision and direction for its cybersecurity and related strategies, resources and activities and advises the leadership on the effective management of the organization's cyber risks.
Competency Areas*	Security Program Management (CA012), Business Continuity and Disaster Recovery (CA023)
Tasks	T0001, T0002, T0011, T0017, T0042, T0043, T0053, T0061, T0085, T0095, T0105, T0108, T0112, T0127, T0128, T0130, T0137, T0140, T0153, T0165, T1501, T1503, T1511, T1513, T1522, T1524, T1525, T1526, T1528, T1529, T1531, T1534, T1535, T1541, T1546, T1547, T1548, T1549, T2000, T2003, T2007, T2008, T2009, T2060, T2526, T4509
Knowledge	K0001, K0003, K0004, K0005, K0008, K0009, K0021, K0029, K0034, K0035, K0037, K0044, K0054, K0061, K0064, K0069, K0073, K0074, K0080, K0092, K0093, K0100, K0113, K0128, K0186, K0187, K0188, K0189, K0205, K0213, K0214, K1506, K1509, K1515, K2013, K2014, K2021, K2022, K2023, K2024, K2025, K2027, K2511, K2513, K3009, K5503, K5524
Skills	S0004, S0018, S0051, S0055, S0058, S0059, S0077, S0078, S0079, S0080, S0082, S0086, S0087, S0088, S0505, S1500, S1501, S1502, S1504, S1506, S1507, S1510, S2501, S2512, S2542, S2546, S2550, S2555

Job Role Details	
Job Role Name	Cybersecurity Manager
Job Role ID	LWD-L-002
Category	Leadership and Workforce Development
Specialty Area	Leadership
Job Role Description	Manages the security of information systems and functions within an organization. Leads a cybersecurity team, unit and/or enterprise level function.
Competency Areas	All competencies relevant to the area they are managing.
Tasks	T0001, T0002, T0011, T0016, T0017, T0023, T0042, T0048, T0053, T0059, T0061, T0063, T0074, T0108, T0112, T0128, T0130, T0137, T0140, T0153, T1502, T1503, T1504, T1505, T1506, T1507, T1510, T1511, T1513, T1516, T1518, T1520, T1521, T1522, T1523, T1524, T1525, T1526, T1527, T1528, T1529, T1530, T1531, T1532, T1534, T1542, T1543, T1545, T1546, T1550, T1551, T1552, T1553, T1554, T2000, T2007, T2008, T2009, T2060, T2510, T2514, T2526, T4509
Knowledge	K0001, K0003, K0004, K0005, K0008, K0019, K0021, K0024, K0029, K0031, K0034, K0035, K0037, K0043, K0044, K0046, K0056, K0061, K0064, K0069, K0073, K0074, K0090, K0092, K0093, K0100, K0101, K0113, K0124, K0125, K0126, K0128, K0133, K0159, K0169, K0176, K0186, K0187, K0188, K0189, K0194, K0205, K0213, K0214, K1500, K1501, K1504, K1505, K1506, K1509, K1511, K1512, K1513, K1514, K1515, K2013, K2014, K2022, K2023, K2024, K2025, K2027, K2030, K2501, K2511, K2513, K3009, K5503, K5524
Skills	S0004, S0009, S0040, S0077, S0078, S0079, S0080, S0082, S0085, S0086, S1007, S1500, S1501, S1504, S1506, S1507, S1510, S1511, S2555, S3001

* In addition to minimum understanding across all other competency areas

Job Role Details	
Job Role Name	Cybersecurity Advisor
Job Role ID	LWD-L-003
Category	Leadership and Workforce Development
Specialty Area	Leadership
Job Role Description	Provides expert consultancy and advice on cybersecurity topics to an organization's leadership and to its cybersecurity leadership and teams.
Competency Areas	All competencies relevant to the area they are advising on.
Tasks	T0001, T0002, T0003, T0011, T0016, T0017, T0042, T0048, T0053, T0112, T0128, T0130, T0138, T0139, T0140, T1501, T1503, T1511, T1525, T1528, T1529, T1537, T1538, T1539, T1540, T1543, T1544, T1554, T1555, T1556, T1557, T2003, T2526, T4509
Knowledge	K0001, K0002, K0003, K0004, K0005, K0008, K0016, K0019, K0021, K0029, K0031, K0034, K0035, K0037, K0044, K0046, K0056, K0061, K0064, K0069, K0073, K0090, K0092, K0093, K0100, K0101, K0113, K0124, K0128, K0133, K0159, K0169, K0176, K0186, K0187, K0188, K0189, K0205, K0214, K1500, K1501, K1502, K1503, K1504, K1505, K1506, K1509, K1510, K1511, K1512, K1513, K1514, K1515, K2027, K2511, K2513, K3009, K5524
Skills	S0004, S0018, S0051, S0055, S0058, S0075, S0077, S0078, S0079, S0080, S0082, S0085, S0086, S0087, S0088, S0090, S0505, S1048, S1049, S1500, S1501, S1502, S1504, S1506, S1507, S1510, S2501, S2512, S2542, S2546, S2548, S2550, S2555

Job Role Details	
Job Role Name	Cybersecurity Human Capital Manager
Job Role ID	LWD-WD-001
Category	Leadership and Workforce Development
Specialty Area	Workforce Development
Job Role Description	Develops plans, strategies and guidance within an organization to support the development and management of the cybersecurity workforce.
Competency Areas	Cybersecurity Training and Awareness (CA020)
Tasks	T0002, T0017, T0046, T0078, T0082, T0085, T0086, T0088, T0095, T0103, T0108, T0109, T0112, T0140, T0160, T0161, T0162, T0163, T0164, T0165, T1503, T1510, T1511, T1516, T1520, T1521, T1522, T1524, T1525, T1527, T1528, T1529, T1530, T1535, T1541, T1542, T1543, T2003, T2006, T2007, T2009, T2510, T2514, T2022, T2023, T2025, T2026, T2027, T2028, T2031, T2032, T2033, T2034, T2035, T2038, T2039, T2040, T2047, T2053, T2055, T2059, T2062, T2063, T2065, T2069
Knowledge	K0001, K0003, K0004, K0005, K0035, K0058, K0061, K0074, K0080, K0092, K0186, K0187, K0188, K0189, K0215, K0216, K1501, K2002, K2011, K2013, K2014, K2022, K2023, K2024, K2025, K2026, K2027, K2029, K2030, K2031, K2032
Skills	S0018, S0055, S0058, S0077, S0078, S0087, S0088, S1500, S1504, S2008, S2015, S2016, S2017, S2512, S2546, S2549, S2550

Job Role Details	
Job Role Name	Cybersecurity Instructional Curriculum Developer
Job Role ID	LWD-WD-002
Category	Leadership and Workforce Development
Specialty Area	Workforce Development
Job Role Description	Develops, plans, coordinates and evaluates cybersecurity training, awareness, and education programs, courses, contents, methods and techniques based on instructional needs.
Competency Areas*	Cybersecurity Training and Awareness (CA020)
Tasks	T0052, T0082, T0085, T0163, T0165, T1528, T2004, T2005, T2010, T2011, T2012, T2013, T2014, T2015, T2016, T2017, T2018, T2019, T2020, T2021, T2022, T2024, T2028, T2029, T2036, T2040, T2044, T2046, T2049, T2050, T2051, T2053, T2054, T2055, T2056, T2057, T2058, T2061, T2064, T2066, T2070, T2072, T2073, T2075, T2076
Knowledge	K0001, K0002, K0003, K0004, K0005, K0035, K0044, K0061, K0074, K0080, K0186, K0187, K0188, K0189, K1061, K2000, K2002, K2004, K2005, K2007, K2009, K2011, K2012, K2013, K2014, K2015, K2021, K2022, K2023, K2024, K2025, K2026, K2027, K2028, K2034, K2036, K2037
Skills	S0001, S0004, S0018, S0023, S0026, S0034, S0051, S0055, S0058, S0069, S0075, S0077, S0078, S0086, S0092, S1504, S2001, S2003, S2004, S2006, S2010, S2012, S2014, S2017, S2018, S2019, S2020, S2023, S2024, S2026, S2028, S2029, S2542, S2546, S2550, S5503

Job Role Details	
Job Role Name	Cybersecurity Instructor
Job Role ID	LWD-WD-003
Category	Leadership and Workforce Development
Specialty Area	Workforce Development
Job Role Description	Teaches, trains, develops and tests people in cybersecurity topics and awareness to encourage secure behaviors.
Competency Areas*	Cybersecurity Training and Awareness (CA020)
Tasks	T0083, T0084, T1528, T2002, T2005, T2010, T2011, T2012, T2013, T2014, T2015, T2016, T2017, T2018, T2019, T2020, T2022, T2024, T2028, T2029, T2036, T2040, T2042, T2044, T2046, T2048, T2049, T2050, T2051, T2054, T2055, T2061, T2064, T2066, T2067, T2068, T2071, T2074, T2075, T2077
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0035, K0044, K0074, K0080, K0133, K0186, K0187, K0188, K0189, K0190, K2000, K2001, K2002, K2004, K2005, K2007, K2009, K2010, K2012, K2014, K2015, K2020, K2021, K2028, K2033, K2034, K2035, K2036, K2037
Skills	S0001, S0004, S0017, S0018, S0019, S0021, S0023, S0026, S0027, S0034, S0041, S0051, S0055, S0058, S0069, S0077, S0086, S0092, S1502, S1504, S2001, S2002, S2003, S2006, S2010, S2012, S2013, S2014, S2018, S2019, S2020, S2021, S2022, S2023, S2024, S2025, S2027, S2028, S2501, S2542, S2546, S2548, S2549, S2550, S3501, S4504, S4505, S5012, S5503

* In addition to the competency areas related to the curricula they are developing
* In addition to the competency areas related to the training they are delivering

3.1.3 Category Group: Governance, Risk, Compliance and Laws (GRCL)

Job Role Details	
Job Role Name	Cybersecurity Risk Officer
Job Role ID	GRCL-GRC-001
Category	Governance, Risk, Compliance and Laws
Specialty Area	Governance, Risk and Compliance
Job Role Description	Identifies, assesses and manages an organization's cybersecurity risks to protect its information and technology assets in line with organizational policies and procedures and related laws and regulations.
Competency Areas	Security Risk Analysis (CA008), Supply Chain Security (CA006), Business Continuity and Disaster Recovery (CA023)
Tasks	T0001, T0003, T0006, T0011, T0012, T0013, T0014, T0015, T0017, T0037, T0039, T0042, T0043, T0053, T0105, T0107, T0108, T0127, T0128, T0130, T0132, T0133, T0138, T0139, T0140, T0146, T1503, T1506, T1522, T1524, T1529, T1545, T2000, T2060, T2500, T2507, T2513, T2526, T2528, T2529, T2530, T2536, T2537, T2538, T3031, T4010, T4014, T4033, T4509
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0021, K0029, K0035, K0037, K0073, K0074, K0080, K0081, K0083, K0092, K0107, K0160, K0166, K0167, K0186, K0187, K0188, K0189, K0190, K2507, K2511, K2513, K5503, K6005
Skills	S0012, S0018, S0040, S0044, S0055, S0056, S0057, S0058, S0062, S0075, S0077, S0078, S0079, S0080, S0081, S0082, S0088, S0089, S0091, S1007, S1504, S1506, S1507, S2546, S2550, S2553, S2555, S4507

Job Role Details	
Job Role Name	Cybersecurity Compliance Officer
Job Role ID	GRCL-GRC-002
Category	Governance, Risk, Compliance and Laws
Specialty Area	Governance, Risk and Compliance
Job Role Description	Ensures an organization's cybersecurity program complies with applicable requirements, policies and standards.
Competency Areas	Cybersecurity Regulations and Compliance (CA021), Data Protection (CA022)
Tasks	T0003, T0019, T0022, T0023, T0063, T0082, T0111, T0139, T2500, T2501, T2504, T2506, T2509, T2514, T2515, T2519, T2522, T2523, T2524, T2525, T2527, T2529, T2530, T2534, T2535, T2539, T2540, T2541, T2542, T2543, T2544, T3031, T3039, T3052, T3056
Knowledge	K0001, K0002, K0003, K0004, K0005, K0008, K0035, K0074, K0186, K0187, K0188, K0189, K0190, K2506, K2507, K2509, K2510, K2512, K5503
Skills	S0018, S0051, S0055, S0058, S0061, S0062, S0073, S0077, S0078, S0087, S0088, S1500, S1504, S1506, S1507, S2014, S2512, S2542, S2546, S2550

Job Role Details	
Job Role Name	Cybersecurity Policy Officer
Job Role ID	GRCL-GRC-003
Category	Governance, Risk, Compliance and Laws
Specialty Area	Governance, Risk and Compliance
Job Role Description	Develops, updates and maintains cybersecurity policies to support and align with an organization's cybersecurity requirements.
Competency Areas	Cybersecurity Regulations and Compliance (CA021), Data Protection (CA022)
Tasks	T0011, T0017, T0046, T0082, T0085, T0086, T0088, T0095, T0103, T0108, T0109, T0140, T0160, T0161, T0162, T0163, T0164, T0165, T1020, T1525, T1546, T2006, T2028, T2510, T2515, T3001, T3002, T3004, T3005, T3007, T3008, T3037
Knowledge	K0001, K0002, K0003, K0004, K0005, K0008, K0018, K0019, K0021, K0029, K0037, K0074, K0092, K0169, K0186, K0187, K0188, K0189, K0195, K0200, K1514, K2013, K2014, K2024, K2025, K2504, K2505, K2516, K3010, K3011, K4016, K4513, K5003, K5006, K5007, K5037, K5503
Skills	S0075, S0077, S0081, S0087, S0088, S1500, S1504, S1506, S1507, S2512, S2513, S2530, S3000, S5503

Job Role Details	
Job Role Name	Security Controls Assessor
Job Role ID	GRCL-GRC-004
Category	Governance, Risk, Compliance and Laws
Specialty Area	Governance, Risk and Compliance
Job Role Description	Analyzes cybersecurity controls and assesses their effectiveness.
Competency Areas	Security Risk Analysis (CA008)
Tasks	T0036, T0037, T0039, T0043, T0050, T0053, T0061, T0074, T0079, T0136, T0146, T0153, T2503, T2505, T2507, T2508, T2509, T2511, T2512, T2514, T2516, T2521, T2531, T2532, T2533, T2535
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0013, K0016, K0017, K0019, K0020, K0021, K0022, K0028, K0029, K0031, K0035, K0037, K0042, K0044, K0061, K0069, K0073, K0074, K0080, K0084, K0085, K0086, K0092, K0093, K0100, K0113, K0124, K0125, K0126, K0128, K0133, K0134, K0146, K0147, K0153, K0169, K0176, K0180, K0183, K0185, K0186, K0187, K0188, K0189, K0190, K0191, K0192, K0193, K0205, K0212, K0213, K0214, K1017, K1511, K2501, K2502, K2509, K2514, K2515, K5503, K5536
Skills	S0001, S0004, S0018, S0023, S0026, S0036, S0037, S0040, S0044, S0045, S0046, S0047, S0048, S0050, S0051, S0055, S0058, S0061, S0064, S0068, S0070, S0073, S0077, S0078, S0082, S0085, S0086, S0092, S0096, S0102, S0103, S0505, S1008, S1009, S1020, S1029, S1058, S1500, S1502, S1504, S2003, S2010, S2023, S2024, S2500, S2501, S2502, S2504, S2506, S2507, S2509, S2512, S2513, S2517, S2521, S2523, S2524, S2525, S2527, S2529, S2530, S2533, S2537, S2540, S2541, S2542, S2543, S2544, S2546, S2547, S2548, S2549, S2550, S2551, S2552, S2554, S2556, S2557, S2558, S3000, S4004, S5503, S5526

Job Role Details	
Job Role Name	Cybersecurity Auditor
Job Role ID	GRCL-GRC-005
Category	Governance, Risk, Compliance and Laws
Specialty Area	Governance, Risk and Compliance
Job Role Description	Designs, performs and manages cybersecurity audits to assess an organization's compliance with applicable requirements, policies, standards and controls. Prepares audit reports and communicates them to authorized parties.
Competency Areas	Security Risk Analysis (CA008)
Tasks	T0024, T0037, T0039, T0041, T0043, T0048, T0053, T0060, T0061, T0074, T0109, T0136, T0147, T0153, T0160, T0161, T0162, T0163, T0164, T2505, T2508, T2509, T2510, T2511, T2512, T2515, T2531, T2532, T2535, T3057
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0011, K0013, K0021, K0022, K0028, K0029, K0035, K0037, K0042, K0044, K0056, K0069, K0074, K0080, K0084, K0085, K0086, K0109, K0113, K0124, K0125, K0126, K0128, K0133, K0134, K0144, K0186, K0187, K0188, K0189, K0190, K0191, K0205, K0209, K0211, K2501, K2505, K2506, K2507, K2509, K2516, K5503
Skills	S0001, S0004, S0019, S0023, S0026, S0028, S0036, S0040, S0048, S0051, S0055, S0058, S0061, S0064, S0068, S0073, S0076, S0077, S0078, S0082, S0086, S0092, S0096, S0103, S0505, S1008, S1009, S1020, S1029, S1058, S1500, S1504, S2003, S2010, S2023, S2024, S2501, S2502, S2504, S2506, S2509, S2512, S2513, S2516, S2521, S2523, S2525, S2526, S2527, S2533, S2537, S2540, S2541, S2542, S2543, S2546, S2548, S2549, S2550, S2551, S2552, S2554, S2556, S2557, S2558, S3000, S5503

Job Role Details	
Job Role Name	Cybersecurity Legal Specialist
Job Role ID	GRCL-LDP-001
Category	Governance, Risk, Compliance and Laws
Specialty Area	Laws and Data Protection
Job Role Description	Provides legal services on topics related to cyber laws and regulations.
Competency Areas	Cybersecurity Regulations and Compliance (CA021)
Tasks	T0003, T0019, T0063, T0088, T0147, T1501, T2514, T2526, T2544, T3001, T3002, T3004, T3005, T3007, T3008, T3010, T3052, T5009
Knowledge	K0002, K0003, K0004, K0005, K0044, K0065, K0074, K0081, K0084, K0125, K0126, K0128, K0187, K0188, K0189, K0198, K0199, K0200, K0201, K0202, K2509, K2510, K2513, K3000, K3001, K3002, K3011, K3012, K3509, K5015, K5032, K5503
Skills	S0058, S0077, S0088, S1504, S3003, S3004, S3005

Job Role Details	
Job Role Name	Data Protection Officer
Job Role ID	GRCL-LDP-002
Category	Governance, Risk, Compliance and Laws
Specialty Area	Laws and Data Protection
Job Role Description	Analyzes data protection risks and ensures compliance with applicable laws. Oversees the implementation of data protection policies and procedures. Supports organizational response to data protection incidents.
Competency Areas	Data Protection (CA022)
Tasks	T0019, T0023, T0063, T0127, T2514, T2521, T2522, T3013, T3014, T3019, T3023, T3025, T3026, T3029, T3030, T3031, T3033, T3036, T3037, T3038, T3039, T3041, T3042, T3049, T3050, T3051, T3052, T3056, T3057
Knowledge	K0002, K0003, K0004, K0005, K0008, K0029, K0035, K0074, K0187, K0188, K0189, K2506, K2507, K2509, K2512, K3005, K3008, K3009, K3010, K5503
Skills	S0018, S0055, S0058, S0061, S0064, S0077, S0078, S0087, S0088, S1504, S2546, S2550, S3000, S3002

3.1.4 Category Group: Protection and Defense (PD)

Job Role Details	
Job Role Name	Cybersecurity Defense Analyst
Job Role ID	PD-D-001
Category	Protection and Defense
Specialty Area	Defense
Job Role Description	Uses data collected from cyber defense tools to analyze events that occur within their organization to detect and mitigate cyber threats.
Competency Areas	Identity and Access Management (CA001), Communications Security (CA003), Data Security and Administration (CA007), Vulnerability Management (CA013), Cyber Threat Intelligence (CA019), Cybersecurity Testing (CA024)
Tasks	T0009, T0015, T0025, T0028, T0029, T0037, T0040, T0044, T0054, T0055, T0056, T0064, T0067, T0068, T0069, T0070, T0071, T0072, T0073, T0075, T0076, T0097, T0098, T0100, T0101, T0102, T0107, T0111, T0122, T0138, T0141, T0151, T0152, T0155, T0156, T0157, T0159, T1025, T1543, T3500, T3503, T3504, T5057
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0013, K0014, K0016, K0017, K0020, K0024, K0031, K0035, K0042, K0043, K0044, K0045, K0046, K0049, K0053, K0054, K0058, K0063, K0064, K0065, K0068, K0069, K0070, K0072, K0074, K0076, K0077, K0078, K0084, K0086, K0087, K0088, K0090, K0099, K0100, K0101, K0102, K0103, K0104, K0113, K0117, K0124, K0125, K0126, K0134, K0136, K0137, K0139, K0145, K0146, K0147, K0153, K0159, K0176, K0177, K0179, K0184, K0186, K0187, K0188, K0189, K0190, K0191, K0192, K0193, K0194, K0197, K0198, K0199, K0200, K0201, K0202, K0205, K0206, K0212, K0213, K0214, K3506, K3507, K3508, K5503
Skills	S0001, S0006, S0009, S0012, S0015, S0023, S0033, S0040, S0041, S0046, S0048, S0056, S0057, S0061, S0063, S0069, S0092, S0097, S0101, S0104, S1506, S1508, S1509, S2002, S2520, S2522, S2526, S2543, S2544, S3500, S3501, S3502, S4006, S5012, S5018, S5026, S5503, S5524, S5525, S5532

Job Role Details	
Job Role Name	Cybersecurity Infrastructure Specialist
Job Role ID	PD-D-002
Category	Protection and Defense
Specialty Area	Defense
Job Role Description	Tests, implements, deploys, maintains and administers hardware and software that protect and defend systems and networks against cybersecurity threats.
Competency Areas	Cloud Security (CA002), Communications Security (CA003), Operating Systems Security (CA005), Hardware and Firmware Security (CA016)
Tasks	T0005, T0038, T0057, T0147, T1543, T3502, T3506, T3507, T3508, T3511, T4023
Knowledge	K0001, K0002, K0003, K0004, K0005, K0017, K0019, K0024, K0035, K0043, K0046, K0063, K0064, K0074, K0084, K0100, K0104, K0119, K0147, K0159, K0177, K0179, K0184, K0186, K0187, K0188, K0189, K0192, K0194, K0205, K0206, K0212, K0519, K1052, K3502, K3509, K5012
Skills	S0001, S0005, S0008, S0009, S0014, S0016, S0021, S0022, S0035, S0038, S0040, S0061, S0065, S0068, S0069, S0071, S0082, S0085, S0092, S0096, S0106, S0506, S1007, S1047, S2011, S2507, S3500, S4006, S5526, S5532

Job Role Details	
Job Role Name	Cybersecurity Specialist
Job Role ID	PD-D-003
Category	Protection and Defense
Specialty Area	Defense
Job Role Description	Provides general cybersecurity support. Assists in cybersecurity tasks.
Competency Areas	Identity and Access Management (CA001), Communications Security (CA003), Operating Systems Security (CA005), Data Security and Administration (CA007)
Tasks	T0005, T0009, T0026, T0028, T0102, T0113, T0142, T3500, T3503, T3504
Knowledge	K0001, K0004, K0005, K0007, K0009, K0013, K0014, K0017, K0019, K0020, K0024, K0031, K0035, K0043, K0045, K0051, K0053, K0063, K0068, K0074, K0084, K0104, K0119, K0159, K0171, K0179, K0184, K0186, K0188, K0189, K0190, K0191, K0192, K0193, K0194, K0206, K5536
Skills	S0001, S0002, S0009, S0012, S0019, S0021, S0022, S0023, S0027, S0028, S0035, S0062, S0068, S0083, S0084, S0085, S0092, S0093, S0094, S0095, S0104, S1052, S2011, S2526, S3501, S3502, S4006, S5025, S5532

Job Role Details	
Job Role Name	Cryptography Specialist
Job Role ID	PD-P-001
Category	Protection and Defense
Specialty Area	Protection
Job Role Description	Develops, evaluates, analyzes and identifies weaknesses of, and improvements to, cryptography systems and algorithms.
Competency Areas	Identity and Access Management (CA001), Cryptography (CA004), Data Security and Administration (CA007)
Tasks	T0010, T0016, T0091, T0096, T0158, T4000, T4008, T4021, T4022, T4034
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0010, K0014, K0015, K0016, K0017, K0018, K0024, K0028, K0029, K0030, K0035, K0039, K0042, K0044, K0046, K0051, K0053, K0074, K0102, K0112, K0113, K0170, K0175, K0176, K0186, K0187, K0188, K0189, K0190, K0192, K0194, K1000, K1011, K1060, K1062, K1063, K4000, K4009, K4011, K4015, K4017, K4020, K4030
Skills	S0004, S0016, S0038, S0039, S0061, S0066, S0067, S1002, S1055, S1056, S1057, S4001, S4002, S4003, S4006, S4009, S5022

Job Role Details	
Job Role Name	Identity and Access Management Specialist
Job Role ID	PD-P-002
Category	Protection and Defense
Specialty Area	Protection
Job Role Description	Manages individuals and entities identities and access to resources through applying identification, authentication and authorization systems and processes.
Competency Areas	Identity and Access Management (CA001)
Tasks	T0100, T1049, T3508, T4016, T4017, T4018, T4019, T4024, T4025, T4026, T4027, T4028, T4029, T4035, T4036
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0013, K0024, K0028, K0035, K0042, K0049, K0059, K0074, K0085, K0106, K0107, K0112, K0124, K0125, K0126, K0133, K0144, K0156, K0175, K0186, K0187, K0188, K0189, K0190, K0191, K0194, K0197, K0207, K0208, K0211, K4000, K4001, K4002, K4004, K4016, K4021, K4022, K4023, K4024, K4025, K4026, K4028, K4029, K4030, K5503
Skills	S0005, S0061, S0096, S1007, S1504, S4000, S4005, S4007, S4008, S5025

Job Role Details	
Job Role Name	Systems Security Analyst
Job Role ID	PD-P-003
Category	Protection and Defense
Specialty Area	Protection
Job Role Description	Develops, tests and maintains systems' security. Analyzes security of operations and integrated systems.
Competency Areas	Identity and Access Management (CA001), Communications Security (CA003), Cryptography (CA004), Operating Systems Security (CA005), Data Security and Administration (CA007), Vulnerability Management (CA013), Cybersecurity Testing (CA024)
Tasks	T0004, T0005, T0015, T0036, T0040, T0043, T0050, T0074, T0079, T0097, T0098, T0100, T0102, T0107, T0111, T0122, T0138, T0146, T0159, T1025, T1026, T4000, T4001, T4002, T4004, T4005, T4006, T4007, T4009, T4010, T4011, T4013, T4014, T4015, T4023, T4030, T4031, T4032, T4033
Knowledge	K0001, K0002, K0003, K0004, K0005, K0014, K0016, K0017, K0020, K0031, K0035, K0042, K0045, K0046, K0048, K0054, K0058, K0062, K0074, K0100, K0101, K0111, K0113, K0120, K0124, K0125, K0126, K0128, K0129, K0133, K0134, K0136, K0146, K0149, K0159, K0171, K0176, K0179, K0184, K0186, K0187, K0188, K0189, K0192, K0193, K0205, K0210, K1015, K4006, K4007, K4008, K4009, K4019, K5503
Skills	S0001, S0008, S0012, S0017, S0023, S0040, S0061, S0072, S0083, S0084, S0092, S1007, S1052, S4007, S4008, S5025, S5526, S5532

Job Role Details	
Job Role Name	Vulnerability Assessment Specialist
Job Role ID	PD-VA-001
Category	Protection and Defense
Specialty Area	Vulnerability Assessment
Job Role Description	Performs vulnerability assessments of systems and networks. Identifies where they deviate from acceptable configurations or applicable policies. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Competency Areas	Vulnerability Management (CA013)
Tasks	T0003, T0009, T0024, T0041, T0113, T0133, T0138, T0139, T4500, T4501, T4502, T4507
Knowledge	K0001, K0002, K0003, K0004, K0005, K0009, K0017, K0019, K0024, K0035, K0042, K0046, K0051, K0064, K0074, K0076, K0087, K0088, K0090, K0099, K0100, K0113, K0119, K0133, K0153, K0179, K0184, K0186, K0187, K0188, K0189, K0192, K0194, K0205, K0213, K0214, K4514, K5503
Skills	S0001, S0009, S0026, S0037, S0044, S0056, S0061, S0068, S0085, S0092, S0102, S1023, S1508, S1509, S2506, S2527, S2557, S4502, S4504, S4505, S4507, S5025, S5532

Job Role Details	
Job Role Name	Penetration Tester/Red Team Specialist
Job Role ID	PD-VA-002
Category	Protection and Defense
Specialty Area	Vulnerability Assessment
Job Role Description	Conducts authorized attempts to penetrate computer systems or networks and physical premises, using realistic threat techniques, to evaluate their security and detect potential vulnerabilities.
Competency Areas	Penetration Testing (CA010), Vulnerability Management (CA013)
Tasks	T4503, T4504, T4505, T4507, T4508, T4509, T4510, T4511, T4512, T4513, T4514, T4515, T4516, T4517
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0054, K0057, K0074, K0075, K0080, K0134, K0153, K0159, K0170, K0171, K0184, K0186, K0187, K0188, K0189, K0190, K0213, K0214, K1013, K4504, K4505, K4506, K4508, K4511, K4512, K4513, K4514, K5503
Skills	S0001, S0011, S0023, S0027, S0044, S0045, S0068, S0070, S0092, S0098, S0099, S2010, S4501, S4503, S4504, S4505, S4506, S4509, S4510, S4512, S5002, S5015, S5025, S5502, S5532

Job Role Details	
Job Role Name	Cybersecurity Incident Responder
Job Role ID	PD-IR-001
Category	Protection and Defense
Specialty Area	Incident Response
Job Role Description	Investigates, analyzes and responds to cybersecurity incidents.
Competency Areas	Incident Management (CA011)
Tasks	T0009, T0026, T0027, T0028, T0031, T0044, T0047, T0051, T0058, T0062, T0087, T0101, T0106, T0138, T0142, T0143, T0144, T0145, T0148, T0150, T0154, T5003, T5025, T5031, T5040, T5057, T5066
Knowledge	K0001, K0002, K0003, K0004, K0005, K0019, K0021, K0024, K0025, K0032, K0043, K0047, K0064, K0074, K0084, K0087, K0088, K0090, K0099, K0100, K0117, K0121, K0123, K0133, K0159, K0169, K0171, K0184, K0186, K0187, K0188, K0189, K0194, K0195, K0196, K0205, K3507, K4511, K4512, K4513, K4514, K5503
Skills	S0002, S0004, S0006, S0009, S0011, S0012, S0013, S0014, S0015, S0018, S0019, S0020, S0022, S0023, S0025, S0026, S0027, S0033, S0035, S0041, S0044, S0046, S0048, S0051, S0052, S0054, S0060, S0068, S0085, S0093, S0094, S0095, S0097, S0098, S0099, S0101, S0103, S0104, S1022, S1023, S1034, S1060, S2002, S2506, S2522, S2523, S2526, S2533, S2557, S3500, S3501, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5025, S5030, S5031, S5032, S5033, S5034, S5501, S5502, S5503, S5504, S5511, S5532, S5534

Job Role Details	
Job Role Name	Digital Forensics Specialist
Job Role ID	PD-IR-002
Category	Protection and Defense
Specialty Area	Incident Response
Job Role Description	Collects and analyzes digital evidence, investigates cybersecurity incidents to derive useful information to mitigate system and network vulnerabilities.
Competency Areas	Digital Forensics (CA009)
Tasks	T0010, T0030, T0032, T0033, T0049, T0149, T5000, T5002, T5004, T5006, T5007, T5010, T5013, T5014, T5015, T5016, T5017, T5019, T5020, T5022, T5023, T5024, T5025, T5026, T5027, T5028, T5029, T5031, T5036, T5037, T5038, T5039, T5040, T5041, T5045, T5057, T5062, T5063, T5064, T5065
Knowledge	K0001, K0002, K0003, K0004, K0005, K0016, K0019, K0045, K0066, K0074, K0075, K0090, K0100, K0119, K0171, K0176, K0186, K0187, K0188, K0189, K0203, K0205, K1503, K1513, K5000, K5002, K5003, K5006, K5007, K5008, K5009, K5010, K5011, K5014, K5015, K5016, K5017, K5019, K5020, K5021, K5022, K5023, K5024, K5028, K5031, K5033, K5034, K5035, K5036, K5037, K5038, K5039, K5040, K5503
Skills	S0013, S0020, S0029, S0030, S0041, S0068, S0069, S0085, S0098, S0099, S0100, S1038, S1039, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5019, S5020, S5021, S5022, S5024, S5025, S5026, S5027, S5029, S5030, S5031, S5032, S5033, S5034, S5527

Job Role Details	
Job Role Name	Cyber Crime Investigator
Job Role ID	PD-IR-003
Category	Protection and Defense
Specialty Area	Incident Response
Job Role Description	Identifies, collects, examines and preserves evidence using controlled and documented analytical and investigative techniques.
Competency Areas	Digital Forensics (CA009)
Tasks	T0018, T0021, T5001, T5005, T5008, T5009, T5010, T5012, T5018, T5023, T5034, T5035, T5040, T5042, T5043, T5046, T5047, T5049, T5057, T5061, T5067
Knowledge	K0001, K0002, K0003, K0004, K0005, K0065, K0074, K0170, K0171, K0179, K0186, K0187, K0188, K0189, K0198, K0199, K0200, K0201, K0202, K5001, K5003, K5006, K5007, K5008, K5015, K5016, K5025, K5026, K5032, K5033, K5034, K5036, K5041, K5042, K5503
Skills	S0013, S0018, S0068, S0069, S1038, S1039, S1501, S1510, S5003, S5019, S5020, S5021, S5023, S5024, S5025, S5031, S5032, S5033, S5527

Job Role Details	
Job Role Name	Malware Reverse Engineering Specialist
Job Role ID	PD-IR-004
Category	Protection and Defense
Specialty Area	Incident Response
Job Role Description	Analyzes (by disassembling and/or decompiling) malicious software, understands how it works, its impact and intent and recommends mitigation techniques and incident response actions.
Competency Areas	Digital Forensics (CA009), Incident Management (CA011), Hardware and Firmware Security (CA016)
Tasks	T0089, T5016, T5052, T5055, T5057, T5058, T5510, T5519, T5525, T5535, T5537, T5538, T5539, T5547
Knowledge	K0001, K0002, K0003, K0004, K0005, K0014, K0016, K0039, K0043, K0047, K0074, K0094, K0095, K0096, K0097, K0098, K0099, K0100, K0101, K0102, K0103, K0104, K0105, K0170, K0171, K0176, K0179, K0186, K0187, K0188, K0189, K0204, K0205, K0206, K5017, K5019, K5020, K5021, K5022, K5023, K5024, K5040
Skills	S0001, S0029, S0030, S0031, S0032, S0048, S0049, S0052, S0053, S0066, S0067, S0068, S0077, S0092, S0100, S0104, S1039, S4502, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5015, S5022, S5025, S5028, S5034, S5527, S5529, S5531

Job Role Details	
Job Role Name	Threat Intelligence Analyst
Job Role ID	PD-TM-001
Category	Protection and Defense
Specialty Area	Threat Management
Job Role Description	Collects and analyzes multi-source information about cybersecurity threats to develop deep understanding and awareness of cyber threats and actors' Tactics, Techniques and Procedures (TTPs), to derive and report indicators that help organizations detect and predict cyber incidents and protect systems and networks from cyber threats.
Competency Areas	Cyber Threat Intelligence (CA019)
Tasks	T5056, T5502, T5504, T5505, T5507, T5515, T5517, T5519, T5524, T5525, T5526, T5527, T5530, T5531, T5535, T5537, T5538, T5539, T5541, T5543, T5546, T5547, T5548, T5549, T5550
Knowledge	K0001, K0002, K0003, K0004, K0005, K0027, K0043, K0066, K0074, K0099, K0159, K0177, K0184, K0186, K0187, K0188, K0189, K0203, K5501, K5502, K5503, K5505, K5510, K5511, K5513, K5514, K5516, K5519, K5520, K5523, K5524, K5529, K5531, K5532, K5535, K5536
Skills	S0049, S0051, S0055, S0056, S0058, S0076, S0077, S0086, S0103, S0505, S1009, S1020, S1502, S1504, S2517, S2520, S2522, S2537, S2542, S2543, S2550, S2552, S2554, S3501, S4502, S5025, S5500, S5501, S5502, S5503, S5504, S5516, S5517, S5518, S5520, S5525, S5528, S5530, S5531, S5532

Job Role Details	
Job Role Name	Threat Hunter
Job Role ID	PD-TM-002
Category	Protection and Defense
Specialty Area	Threat Management
Job Role Description	Proactively searches for undetected threats in networks and systems, identifies their Indicators of Compromise (IOCs) and recommends mitigation plans
Competency Areas	Cyber Threat Intelligence (CA019)
Tasks	T0009, T0017, T0018, T0021, T0026, T0027, T0028, T0030, T0032, T0033, T0035, T0049, T0054, T0055, T0056, T0057, T0060, T0069, T0080, T0089, T0109, T0140, T0142, T0143, T0144, T0149, T0151, T0152, T0156, T0160, T0161, T0162, T0163, T0164, T1528, T5010, T5016, T5023, T5500, T5501, T5507, T5509, T5510, T5511, T5512, T5514, T5515, T5517, T5519, T5520, T5521, T5523, T5524, T5525, T5532, T5546, T5547
Knowledge	K0001, K0002, K0003, K0004, K0005, K0013, K0014, K0016, K0028, K0031, K0032, K0034, K0035, K0043, K0044, K0047, K0064, K0065, K0068, K0074, K0086, K0088, K0107, K0176, K0186, K0187, K0188, K0189, K0191, K0195, K0196, K0198, K0199, K0200, K0201, K0202, K5503, K5505, K5510, K5519, K5521, K5522, K5525, K5526, K5529, K5531, K5535, K5537
Skills	S0001, S0029, S0030, S0031, S0032, S0050, S0051, S0052, S0053, S0056, S0059, S0062, S0068, S0069, S0070, S0076, S0077, S0092, S0100, S0103, S0104, S2520, S2522, S2525, S2526, S2527, S4502, S4507, S5008, S5009, S5010, S5011, S5012, S5018, S5022, S5025, S5503, S5511, S5515, S5519, S5523, S5524, S5528, S5529, S5531, S5532, S5533, S5534

3.1.5 Category Group: Industrial Control Systems and Operational Technologies (ICS/OT)

Job Role Details	
Job Role Name	ICS/OT Cybersecurity Architect
Job Role ID	ICSOT-ICSOT-001
Category	Industrial Control Systems and Operational Technologies (ICS/OT)
Specialty Area	Industrial Control Systems and Operational Technologies (ICS/OT)
Job Role Description	Designs and oversees the development, implementation and configuration of cybersecurity systems and networks in ICS/OT environments.
Competency Areas	Cybersecurity Design and Architecture (CA017), Industrial and IoT Security (CA018)
Tasks	T0036, T0043, T0146, T0507, T0508, T0511, T0512, T0514, T0515, T0516, T0517, T0518, T0519, T0520, T0534, T0535, T0536, T0537, T0538, T0539, T1543, T2511, T4502, T6000, T6001, T6002, T6003, T6004, T6006, T6009, T6010, T6012, T6017, T6018
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0016, K0017, K0020, K0021, K0022, K0025, K0027, K0028, K0034, K0035, K0042, K0044, K0045, K0046, K0048, K0053, K0057, K0058, K0062, K0074, K0093, K0101, K0111, K0112, K0120, K0121, K0124, K0125, K0126, K0129, K0133, K0146, K0149, K0175, K0176, K0186, K0187, K0188, K0189, K0190, K0191, K0192, K0193, K0209, K0210, K1015, K1036, K1505, K4000, K4030, K5503, K6002, K6003, K6004, K6005, K6006, K6007, K6009, K6010, K6011, K6012, K6013, K6014, K6015, K6016, K6017, K6019, K6020, K6021, K6022, K6023
Skills	S0001, S0003, S0008, S0016, S0021, S0023, S0027, S0038, S0039, S0040, S0051, S0058, S0061, S0064, S0071, S0072, S0074, S0075, S0082, S0092, S0507, S0508, S0509, S1004, S1008, S1034, S1046, S1060, S1504, S1506, S2010, S2501, S6000, S6001, S6002, S6003, S6004, S6005, S6006, S6007, S6008, S6012, S6013

Job Role Details	
Job Role Name	ICS/OT Cybersecurity Infrastructure Specialist
Job Role ID	ICSOT-ICSOT-002
Category	Industrial Control Systems and Operational Technologies (ICS/OT)
Specialty Area	Industrial Control Systems and Operational Technologies (ICS/OT)
Job Role Description	Tests, implements, deploys, maintains and administers hardware and software that protect and defend systems and networks against cybersecurity threat in ICS/OT environments.
Competency Areas	Communications Security (CA003), Operating Systems Security (CA005), Hardware and Firmware Security (CA016), Industrial and IoT Security (CA018)
Tasks	T0038, T0057, T0147, T1543, T3502, T3506, T3507, T3508, T4023, T6005, T6007, T6008, T6012, T6019
Knowledge	K0001, K0002, K0003, K0004, K0005, K0017, K0019, K0024, K0035, K0043, K0046, K0063, K0064, K0074, K0084, K0100, K0119, K0147, K0186, K0187, K0188, K0189, K0192, K0194, K0205, K0206, K0212, K0519, K1052, K3502, K3509, K5012, K6012, K6014, K6015, K6016, K6017, K6019, K6020, K6022, K6023
Skills	S0001, S0005, S0008, S0009, S0014, S0016, S0021, S0022, S0035, S0038, S0040, S0061, S0065, S0068, S0069, S0071, S0082, S0085, S0092, S0096, S0106, S1007, S2507, S3500, S4006, S5526, S6004, S6005, S6007, S6008, S6009, S6011

Job Role Details	
Job Role Name	ICS/OT Cybersecurity Defense Analyst
Job Role ID	ICSOT-ICSOT-003
Category	Industrial Control Systems and Operational Technologies (ICS/OT)
Specialty Area	Industrial Control Systems and Operational Technologies (ICS/OT)
Job Role Description	Uses data collected from a variety of cybersecurity tools to analyze events that occur within ICS/OT environments to detect and mitigate cybersecurity threats.
Competency Areas	Identity and Access Management (CA001), Communications Security (CA003), Operating Systems Security (CA005), Vulnerability Management (CA013), Industrial and IoT Security (CA018), Cyber Threat Intelligence (CA019), Cybersecurity Testing (CA024)
Tasks	T0009, T0015, T0025, T0028, T0029, T0037, T0040, T0044, T0054, T0055, T0056, T0058, T0064, T0067, T0068, T0069, T0070, T0071, T0072, T0073, T0075, T0076, T0097, T0098, T0100, T0101, T0102, T0107, T0111, T0122, T0138, T0141, T0151, T0152, T0155, T0156, T0157, T0159, T1543, T3500, T3503, T3504, T6005
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0013, K0014, K0016, K0017, K0020, K0024, K0031, K0035, K0042, K0043, K0044, K0045, K0046, K0049, K0053, K0054, K0058, K0063, K0064, K0065, K0068, K0069, K0070, K0074, K0076, K0077, K0078, K0084, K0086, K0087, K0088, K0090, K0099, K0100, K0101, K0102, K0103, K0113, K0117, K0124, K0125, K0126, K0134, K0136, K0137, K0139, K0145, K0146, K0147, K0153, K0176, K0177, K0186, K0187, K0188, K0189, K0190, K0191, K0192, K0193, K0194, K0197, K0198, K0199, K0200, K0201, K0202, K0205, K0206, K0212, K0213, K0214, K3506, K3507, K5503, K6012, K6014, K6015, K6016, K6017, K6019, K6020, K6022, K6023
Skills	S0001, S0006, S0009, S0012, S0015, S0023, S0033, S0040, S0041, S0046, S0048, S0056, S0057, S0061, S0063, S0069, S0092, S0097, S0101, S0104, S2002, S2520, S2522, S2526, S3500, S3501, S3502, S4006, S5012, S5018, S5026, S5503, S5525, S6004, S6005, S6006, S6007, S6009

Job Role Details	
Job Role Name	ICS/OT Cybersecurity Risk Officer
Job Role ID	ICSOT-ICSOT-004
Category	Industrial Control Systems and Operational Technologies (ICS/OT)
Specialty Area	Industrial Control Systems and Operational Technologies (ICS/OT)
Job Role Description	Identifies, assesses and manages cybersecurity risks within ICS/OT environments. Evaluates and analyzes the effectiveness of existing cybersecurity controls and provides feedback and recommendations based on assessments.
Competency Areas	Security Risk Analysis (CA008), Industrial and IoT Security (CA018)
Tasks	T0001, T0006, T0012, T0013, T0014, T0039, T0043, T0053, T0105, T0109, T0128, T0130, T0132, T0133, T0160, T0161, T0162, T0163, T0164, T2500, T2529, T6014, T6016, T6020
Knowledge	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0029, K0037, K0073, K0074, K0080, K0081, K0083, K0092, K0107, K0160, K0166, K0167, K0186, K0187, K0188, K0189, K0190, K2511, K5503, K6003, K6005, K6012, K6014, K6015, K6016, K6017, K6019, K6020, K6022, K6023
Skills	S0012, S0040, S0044, S0056, S0057, S0062, S0075, S0077, S0079, S0080, S0081, S0082, S0089, S0091, S1007, S1504, S2553, S4507, S6006, S6007, S6009

Job Role Details	
Job Role Name	ICS/OT Cybersecurity Incident Responder
Job Role ID	ICSOT-ICSOT-005
Category	Industrial Control Systems and Operational Technologies (ICS/OT)
Specialty Area	Industrial Control Systems and Operational Technologies (ICS/OT)
Job Role Description	Investigates, analyzes and responds to cybersecurity incidents within ICS/OT environments.
Competency Areas	Incident Management (CA011), Industrial and IoT Security (CA018)
Tasks	T0009, T0026, T0027, T0028, T0031, T0044, T0047, T0051, T0058, T0062, T0087, T0101, T0106, T0138, T0142, T0143, T0144, T0145, T0148, T0150, T0154, T5025, T5031, T6014, T6015, T6020
Knowledge	K0001, K0002, K0003, K0004, K0005, K0019, K0021, K0024, K0025, K0032, K0043, K0047, K0064, K0074, K0084, K0087, K0088, K0090, K0099, K0100, K0117, K0121, K0123, K0133, K0171, K0186, K0187, K0188, K0189, K0194, K0195, K0196, K0205, K3507, K4511, K4512, K4513, K5503, K6012, K6014, K6015, K6016, K6017, K6019, K6020, K6022, K6023
Skills	S0002, S0004, S0006, S0009, S0011, S0012, S0013, S0014, S0015, S0018, S0020, S0022, S0023, S0025, S0026, S0027, S0033, S0035, S0041, S0044, S0046, S0048, S0051, S0052, S0054, S0060, S0068, S0085, S0093, S0094, S0095, S0097, S0098, S0099, S0101, S0103, S0104, S1022, S1023, S1034, S1060, S2002, S2506, S2523, S2526, S2533, S2557, S3500, S3501, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5025, S5030, S5031, S5032, S5033, S5034, S5501, S5502, S5503, S5504, S5511, S5534, S6001, S6004, S6006, S6007, S6009, S6010

3.2 Appendix B: List of Tasks, Knowledge and Skills

As stated before, SCyWF is developed using global best practices. However, the SCyWF categories, specialty areas and job roles have been tailored to address the cybersecurity workforce demand in Saudi Arabia.

Moreover, the TKSs for the job roles in the SCyWF have been developed using the long list of TKSs in global best practices with necessary changes being made to address the cybersecurity workforce demand in Saudi Arabia.

TKSs in the SCyWF are numbered as shown in Table 8. Tables 9, 10 and 11 show the descriptions of tasks, knowledge and skills, respectively.

Category	Specialty Area	Numbering Range for TKS
General Roles	General	0000-0499
Cybersecurity Architecture, Research and Development	Cybersecurity Architecture	0500-0999
	Cybersecurity Research and Development	1000-1499
Leadership and Workforce Development	Leadership	1500-1999
	Workforce Development	2000-2499
Governance, Risk, Compliance and Laws	Governance, Risk and Compliance	2500-2999
	Laws and Data Protection	3000-3499
Protection and Defense	Defense	3500-3999
	Protection	4000-4499
	Vulnerability Assessment	4500-4999
	Incident Response	5000-5499
	Threat Management	5500-5999
Industrial Control Systems and Operational Technologies (ICS/OT)	Industrial Control Systems and Operational Technologies (ICS/OT)	6000-6499

TABLE 8: SCYWF NUMBERING SCHEME OF TKSS

Task ID	Task Description
T0001	Advise senior management on cybersecurity risk levels and cybersecurity posture
T0002	Effectively communicate financial aspects of cybersecurity related activities to senior management
T0003	Evaluate organizational cybersecurity policy regulatory compliance
T0004	Implement application cybersecurity policies
T0005	Implement system cybersecurity controls
T0006	Develop cybersecurity risk profiles
T0009	Correlate incident data
T0010	Perform technical decryption of seized data
T0011	Develop cybersecurity policies and procedures
T0012	Develop risk mitigation strategies
T0013	Develop cybersecurity countermeasures for systems and applications
T0014	Document preliminary or residual security risks for system operation
T0015	Use cybersecurity products and security control technologies to reduce identified risk to an acceptable level
T0016	Determine if protection and detection capabilities are consistent with organization-level cybersecurity architecture
T0017	Establish stakeholder communication channels
T0018	Establish internal and external cross-team relationships
T0019	Ensure that contracts adhere to legal and organizational cybersecurity and data protection requirements
T0021	Identify data or intelligence of evidentiary value

Task ID	Task Description
T0022	Evaluate fulfillment of cybersecurity requirements in implemented products
T0023	Improve cybersecurity documentation to satisfy compliance requirements
T0024	Maintain deployable cyber defense audit toolkits
T0025	Escalate incidents that may cause ongoing and immediate impact to the environment
T0026	Identify potential threats to network resources
T0027	Perform cybersecurity incident triage
T0028	Perform cyber defense trend analysis and reporting
T0029	Determine the effectiveness of an observed attack
T0030	Perform file signature analysis
T0031	Recommend mitigation and remediation strategies for enterprise systems
T0032	Perform real-time forensic analysis
T0033	Perform timeline analysis
T0035	Mitigate programming vulnerabilities
T0036	Identify gaps in security architecture
T0037	Perform cybersecurity reviews of security architecture to inform risk mitigation strategies
T0038	Perform system administration on specialized cyber defense applications and systems
T0039	Conduct risk analysis of applications and systems undergoing major changes
T0040	Recommend system modifications to close identified vulnerabilities

Task ID	Task Description
T0041	Prepare audit reports
T0042	Inform the business about business continuity management (BCM) and data protection plans
T0043	Advise on risk management framework process activities and related documentation
T0044	Determine causes of network alerts
T0046	Provide cybersecurity expertise on organizational and sectoral policy boards
T0047	Track cyber defense incidents from initial detection through final resolution
T0048	Determine if appropriate threat mitigation actions have been taken
T0049	Capture network traffic associated with malicious activities
T0050	Update security documentation to reflect current application and system security design features
T0051	Produce incident findings reports
T0052	Research current technology to understand cyber defense capability required by systems or networks
T0053	Provide cybersecurity guidance to organizational risk governance processes
T0054	Detect cybersecurity attacks and intrusions
T0055	Perform continuous monitoring of system activity
T0056	Determine impact of malicious activity on systems and information
T0057	Identify, prioritize and coordinate the protection of critical cyber defense infrastructure and resources
T0058	Employ defense-in-depth principles and practices in line with organizational policies
T0059	Effectively manage vulnerability remediation

Task ID	Task Description
T0060	Create auditable evidence of security measures
T0061	Determine if acquisitions, procurement, and outsourcing efforts address cybersecurity requirements
T0062	Mitigate potential cyber defense incidents
T0063	Determine organizational compliance
T0064	Establish intrusion set procedures
T0067	Identify network traffic anomalies
T0068	Identify indications and warnings through research, analysis and correlation across multiple data sets
T0069	Validate intrusion detection system alerts
T0070	Remove malware
T0071	Analyze network traffic to identify a device's environment components
T0072	Use network traffic to reconstruct malicious activity
T0073	Identify network mapping and operating system (OS) fingerprinting activities
T0074	Assess the effectiveness of cybersecurity controls
T0075	Construct cyber defense network tool signatures
T0076	Report suspected cyber incidents in line with the organization's cyber incident response plan
T0078	Acquire adequate funding for cybersecurity training
T0079	Determine effectiveness of configuration management processes
T0080	Collect metrics and trending data

Task ID	Task Description
T0082	Determine if cybersecurity workforce management policies and procedures comply with legal and organizational requirements
T0083	Present technical information to technical and non-technical audiences
T0084	Present data in creative formats
T0085	Promote awareness of cybersecurity policy among management
T0086	Identify training requirements
T0087	Prepare after action reviews (AARs)
T0088	Integrate laws and regulations into policy
T0089	Use reverse engineering tools
T0090	Design data management systems
T0091	Integrate encryption best practice into applications
T0095	Align the organization's cybersecurity strategy with its business strategy
T0096	Design system security measures
T0097	Analyze organizational cybersecurity posture trends
T0098	Develop system security posture trend reports
T0100	Determine adequacy of access controls
T0101	Maintain currency of cyber defense threat conditions
T0102	Determine effectiveness of system implementation and testing processes
T0103	Determine the effectiveness of organizational cybersecurity policies and procedures

Task ID	Task Description
T0105	Conduct cybersecurity risk assessments
T0106	Coordinate incident response functions
T0107	Recommend threat and vulnerability risk mitigation strategies
T0108	Advise management, staff, and users on cybersecurity policy
T0109	Conduct technology program and project audits
T0111	Work with stakeholders to resolve cybersecurity incidents and vulnerability compliance issues
T0112	Provide cybersecurity advice and input for disaster recovery, contingency, and continuity of operations plans
T0113	Perform technical and nontechnical risk and vulnerability assessments of organizational technology environments
T0122	Notify appropriate personnel of imminent hostile intentions or activities
T0127	Ensure that appropriate controls are in place to effectively mitigate risk and address data protection concerns during a risk assessment process
T0128	Establish a cybersecurity risk management program
T0130	Establish organizational risk management strategies
T0132	Facilitate stakeholders situational awareness of risk levels through regular risk monitoring
T0133	Perform continuous monitoring
T0134	Develop security architecture elements to mitigate threats as they emerge
T0136	Develop vulnerability remediation plans
T0137	Verify the inclusion of sound cybersecurity principles in the organization's vision and goals
T0138	Determine the operational impacts of cybersecurity breaches

Task ID	Task Description
T0139	Evaluate organizational cybersecurity policy alignment with organizational directives
T0140	Maintain stakeholder communication channels
T0141	Document cybersecurity incidents
T0142	Identify anomalous network activity
T0143	Recommend incident remediation strategies
T0144	Determine the scope, urgency, and impact of cybersecurity incidents
T0145	Perform forensically sound image collection
T0146	Develop a cybersecurity risk management plan
T0147	Administer Virtual Private Network (VPN) devices
T0148	Document cyber defense incidents from initial detection through final resolution
T0149	Analyze network traffic associated with malicious activities
T0150	Communicate incident findings to appropriate constituencies
T0151	Communicate cybersecurity attacks and intrusions alerts
T0152	Distinguish between benign and potentially malicious cybersecurity attacks and intrusions
T0153	Determine if vulnerability remediation plans are in place
T0154	Collect intrusion artifacts
T0155	Analyze network traffic anomalies
T0156	Perform network packet analysis

Task ID	Task Description
T0157	Isolate malware
T0158	Update system security measures
T0159	Develop organizational cybersecurity posture trend reports
T0160	Oversee independent cybersecurity audits
T0161	Implement independent cybersecurity audit processes for application software, networks, and systems
T0162	Develop independent cybersecurity audit processes for application software, networks, and systems
T0163	Determine if research and design processes and procedures are in compliance with cybersecurity requirements
T0164	Determine if research and design processes and procedures are accurately followed by cybersecurity staff when performing their day-to-day activities
T0165	Promote awareness of cybersecurity strategy among management
T0500	Deliver secure cloud solutions to development teams
T0502	Determine cybersecurity design and architecture effectiveness
T0503	Develop a secure cloud strategy
T0504	Develop secure designs for cloud services
T0505	Build solutions to identify existing organizational data within cloud environments
T0507	Employ secure configuration management processes
T0508	Prioritize essential system capabilities and business functions
T0511	Analyze candidate architectures, allocate security services and select security mechanisms
T0512	Define system security contexts

Task ID	Task Description
T0514	Create cybersecurity architecture functional specifications
T0515	Develop a secure architectural plan that addresses business needs
T0516	Develop a secure enterprise architecture that addresses business needs
T0517	Document and update as necessary all definition and architecture activities
T0518	Identify the adequate cybersecurity controls for cyber-related assets
T0519	Design cybersecurity management functions
T0520	Determine disaster recovery and continuity of operations system requirements
T0523	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event
T0524	Develop and integrate cybersecurity designs for cyber-related assets with multilevel security requirements
T0525	Define acquisition life cycle cybersecurity architecture requirements
T0526	Determine if systems and architecture are consistent with cybersecurity architecture guidelines
T0527	Translate cybersecurity capabilities into technical requirements
T0529	Design proof-of-concept (POC) and pilots in emerging technology areas
T0530	Read and interpret technical diagrams, specifications, drawings, blueprints and schematics relating to systems and networks
T0532	Implement a secure cloud strategy
T0533	Enforce secure designs for cloud services
T0534	Determine essential system capabilities and business functions
T0535	Develop the concept of operations (conOps) documents for system security

Task ID	Task Description
T0536	Define baseline system security requirements
T0537	Determine business requirements for developing an effective and secure architecture
T0538	Conduct cybersecurity management assessments
T0539	Define system availability levels
T0540	Define acquisition life cycle systems security engineering requirements
T0541	Assess the alignment of the Concept of Operations (ConOps) documentation with best practices
T0542	Implement secure Infrastructure as Code (IaC) processes for provisioning and managing multi-cloud resources
T0543	Manage container orchestration platforms to maintain a secure, scalable foundation for cloud-based applications
T1000	Determine data specifications
T1001	Plan for anticipated changes in data capacity requirements
T1002	Recommend development of new applications or modification of existing applications
T1003	Analyze feasibility of software design within time and cost constraints
T1004	Determine life cycle support requirements
T1005	Perform code reviews
T1006	Apply secure code documentation
T1007	Determine effectiveness of system cybersecurity measures
T1008	Build, test and modify product prototypes to demonstrate compliance with cybersecurity requirements using working or theoretical models
T1009	Integrate organizational goals and objectives into security architecture

Task ID	Task Description
T1010	Create program documentation during initial development and subsequent revision phases
T1011	Determine system performance requirements
T1012	Develop threat models
T1013	Evaluate interfaces between hardware and software
T1014	Determine if desired program results are produced
T1015	Develop cybersecurity or cybersecurity-enabled products
T1016	Determine if hardware, operating systems, and software applications adequately address cybersecurity requirements
T1017	Develop technical and procedural processes for secure system backups
T1018	Create system testing and validation procedures and documentation
T1019	Validate data mining and data warehousing programs, processes, and requirements
T1020	Develop data standards, policies and procedures
T1021	Develop systems security design documentation
T1022	Develop disaster recovery and continuity of operations plans for systems under development
T1023	Develop secure code and error handling
T1024	Determine hardware configuration
T1025	Determine relevance of recovered data
T1026	Allocate security functions to system components and elements
T1027	Remediate technical problems encountered during system testing and implementation

Task ID	Task Description
T1029	Identify programming code flaws
T1031	Develop cybersecurity requirements for the software development lifecycle
T1033	Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts)
T1034	Manage the compilation, cataloging, caching, distribution and retrieval of data
T1035	Perform integrated quality assurance testing
T1036	Develop workflow charts and diagrams
T1038	Develop guidelines for implementing developed systems for customers and installation teams
T1039	Recommend new database technologies and architectures
T1040	Address security implications in the software acceptance phase
T1041	Analyze system capabilities and requirements
T1042	Conduct test and evaluation activities
T1043	Integrate security requirements into application design elements
T1044	Utilize models and simulations to analyze or predict system performance under different operating conditions
T1045	Develop cybersecurity capability strategies for custom hardware and software development
T1046	Perform penetration testing
T1048	Plan system security development
T1049	Develop cybersecurity designs to meet specific operational needs and environmental factors
T1050	Identify cybersecurity solutions tools and technologies

Task ID	Task Description
T1051	Develop cybersecurity tools and technologies
T1052	Identify and leverage the enterprise-wide version control system when designing and developing secure applications
T1053	Implement and integrate system development life cycle methodologies into cybersecurity systems development environment
T1054	Consult with customers about software system design and maintenance
T1055	Develop software documentation
T1057	Recommend network infrastructure enhancements
T1058	Follow software and systems engineering life cycle standards and processes when developing cybersecurity systems and solutions
T1059	Analyze data sources to provide actionable recommendations
T1060	Determine the validity of findings
T1061	Conduct hypothesis testing
T1062	Confer with systems analysts, engineers, programmers and others to design cybersecurity applications
T1063	Implement secure interfaces between information systems, physical systems, and embedded technologies
T1064	Develop data gathering processes
T1066	Program custom algorithms
T1069	Effectively allocate storage capacity in the design of data management systems
T1070	Read, interpret, write, modify and execute simple scripts to perform tasks
T1071	Utilize different programming languages to write code, open files, read files and write output to different files
T1072	Utilize open source languages

Task ID	Task Description
T1073	Troubleshoot prototype design and process issues
T1074	Recommend vulnerability mitigation functional, and security-related features
T1075	Design and develop secure applications
T1076	Analyze and provide information to stakeholders to support the development or modification of security applications
T1078	Conduct trial runs of programs and software applications
T1079	Determine if systems meet minimum security requirements
T1081	Develop software system testing and validation procedures
T1083	Develop and implement data mining and data warehousing programs
T1085	Upgrade software interfaces
T1087	Identify cybersecurity gaps in enterprise architecture
T1088	Provide cybersecurity advice on implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials
T1089	Determine if design components meet system requirements
T1090	Determine scalability of system architecture
T1091	Determine if hardware and software comply with defined specifications and requirements
T1092	Prepare vulnerability analysis reports
T1093	Submit operational requirements for research, development, and acquisition of cyber capabilities
T1094	Develop world class automated processes and artificial intelligence solutions
T1096	Conduct predictive analytics

Task ID	Task Description
T1098	conduct quantitative data analysis using a variety of datasets
T1099	Keep current with computer vision and machine learning research to replicate and baseline new techniques
T1100	Create data visualizations and dashboards to communicate results
T1101	Perform data profiling
T1102	Convert workflow charts and diagrams into coded computer language instructions
T1104	Incorporate product end-of-life cybersecurity measures
T1105	Integrate security testing tools into quality assurance processes
T1106	Determine data requirements
T1108	Create development plans of new applications or modification of existing applications
T1109	Design application interfaces
T1110	Correct program errors
T1111	Design cybersecurity or cybersecurity-enabled products
T1112	Develop technical and procedural processes for backup data storage
T1113	Determine effectiveness of disaster recovery and continuity of operations plans for systems under development during testing phase
T1114	Direct the remediation of technical problems encountered during system testing and implementation
T1115	Document software attack surface elements
T1116	Conduct threat modeling
T1117	Conduct system security development

Task ID	Task Description
T1118	Design cybersecurity tools and technologies
T1119	Evaluate network infrastructure vulnerabilities
T1120	Design secure interfaces between information systems, physical systems, and embedded technologies
T1121	Recommend vulnerability exploitation functional and security-related features
T1122	Determine if applications meet minimum security requirements
T1123	Create software system documentation
T1124	Improve software performance
T1125	Adapt software to new hardware
T1126	Conduct cybersecurity reviews for enterprise architecture
T1127	Conduct vulnerability analysis of software patches and updates
T1128	Prioritize operational requirements for research, development, and acquisition of cyber capabilities
T1129	Approve operational requirements for research, development, and acquisition of cyber capabilities
T1130	Perform statistical and machine learning analysis
T1131	Determine cybersecurity measures for steady state operation and management of software
T1132	Ensure secure integration of application databases
T1133	Record test data
T1134	Manage test data
T1135	Determine special needs of cyber-physical systems

Task ID	Task Description
T1501	Provide inspectors general, and oversight and compliance with legal analysis and decisions
T1502	Ensure appropriate data is collected and maintained to meet defined cybersecurity reporting requirements
T1503	Communicate the value of cybersecurity to organizational stakeholders
T1504	Determine if security improvement actions are evaluated, validated, and implemented as required
T1505	Determine if cybersecurity inspections, tests, and reviews are coordinated for the network environment
T1506	Determine if cybersecurity requirements are included in business continuity and disaster recovery planning operations
T1507	Determine if cybersecurity architecture design is aligned with the organization's cybersecurity strategy
T1510	Determine implications of new and upgraded technologies to the cybersecurity program
T1511	Communicate effectively with third parties in the event of a cybersecurity incident
T1513	Maintain situational awareness of cyber-related intelligence requirements and associated tasking
T1516	Oversee the cybersecurity training and awareness program
T1518	Participate in the development or modification of cybersecurity program plans and requirements
T1520	Ensure that cybersecurity awareness training is provided to all members of staff
T1521	Ensure that cybersecurity requirements are included as appropriate in any procurement action
T1522	Ensure that appropriate reporting is provided to senior management as necessary
T1523	Identify potential security incidents and report as necessary
T1524	Ensure that appropriate resources are allocated to meet the organization's cybersecurity requirements
T1525	Maintain and regularly review the organization's cybersecurity policy and associated documentation

Task ID	Task Description
T1526	Take appropriate actions to mitigate the risk in the event of a cybersecurity incident
T1527	Inform and enhance organizational documentation leveraging international best practice documentation
T1528	Promote cybersecurity awareness to management
T1529	Ensure that organizational cybersecurity strategy is effectively addressed by cybersecurity policies and related documents
T1530	Recommend improvements to procurement activities to address cybersecurity requirements
T1531	Ensure cybersecurity requirements of all information technology systems are determined
T1532	Participate in the acquisition process as necessary and ensure that appropriate supply chain risk management practices are adopted
T1534	Implement critical infrastructure protection policies and procedures
T1535	Identify future cybersecurity strategy requirements
T1537	Brief senior management on developments and trends in cybersecurity
T1538	Brief senior management on cybersecurity controls required to protect the organization
T1539	Evaluate cybersecurity aspects of supplier selection and proposition
T1540	Report findings from international cybersecurity events to senior management
T1541	Attend international cybersecurity events
T1542	Conduct periodic reviews of security assumptions
T1543	Identify critical technology procurement requirements
T1544	Provide outside and honest viewpoint to senior management
T1545	Determine if procurement activities sufficiently address supply chain risks

Task ID	Task Description
T1546	Develop critical infrastructure protection policies and procedures
T1547	Present at international cybersecurity events
T1548	Acquire resources to support cybersecurity program goals and objectives
T1549	Coordinate strategic planning initiatives with both internal and external stakeholders
T1550	Maintain a RACI matrix for cybersecurity tasks
T1551	Compile periodic cybersecurity performance and incidents report
T1552	Perform cost/benefit analyses of cybersecurity programs, policies, processes, systems, and elements
T1553	Evaluate cost/benefit, economic, and risk analysis in decision-making process
T1554	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements
T1555	Convert strategic requirements into functional specifications
T1556	Evaluate cybersecurity business cases
T1557	Provide support for decision makers in business cases related to cybersecurity
T2000	Obtain relevant resources needed for developing an effective business continuity management (BCM) plan
T2002	Conduct interactive training exercises
T2003	Develop organizational cybersecurity strategy
T2004	Develop awareness training materials that are appropriate for intended audiences
T2005	Evaluate the effectiveness and comprehensiveness of training programs
T2006	Identify organizational policy stakeholders

Task ID	Task Description
T2007	Determine if cybersecurity requirements for IT are aligned with the organization's cybersecurity strategy
T2008	Manage financial aspects of cybersecurity, including budgeting and resourcing
T2009	Ensure the effective communication of cybersecurity threats and mitigations to interested third parties
T2010	Review cybersecurity training documentation
T2011	Design and execute exercise scenarios
T2012	Produce cybersecurity instructional materials
T2013	Develop training modules and classes
T2014	Develop training assignments
T2015	Develop training evaluations
T2016	Develop grading and proficiency standards
T2017	Create learner development, training, and remediation plans
T2018	Develop learning objectives and goals
T2019	Develop organizational training materials
T2020	Develop proficiency assessments
T2021	Assess the effectiveness and efficiency of instruction against different performance indicators
T2022	Conduct learning needs assessments
T2023	Determine if qualification standards meet organizational functional requirements and comply with industry standards
T2024	Create interactive learning exercises

Task ID	Task Description
T2025	Develop standardized cybersecurity position descriptions in alignment with SCyWF job roles
T2026	Develop recruiting, hiring, and retention processes for cybersecurity roles
T2027	Develop or implement cybersecurity career classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers
T2028	Develop cybersecurity training policies and procedures
T2029	Develop cybersecurity curriculum goals and objectives
T2031	Establish cybersecurity workforce readiness metrics
T2032	Determine cybersecurity career field qualification requirements
T2033	Establish organizational cybersecurity career pathways
T2034	Develop cybersecurity workforce reporting requirements
T2035	Establish cybersecurity workforce management programs
T2036	Develop instructional strategies
T2038	Determine organizational policies related to or influencing the cyber workforce
T2039	Integrate cybersecurity workforce personnel into information systems life cycle development processes
T2040	Correlate training and learning to business or mission requirements
T2042	Deliver training courses
T2044	Develop technical training curriculum and resources
T2046	Determine if cybersecurity training, education, and awareness meet established goals
T2047	Identify cyber workforce planning and management issues

Task ID	Task Description
T2048	Plan classroom learning sessions
T2049	Plan delivery of non-classroom learning
T2050	Perform periodic reviews of learning materials and courses for accuracy and currency
T2051	Recommend revisions to learning materials and curriculum
T2053	Review and approve training supplier selection and management policies
T2054	Create data protection and legal training materials
T2055	Implement organizational training and education policies and procedures
T2056	Design assessments and activities to measure learner performance and effectiveness of the curriculum
T2057	Establish clear and measurable learning objectives
T2058	Partnering with subject matter experts to create, review, and update content
T2059	Periodically review cybersecurity roles and responsibilities within the organization
T2060	Implement and maintain an effective business continuity management (BCM) plan
T2061	Develop organizational training programs
T2062	Conduct cybersecurity workforce assessments
T2063	Assess cybersecurity workforce management programs
T2064	Deliver training to trainees
T2065	Address cyber workforce planning and management issues
T2066	Coordinate training and education

Task ID	Task Description
T2067	Deliver data protection awareness trainings
T2068	Integrate leadership priorities
T2069	Establish waiver processes for cybersecurity career field entry and training qualification requirements
T2070	Run phishing simulation campaigns to assess user awareness and response
T2071	Design phishing simulation campaigns to assess user awareness and response
T2072	Evaluate the impact and effectiveness of cybersecurity awareness initiatives
T2073	Coordinate periodic cybersecurity awareness activities and campaigns
T2074	Develop scenario-based awareness materials simulating real-world social engineering attacks
T2075	Implement feedback mechanisms to improve awareness program quality
T2076	Deliver short cybersecurity awareness briefings tied to organizational events (e.g., phishing incidents, software rollouts)
T2077	Design gamified awareness activities or competitions (e.g., cybersecurity quizzes, challenges, leaderboards)
T2500	Develop risk, compliance, and assurance monitoring strategies
T2501	Document security, resilience, and dependability requirements
T2503	Manage agreed accreditation packages
T2504	Determine if systems comply with security, resilience, and dependability requirements
T2505	Plan security authorization reviews for system and network installations
T2506	Prepare technical evaluations of software applications, systems, and networks
T2507	Determine if authorization and assurance documents identify an acceptable level of risk for software applications, systems, and networks

Task ID	Task Description
T2508	Carry out an audit of application software/network/system security against documented cybersecurity policies and provide recommendations for remediation where gaps appear
T2509	Develop cybersecurity compliance processes for external services
T2510	Regularly review and ensure that cybersecurity policies and related documentation are aligned with the organization's stated business objectives and strategy
T2511	Determine and document the impact of new system and interface implementations on organization's cybersecurity posture
T2512	Document cybersecurity design and development activities
T2513	Identify supply chain risks for critical system elements
T2514	Support cybersecurity compliance activities
T2515	Determine if the cybersecurity audits test all relevant aspects of the organization's infrastructure and policy compliance
T2516	Ensure that software application, network, or system configurations comply with the organization's cybersecurity policies
T2519	Cooperate with relevant regulatory agencies and other legal entities in any compliance reviews or investigations
T2521	Scope analysis reports to various audiences that accounts for data sharing classification restrictions
T2522	Ensure proper reporting of incidents to regulatory bodies as required
T2523	Establish monitoring systems to detect and report non-compliance
T2524	Monitor changes in laws and regulations to keep compliance programs up-to-date
T2525	Perform internal audits to ensure compliance with cybersecurity requirements
T2526	Support the business in managing their cyber risk
T2527	Work with third-party auditors to manage external audits and certifications
T2528	Periodically review cybersecurity risk management plans and procedures

Task ID	Task Description
T2529	Develop risk, compliance, and assurance measurement strategies
T2530	Develop risk, compliance, and assurance specifications
T2531	Approve agreed accreditation packages
T2532	Develop security assurance cases for system and network installations
T2533	Conduct security authorization reviews for system and network installations
T2534	Document software application, system, and network security postures, capabilities, and vulnerabilities
T2535	Develop cybersecurity audit processes for external services
T2536	Document supply chain risks for critical system elements
T2537	Promote risk-based behavior and decision
T2538	Establish appropriate controls and compensatory controls that strengthen the existing cybersecurity policies
T2539	Determine impact of noncompliance on organizational risk levels
T2540	Determine impact of noncompliance on effectiveness of the enterprise's cybersecurity program
T2541	Determine if new and existing services comply with cybersecurity and data protection obligations
T2542	Identify organizational cybersecurity compliance gaps
T2543	Correct organizational cybersecurity compliance gaps
T2544	Provide cybersecurity legal advice for business partner contracts
T3001	Interpret and apply laws, regulations, policies, standards, or procedures as necessary
T3002	Resolve conflicts in laws, regulations, policies, standards, or procedures

Task ID	Task Description
T3004	Identify alleged violations of law, regulations, policy, or guidance
T3005	Develop cybersecurity implementation policies and guidelines
T3007	Evaluate the impact of legal, regulatory, policy, standard, or procedural changes
T3008	Provide cybersecurity related guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients
T3010	Prepare legal documents
T3013	Build relationships with regulators and government departments responsible for data security issues
T3014	Register databases with data protection authorities
T3019	Serve as information protection liaison to technology system users
T3023	Manage organizational participation in public data protection and cybersecurity initiatives
T3025	Prepare data protection program status reports
T3026	Develop organizational data protection program
T3029	Develop sanctions for failure to comply with data protection policies
T3030	Resolve allegations of noncompliance with data protection policies
T3031	Develop a risk management and compliance framework for data protection
T3033	Establish complaint processes related to data protection incidents and violations
T3036	Maintain the organizational data protection program
T3037	Develop organizational data protection policies and procedures
T3038	Monitor advancements in data protection technologies and controls

Task ID	Task Description
T3039	Monitor systems development and operations to ensure compliance with cybersecurity and data protection policies
T3041	Align cybersecurity and data protection practices in system information security plans
T3042	Develop vendor review procedures
T3049	Develop information sharing strategic plans
T3050	Implement and maintain organizational data protection policies and procedures
T3051	Manage data breaches
T3052	Maintain awareness of applicable data protection laws, regulations and standards
T3056	Administer action on organizational cybersecurity complaints
T3057	Develop vendor auditing procedures
T3500	Deploy cyber defense tools
T3502	Administer rule and signature updates for specialized cyber defense applications
T3503	Validate network alerts
T3504	Communicate daily network event and activity reports
T3506	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure
T3507	Evaluate platforms managed by service providers
T3508	Manage network access control lists on specialized cyber defense systems
T3511	Document functional descriptions of system security control implementations
T4000	Apply service-oriented security architecture principles to meet the organization's confidentiality, integrity and availability requirements

Task ID	Task Description
T4001	Determine if systems security operations and maintenance activities are properly documented and updated
T4002	Apply security patches to commercial products
T4004	Integrate automated capabilities for updating or patching system software
T4005	Perform cybersecurity testing of developed applications and systems
T4006	Document systems security activities
T4007	Provide cybersecurity guidance to leadership
T4008	Detect concealed data
T4009	Develop procedures for system operations transfer to alternate sites
T4010	Execute disaster recovery and continuity of operations processes
T4011	Implement security measures for systems and system components
T4013	Ensure the integration and implementation of cross-domain solutions in a secure environment
T4014	Make recommendations to management to make mitigation and correction measures or accept risks when security deficiencies are identified during testing
T4015	Define minimum security requirements for applications
T4016	Design and deploy identity access management solutions
T4017	Develop the identity access management strategy
T4018	Determine if identity access management implementations follow organization's standards and policies
T4019	Identify and address gaps in the identity access management implementation
T4021	Design and develop cryptographic algorithms

Task ID	Task Description
T4022	Analyze cryptographic algorithms to find weaknesses and break ciphers
T4023	Develop processes and procedures for manual updating and patching of system software
T4024	Develop group policies
T4025	Administer system and network user accounts
T4026	Develop system administration and management functionality for privileged access users
T4027	Establish systems and equipment access protocols
T4028	Establish access control processes for continuous monitoring tools and technologies
T4029	Implement access control processes for continuous monitoring tools and technologies
T4030	Determine if the application of security patches for commercial products meets timeline requirements
T4031	Test failover for system operations transfer to alternative sites
T4032	Resolve vulnerabilities in systems and system components
T4033	Mitigate risks in systems and system components
T4034	Implement cryptographic algorithms
T4035	Develop access control lists
T4036	Design system administration and management functionality for privileged access users
T4500	Perform authorized penetration testing on enterprise network assets
T4501	Conduct required reviews, including reviews of defensive measures, according to the organization's policies
T4502	Recommend cost-effective security controls

Task ID	Task Description
T4503	Perform network topography and usage analysis
T4504	Mimic malicious social engineering techniques used by attackers
T4505	Identify methods that attackers could use to exploit system and network vulnerabilities
T4507	Carry out vulnerability scanning on system
T4508	Report penetration testing and vulnerability assessment findings including risk level, proposed mitigation and details necessary to reproduce the test results
T4509	Discuss security findings with management, leadership and IT teams
T4510	Design and develop penetration testing team processes
T4511	Conduct network remote testing
T4512	Plan and create penetration methods, scripts and tests
T4513	Design simulated attacks to reflect impact in the organization's business and its users
T4514	Present test findings, risks and conclusions to technical and non-technical audiences
T4515	Determine the business impact of identified vulnerabilities
T4516	Conduct physical security assessments of servers, systems and network devices
T4517	Test for vulnerabilities in web applications, client applications and standard applications
T5000	Determine best methods for identifying the perpetrator(s) of a network intrusion
T5001	Conduct victim and witness interviews
T5002	Identify intrusions
T5003	Resolve cyber defense incidents

Task ID	Task Description
T5004	Create forensically sound duplicates of evidence
T5005	Investigate suspicious activity and alleged digital crimes
T5006	Create technical summary of findings reports
T5007	Ensure that chain of custody is followed for all acquired digital media in accordance with national law or organizational policies as applicable
T5008	Conduct analysis of computer network attacks
T5009	Determine if security incidents are indicative of a violation of law that requires specific legal action
T5010	Identify digital evidence for analysis
T5012	Collect documentary or physical evidence of cyber intrusion incidents, investigations, and operations
T5013	Perform dynamic analysis on drives
T5014	Perform hash comparison against databases required by organizational policies
T5015	Perform static media analysis
T5016	Perform tier 1, 2 and 3 malware analysis
T5017	Prepare digital media for imaging
T5018	Process crime scenes
T5019	Process digital evidence
T5020	Recognize and report forensic artifacts in line with reporting policies
T5022	Extract data from devices
T5023	Recover information from forensic data sources

Task ID	Task Description
T5024	Conduct binary analysis
T5025	Work as a technical expert in support of law enforcement, explaining incident details and forensic analysis as required
T5026	Scan digital media for viruses
T5027	Perform forensic analysis of file systems
T5028	Perform static analysis to mount an "image" of a drive; with or without the original
T5029	Perform static malware analysis
T5031	Correlate threat assessment data
T5034	Determine the impact of threats on cybersecurity
T5035	Advise trial counsel as technical expert
T5036	Process forensic images
T5037	Perform Windows registry analysis
T5038	Perform file and registry monitoring on running systems
T5039	Enter digital media information into tracking databases
T5040	Report cyber incidents to inform cyber defense
T5041	Prepare cyber defense toolkits
T5042	Analyze material from cybersecurity incidents for evidence of hostile foreign actor or criminal activity
T5043	Preserve digital evidence
T5045	Conduct log file analysis

Task ID	Task Description
T5046	Identify responsible parties for intrusions and other crimes
T5047	Document original condition of digital evidence
T5049	Prepare investigative reports
T5052	Review gathered information for validity and relevance to the investigation in line with organizational policies
T5055	Sanitize reports to protect proprietary, commercial, personal or otherwise sensitive or confidential data or methods
T5056	Track status of information requests
T5057	Document lessons learned during events and exercises
T5058	Identify potential malicious activity from memory dumps, logs and packet captures
T5060	Assess the exploitability of the targets using custom exploits, solutions and techniques
T5061	Interview cybercrime suspects
T5062	Identify intrusion via dynamic analysis
T5063	Set up a forensic workstation
T5064	Document what is known about intrusions
T5065	Analyze intrusions
T5066	Coordinate technical support to enterprise-wide cybersecurity defense technicians
T5067	Recommend potential courses of action
T5500	Recommend new or revised security, resilience, and dependability measures
T5501	Analyze the results of various systems testing to identify cost-effective improvements that can reduce identified risks

Task ID	Task Description
T5502	Answer requests for information in line with the organization's policies
T5504	Enhance incident response plans based on Knowledge about threat actors and activities
T5505	Coordinate, validate and manage the organization's cyber threat intelligence sources and feeds
T5507	Prepare and deliver briefs on specific threats to the organization
T5509	Conduct network scouting
T5510	Conduct nodal analysis
T5511	Detect exploits against targeted networks and hosts
T5512	Determine what technologies are used by a given target
T5514	Collect and analyze threat actors data
T5515	Evaluate threat decision-making processes
T5517	Identify organization's principal cyber threats
T5519	Identify cyber threat tactics and methodologies
T5520	Identify vulnerabilities
T5521	Identify the threat actor's structure and components
T5523	Develop courses of action based on threat factors
T5524	Monitor changes to designated cyber operations warning problem sets
T5525	Monitor threat activities
T5526	Monitor open source websites for hostile content directed towards organizational or partner interests

Task ID	Task Description
T5527	Monitor and report threat actor activities
T5530	Provide intelligence analysis and support
T5531	Prepare network intrusion reports
T5532	Perform real-time cyber defense incident handling
T5535	Maintain a common intelligence picture
T5537	Develop priority information requirements
T5538	Generate requests for cybersecurity information
T5539	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products
T5541	Recommend adjustments to intelligence collection strategies
T5543	Determine effectiveness of intelligence collection operations
T5546	Prepare change reports for designated cyber operations warning problem sets
T5547	Prepare threat activity reports
T5548	Manage collection requirements
T5549	Assess effectiveness of intelligence reporting
T5550	Assess effectiveness of intelligence production
T6000	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event in ICS/OT environments
T6001	Develop cybersecurity designs to meet specific operational needs and environmental factors in ICS/OT environments
T6002	Define acquisition life cycle for cybersecurity architecture requirements in ICS/OT environments

Task ID	Task Description
T6003	Determine if systems and architecture are consistent with cybersecurity architecture guidelines in ICS/OT environments
T6004	Translate proposed capabilities into technical requirements in ICS/OT environments
T6005	Conduct analysis of physical and logical digital technologies in ICS/OT environments to identify potential avenues of access
T6006	Research emerging communications technology trends to inform organizational design and security policies in ICS/OT environments
T6007	Identify required system security controls in ICS/OT environments
T6008	Implement system security controls in ICS/OT environments
T6009	Determine implications of new and upgraded technologies to the cybersecurity program in ICS/OT environments
T6010	Design systems and solutions to support successful proofs-of-concept and pilot projects in emerging technology areas in ICS/OT environments
T6012	Troubleshoot industrial automation and communication systems and servers
T6014	Resolve ICS/OT cyber defense incidents
T6015	Perform real-time cyber defense incident handling in ICS/OT environments
T6016	Conduct risk analysis of ICS/OT environments
T6017	Integrate organizational goals and objectives into security architecture in ICS/OT environments
T6018	Define acquisition life cycle for systems security engineering requirements in ICS/OT environments.
T6019	Document planned system security control implementations in ICS/OT environments
T6020	Coordinate technical support to ICS/OT cybersecurity defense technicians

TABLE 9: TASKS DESCRIPTIONS

ID	Description
K0001	Knowledge of network components and operations
K0002	Knowledge of risk assessment principles and practices
K0003	Knowledge of cybersecurity laws and regulations
K0004	Knowledge of cybersecurity principles and practices
K0005	Knowledge of cybersecurity threats
K0007	Knowledge of authentication and authorization tools and techniques
K0008	Knowledge of the organization's business model and practices to derive appropriate cybersecurity strategies
K0009	Knowledge of common application vulnerabilities
K0010	Knowledge of network infrastructure principles and practices
K0011	Knowledge of network equipment capabilities and applications
K0012	Knowledge of requirements analysis principles and practices
K0013	Knowledge of cyber defense tools and techniques
K0014	Knowledge of computer algorithm capabilities and applications
K0015	Knowledge of programming principles and practices
K0016	Knowledge of encryption algorithm capabilities and applications
K0017	Knowledge of cryptography principles and practices
K0018	Knowledge of data administration policies and procedures
K0019	Knowledge of data backup and recovery policies and procedures
K0020	Knowledge of database systems and software

ID	Description
K0021	Knowledge of business continuity and disaster recovery (BCDR) policies and procedures
K0022	Knowledge of enterprise cybersecurity architecture principles and practices
K0024	Knowledge of host access control (HAC) systems and software
K0025	Knowledge of network communications principles and practices
K0027	Knowledge of human-computer interaction (HCI) principles and practices
K0028	Knowledge of cybersecurity assessment and authorization processes
K0029	Knowledge of risk management principles and practices
K0030	Knowledge of software development principles and practices as they relate to cybersecurity
K0031	Knowledge of information sources for identifying and effectively addressing vulnerabilities
K0032	Knowledge of incident response principles and practices
K0034	Knowledge of methods to conduct best practice analysis
K0035	Knowledge of Confidentiality, Integrity and Availability (CIA) principles and practices
K0037	Knowledge of risk management policies and procedures
K0039	Knowledge of low-level programming languages
K0042	Knowledge of identity and access management (IAM) principles and practices
K0043	Knowledge of network traffic analysis tools and techniques
K0044	Knowledge of new and emerging technologies, as they relate to cybersecurity
K0045	Knowledge of operating system (OS) principles
K0046	Knowledge of network traffic protocols

ID	Description
K0047	Knowledge of packet-level analysis tools and techniques
K0048	Knowledge of parallel and distributed computing principles and practices
K0049	Knowledge of policy-based access controls
K0051	Knowledge of programming language structures and logic
K0053	Knowledge of cybersecurity management principles and practices
K0054	Knowledge of system design tools and techniques
K0056	Knowledge of all aspects of system lifecycle management
K0057	Knowledge of systems testing and evaluation tools and techniques
K0058	Knowledge of telecommunications principles and practices
K0059	Knowledge of data management tools and techniques
K0061	Knowledge of the organization's IT strategy and objectives
K0062	Knowledge of systems engineering processes
K0063	Knowledge of virtual private network (VPN) systems and software
K0064	Knowledge of network attack characteristics
K0065	Knowledge of insider threat laws and regulations
K0066	Knowledge of computer physical components
K0068	Knowledge of network tools and techniques
K0069	Knowledge of defense-in-depth principles and practices
K0070	Knowledge of network communication types

ID	Description
K0072	Knowledge of file extensions
K0073	Knowledge of supply chain risk management principles and practices
K0074	Knowledge of the national cybersecurity regulations and requirements relevant to the organization
K0075	Knowledge of digital forensics data characteristics
K0076	Knowledge of interpreted and compiled computer languages
K0077	Knowledge of threat intelligence sources, capabilities and limitations
K0078	Knowledge of how threat intelligence sources collect intelligence
K0080	Knowledge of new and emerging cybersecurity risks
K0081	Knowledge of import and export control laws and regulations as they relate to cybersecurity
K0083	Knowledge of supply chain risk management standards and best practices as they relate to cybersecurity
K0084	Knowledge of cybersecurity policies and procedures
K0085	Knowledge of the organization's IT user security policies
K0086	Knowledge of network attack vectors
K0087	Knowledge of cyberattack characteristics
K0088	Knowledge of cyberattack actor characteristics
K0090	Knowledge of system administration, network management and operating system hardening methods
K0092	Knowledge of cyber-related supply chain risk management policies and procedures
K0093	Knowledge of critical information systems that were designed with limited technical cybersecurity controls
K0094	Knowledge of hardware reverse engineering tools and techniques

ID	Description
K0095	Knowledge of middleware software capabilities and applications
K0096	Knowledge of networking protocols
K0097	Knowledge of software reverse engineering tools and techniques
K0098	Knowledge of Extensible Markup Language (XML) schemas
K0099	Knowledge of the stages of a cyberattack
K0100	Knowledge of network architecture principles and practices
K0101	Knowledge of network systems management principles and practices
K0102	Knowledge of encryption tools and techniques
K0103	Knowledge of malware signature principles and practices
K0104	Knowledge of Windows ports and services
K0105	Knowledge of data remediation tools and techniques
K0106	Knowledge of cloud computing principles and practices
K0107	Knowledge of data classification standards and best practices
K0108	Knowledge of database access application programming interfaces
K0109	Knowledge of process improvement principles and practices
K0111	Knowledge of service management principles and practices
K0112	Knowledge of application firewall principles and practices
K0113	Knowledge of industry cybersecurity standards and frameworks
K0114	Knowledge of covert communication tools and techniques

ID	Description
K0117	Knowledge of the Open Systems Interconnect (OSI) reference model
K0119	Knowledge of operating system administration principles and practices
K0120	Knowledge of computer architecture principles and practices
K0121	Knowledge of cloud service models and frameworks
K0123	Knowledge of malware analysis principles and practices
K0124	Knowledge of Personally Identifiable Information (PII) data security standards and best practices
K0125	Knowledge of Payment Card Industry (PCI) data security standards and best practices
K0126	Knowledge of data security standards relating to the sector in which the organization operates
K0128	Knowledge of critical infrastructure laws and regulations as they relate to cybersecurity
K0129	Knowledge of configuration management tools and techniques
K0132	Knowledge of content synchronization tools and techniques
K0133	Knowledge of cybersecurity data classification tools and techniques
K0134	Knowledge of cybersecurity system testing tools and techniques
K0135	Knowledge of network hardware threats and vulnerabilities
K0136	Knowledge of countermeasure design principles and practices
K0137	Knowledge of network mapping principles and practices
K0139	Knowledge of subnetting tools and techniques
K0144	Knowledge of cybersecurity information sharing principles and practices
K0145	Knowledge of command-line tools and techniques

ID	Description
K0146	Knowledge of embedded systems and how cybersecurity controls can be applied to them
K0147	Knowledge of Intrusion Detection System (IDS) tools and techniques
K0149	Knowledge of network design principles and practices
K0153	Knowledge of penetration testing principles and practices
K0156	Knowledge of database administration principles and practices
K0159	Knowledge of operations security (OPSEC) principles and practices
K0160	Knowledge of organizational objectives and leadership priorities
K0166	Knowledge of risk scoring principles and practices
K0167	Knowledge of risk assessment tools and techniques
K0169	Knowledge of data compromise reporting policies and procedures
K0170	Knowledge of hexadecimal data
K0171	Knowledge of code analysis tools and techniques
K0172	Knowledge of Public Key Infrastructure (PKI) principles
K0173	Knowledge of digital certificate management principles and practices
K0174	Knowledge of research and design processes and procedures
K0175	Knowledge of network firewall principles and practices
K0176	Knowledge of encryption algorithms
K0177	Knowledge of network configurations
K0178	Knowledge of behavior analytics tools and techniques

ID	Description
K0179	Knowledge of biometric identity tools and techniques
K0180	Knowledge of data loss prevention (DLP) tools and techniques
K0181	Knowledge of Internet of things (IoT) security principles and practices
K0182	Knowledge of multi-factor authentication (MFA) tools and techniques
K0183	Knowledge of network segmentation principles and practices
K0184	Knowledge of security orchestration, automation, and response (SOAR) tools and techniques
K0185	Knowledge of zero trust principles and practices
K0186	Knowledge of cybersecurity controls
K0187	Knowledge of risk mitigation principles and practices
K0188	Knowledge of data protection principles and practices
K0189	Knowledge of cybersecurity vulnerabilities
K0190	Knowledge of access control methods
K0191	Knowledge of vulnerability assessment tools and techniques
K0192	Knowledge of cryptographic key management principles and practices
K0193	Knowledge of secure database design practices
K0194	Knowledge of network access control (NAC) systems and software
K0195	Knowledge of incident response policies and procedures
K0196	Knowledge of incident response tools and techniques
K0197	Knowledge of Risk Adaptive (Adaptable) Access Controls (RAdAC)

ID	Description
K0198	Knowledge of insider threat tools and techniques
K0199	Knowledge of insider threat operational indicators
K0200	Knowledge of insider threat policies and procedures
K0201	Knowledge of insider threat tactics
K0202	Knowledge of insider threat targets
K0203	Knowledge of computer peripherals
K0204	Knowledge of middleware cybersecurity best approaches
K0205	Knowledge of network cybersecurity principles and practices
K0206	Knowledge of Unix ports and services
K0207	Knowledge of Knowledge management principles and practices
K0208	Knowledge of Knowledge management tools and techniques
K0209	Knowledge of process maturity models and frameworks
K0210	Knowledge of service management standards and best practices
K0211	Knowledge of cybersecurity information sharing tools and techniques
K0212	Knowledge of Intrusion Prevention System (IPS) tools and techniques
K0213	Knowledge of penetration testing tools and techniques
K0214	Knowledge of red team functions and capabilities
K0215	Knowledge of exploitation laws and regulations
K0216	Knowledge of cyber defense laws and regulations

ID	Description
K0500	Knowledge of scripting principles and practices
K0503	Knowledge of network hardware devices and functions
K0504	Knowledge of network technologies
K0507	Knowledge of multi-level security (MLS) systems and cross domain solutions
K0509	Knowledge of N-tiered topologies in IT systems
K0510	Knowledge of information technology (IT) architecture models and frameworks
K0512	Knowledge of Information Technology (IT) evaluation and validation principles and practices
K0513	Knowledge of Information Technology (IT) fault tolerance tools and techniques
K0514	Knowledge of demilitarized zones in Information Technology (IT) environments
K0516	Knowledge of design modeling
K0517	Knowledge of design methods
K0518	Knowledge of fail-over or alternate site requirements
K0519	Knowledge of system backup requirements
K0520	Knowledge of performance tuning tools and techniques
K0521	Knowledge of container orchestration security best practices
K1000	Knowledge of complex data structures
K1001	Knowledge of data warehousing principles and practices
K1002	Knowledge of database management system (DBMS) principles and practices
K1003	Knowledge of digital rights management (DRM) tools and techniques

ID	Description
K1005	Knowledge of enterprise communication systems and software
K1006	Knowledge of resiliency and redundancy principles and practices
K1007	Knowledge of cybersecurity systems engineering principles and standards used by the organization
K1008	Knowledge of Local Area Networks (LAN) principles and practices
K1009	Knowledge of process engineering principles and practices
K1010	Knowledge of query languages
K1011	Knowledge of configuration management (CM) tools and techniques
K1012	Knowledge of software debugging principles and practices
K1013	Knowledge of software design tools and techniques
K1014	Knowledge of software development models and frameworks
K1015	Knowledge of software engineering principles and practices
K1016	Knowledge of the organization's data-sets sources, characteristics and uses
K1017	Knowledge of structured analysis principles and practices
K1021	Knowledge of secure coding tools and techniques
K1023	Knowledge of software quality assurance (SQA) principles and practices
K1024	Knowledge of secure software deployment tools and techniques
K1025	Knowledge of logging tools and technologies
K1027	Knowledge of data analysis tools and techniques
K1028	Knowledge of machine learning principles and practices

ID	Description
K1030	Knowledge of mobile communications architecture
K1031	Knowledge of operating system structures and internals
K1032	Knowledge of network analysis tools and techniques
K1034	Knowledge of ethical hacking tools and techniques
K1035	Knowledge of computer engineering principles and practices
K1036	Knowledge of information theory principles and practices
K1037	Knowledge of root cause analysis tools and techniques
K1038	Knowledge of research strategies
K1039	Knowledge of developing software in high-level languages
K1040	Knowledge of operating system scripts
K1041	Knowledge of software testing tools and techniques
K1043	Knowledge of natural language processing tools and techniques
K1045	Knowledge of Machine Learning algorithms
K1047	Knowledge of open-source technologies
K1048	Knowledge of software testing methods
K1049	Knowledge of data mapping tools and techniques
K1050	Knowledge of coding and testing standards
K1051	Knowledge of hardware design principles and practices
K1052	Knowledge of data storage principles and practices

ID	Description
K1053	Knowledge of software and systems engineering life cycle standards
K1054	Knowledge of data gathering tools and techniques
K1055	Knowledge of Artificial Intelligence (AI) principles and practices
K1056	Knowledge of Artificial Intelligence (AI) tools and techniques
K1057	Knowledge of API security principles and practices
K1058	Knowledge of deepfake detection tools and techniques
K1059	Knowledge of DevSecOps principles and practices
K1060	Knowledge of homomorphic encryption tools and techniques
K1061	Knowledge of phishing prevention tools and techniques
K1062	Knowledge of quantum cryptography challenges and opportunities
K1063	Knowledge of quantum key distribution (QKD) principles and practices
K1064	Knowledge of security information and event management (SIEM) tools and techniques
K1065	Knowledge of data mining principles and practices
K1066	Knowledge of database query language capabilities and applications
K1067	Knowledge of database schema capabilities and applications
K1068	Knowledge of Wide Area Networks (WAN) principles and practices
K1069	Knowledge of data visualization tools and techniques
K1500	Knowledge of system performance indicators
K1501	Knowledge of resource management principles and practices

ID	Description
K1502	Knowledge of server administration principles and practices
K1503	Knowledge of client and server architecture
K1504	Knowledge of system design standards and best practices
K1505	Knowledge of technology integration processes
K1506	Knowledge of program management principles and practices
K1509	Knowledge of technology procurement principles and practices
K1510	Knowledge of continuous monitoring tools and techniques
K1511	Knowledge of data security controls
K1512	Knowledge of system availability measures
K1513	Knowledge of mobile operating systems
K1514	Knowledge of system design policies and practices
K1515	Knowledge of project management principles and practices
K2000	Knowledge of cognitive domain models and frameworks
K2001	Knowledge of virtualization tools and techniques
K2002	Knowledge of learning assessment tools and techniques
K2004	Knowledge of instructional design principles and practices
K2005	Knowledge of training best practices
K2007	Knowledge of learning management system (LMS) systems and software
K2009	Knowledge of learning modes

ID	Description
K2010	Knowledge of training systems and software
K2011	Knowledge of Saudi Cybersecurity Workforce Framework (SCyWF), job roles and associated tasks, Knowledge and skills
K2012	Knowledge of media production tools and techniques
K2013	Knowledge of the organization's human resource policies, processes and procedures
K2014	Knowledge of the organization's training and education policies and procedures
K2015	Knowledge of training needs assessment principles and practices
K2020	Knowledge of technical delivery options for cybersecurity training and exercising and their limitations
K2021	Knowledge of cybersecurity exercises and competitions
K2022	Knowledge of organizational cybersecurity workforce requirements
K2023	Knowledge of the organizational cybersecurity workforce
K2024	Knowledge of cybersecurity workforce policies and procedures
K2025	Knowledge of organizational cybersecurity goals and objectives
K2026	Knowledge of cybersecurity career paths
K2027	Knowledge of cybersecurity workforce trends
K2028	Knowledge of instructional design models and frameworks
K2029	Knowledge of organizational career progressions
K2030	Knowledge of cybersecurity personnel roles and responsibilities
K2031	Knowledge of mission assurance practices and principles
K2032	Knowledge of personnel systems and software

ID	Description
K2033	Knowledge of cybersecurity awareness program design principles and practices
K2034	Knowledge of phishing simulation tools and techniques
K2035	Knowledge of gamification techniques and their application in cybersecurity training and awareness programs
K2036	Knowledge of cybersecurity awareness evaluation methods
K2037	Knowledge of cybersecurity awareness best practices
K2501	Knowledge of technology suitability evaluation methods
K2502	Knowledge of enterprise information technology (IT) architecture principles and practices
K2504	Knowledge of all-source intelligence reporting policies and procedures
K2505	Knowledge of auditing policies and procedures
K2506	Knowledge of formats for issuing cybersecurity compliance reports to external partners
K2507	Knowledge of organization's formats for cybersecurity risk and compliance reporting
K2509	Knowledge of auditing laws and regulations
K2510	Knowledge of local and international accreditation standards
K2511	Knowledge of organization's current risk profile
K2512	Knowledge of cross-border data transfer regulations, including data residency, data sovereignty, and data localization requirements
K2513	Knowledge of cyber insurance principles and practices
K2514	Knowledge of endpoint detection and response (EDR) tools and techniques
K2515	Knowledge of extended detection and response (XDR) tools and techniques
K2516	Knowledge of logging policies and procedures

ID	Description
K3000	Knowledge of digital forensic data principles and practices
K3001	Knowledge of intelligence data gathering principles and practices
K3002	Knowledge of the organization's policies and standard operating procedures relating to cybersecurity
K3005	Knowledge of data protection-enhancing tools and techniques
K3008	Knowledge of data protection and cybersecurity regulators
K3009	Knowledge of organizational data protection policies and procedures
K3010	Knowledge of data protection controls
K3011	Knowledge of intelligence data gathering policies and procedures
K3012	Knowledge of intelligence data gathering laws and regulations
K3502	Knowledge of signal jamming tools and techniques
K3506	Knowledge of protocol analyzer tools and techniques
K3507	Knowledge of organizational cybersecurity incident response plans
K3508	Knowledge of ransomware defense tools and techniques
K3509	Knowledge of signal jamming laws and regulations
K4000	Knowledge of remote access principles and practices
K4001	Knowledge of the capabilities and functionality associated with content creation technologies
K4002	Knowledge of the capabilities and functionality of collaborative technologies and their implications for cybersecurity
K4004	Knowledge of taxonomy and semantic ontology theory
K4006	Knowledge of supplier and product evaluation methods

ID	Description
K4007	Knowledge of IT service catalogues
K4008	Knowledge of credential management systems and software
K4009	Knowledge of data-at-rest encryption (DARE) standards and best practices
K4011	Knowledge of data concealment tools and techniques
K4012	Knowledge of data mining tools and techniques
K4015	Knowledge of wireless local area network (WLAN) tools and techniques
K4016	Knowledge of reporting policies and procedures
K4017	Knowledge of obfuscation tools and techniques
K4019	Knowledge of system availability requirements
K4020	Knowledge of symmetric encryption principles and practices
K4021	Knowledge of Attribute-Based Access Control (ABAC) principles and practices
K4022	Knowledge of Cloud Access Security Broker (CASB) principles and practices
K4023	Knowledge of Discretionary Access Control (DAC) principles and practices
K4024	Knowledge of Kerberos authentication principles and practices
K4025	Knowledge of Mandatory Access Control (MAC) principles and practices
K4026	Knowledge of Role-Based Access Control (RBAC) principles and practices
K4027	Knowledge of secure access service edge (SASE) tools and techniques
K4028	Knowledge of Single Sign-On (SSO) principles and practices
K4029	Knowledge of Single Sign-On (SSO) tools and techniques

ID	Description
K4030	Knowledge of remote access tools and techniques
K4504	Knowledge of programming languages
K4505	Knowledge of operating system (OS) tools and techniques
K4506	Knowledge of social engineering tools and techniques
K4508	Knowledge of network systems management tools and techniques
K4511	Knowledge of cybersecurity adversarial tactics principles and practices
K4512	Knowledge of cybersecurity adversarial tactics tools and techniques
K4513	Knowledge of cybersecurity adversarial tactics policies and procedures
K4514	Knowledge of red, blue, and purple teaming principles and practices
K5000	Knowledge of server diagnostic tools and techniques
K5001	Knowledge of the main types of electronic devices and their capabilities
K5002	Knowledge of file system implementation principles and practices
K5003	Knowledge of digital evidence seizure policies and procedures
K5006	Knowledge of digital evidence preservation policies and procedures
K5007	Knowledge of chain of custody policies and procedures
K5008	Knowledge of persistent data principles and practices
K5009	Knowledge of web mail tools and techniques
K5010	Knowledge of system file characteristics
K5011	Knowledge of deployable forensics principles and practices

ID	Description
K5012	Knowledge of web filtering systems and software
K5014	Knowledge of event correlation tools and techniques
K5015	Knowledge of electronic evidence laws and regulations
K5016	Knowledge of national or applicable judicial and court procedure for cybercrime and fraud cases
K5017	Knowledge of data carving tools and techniques
K5019	Knowledge of anti-forensics tools and techniques
K5020	Knowledge of forensics lab design principles and practices
K5021	Knowledge of debugging tools and techniques
K5022	Knowledge of filename extension abuse
K5023	Knowledge of malware analysis tools and techniques
K5024	Knowledge of virtual machine detection tools and techniques
K5025	Knowledge of crisis management protocols
K5026	Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity
K5028	Knowledge of binary analysis tools and techniques
K5031	Knowledge of operational design principles and practices
K5032	Knowledge of intelligence collection laws and regulations
K5033	Knowledge of digital forensics tools and techniques
K5034	Knowledge of data integrity principles and practices
K5035	Knowledge of information sanitization methods

ID	Description
K5036	Knowledge of steganography practices and principles
K5037	Knowledge of chain of custody processes
K5038	Knowledge of Fault Detection and Diagnostics (FDD) tools and techniques
K5039	Knowledge of deployable forensics tools and techniques
K5040	Knowledge of forensics lab design systems and software
K5041	Knowledge of crisis management processes
K5042	Knowledge of crisis management tools and techniques
K5501	Knowledge of content management system (CMS) capabilities and applications
K5502	Knowledge of cyberattack tools and techniques
K5503	Knowledge of data classification policies and procedures
K5505	Knowledge of computer networking principles and practices
K5510	Knowledge of cyber operations principles and practices
K5511	Knowledge of host-based security products and their capabilities
K5513	Knowledge of electronic communication systems threats and risks
K5514	Knowledge of wireless networks threats and risks
K5516	Knowledge of different types of organization, team and people involved in cyber threat intelligence collection
K5519	Knowledge of the tactics an organization can employ to anticipate and counter an attacker's capabilities and actions
K5520	Knowledge of network addressing principles and practices
K5521	Knowledge of cyber threat actors

ID	Description
K5522	Knowledge of performing threat environment analysis
K5523	Knowledge of malware
K5524	Knowledge of cyber decision-making policies and procedures
K5525	Knowledge of cyber threat actors functions and capabilities
K5526	Knowledge of cyber threat actors tools and techniques
K5529	Knowledge of the factors of threat that could impact collection operations
K5531	Knowledge of threat systems and software
K5532	Knowledge of machine virtualization tools and techniques
K5535	Knowledge of denial and deception tools and techniques
K5536	Knowledge of analytical tools and techniques
K5537	Knowledge of threat hunting principles and practices
K6002	Knowledge of ICS/OT products capabilities and functions
K6003	Knowledge of ICS/OT risk management standards and best practices
K6004	Knowledge of multi-level security systems and cross domain solutions applicable to IT and ICS/OT environments
K6005	Knowledge of system protection planning measures for IT and ICS/OT environments
K6006	Knowledge of N-tiered topologies for ICS/OT environments
K6007	Knowledge of the organization's architectural concepts and patterns in ICS/OT environments
K6009	Knowledge of evaluation and validation criteria relevant to the ICS/OT domains
K6010	Knowledge of system fault tolerance methodologies in ICS/OT environments

ID	Description
K6011	Knowledge of demilitarized zones in ICS/OT environments
K6012	Knowledge of supervisory control and data acquisition (SCADA) systems and software
K6013	Knowledge of architectures and designs of telephony networks in ICS/OT environments
K6014	Knowledge of ICS/OT operating environments and functions
K6015	Knowledge of ICS/OT network traffic protocols
K6016	Knowledge of ICS/OT devices
K6017	Knowledge of the ICS/OT threat landscape
K6019	Knowledge of Intrusion Detection System (IDS) tools and techniques for ICS/OT environments
K6020	Knowledge of ICS security tools and techniques
K6021	Knowledge of design methods for ICS/OT environments
K6022	Knowledge of ICS/OT programming languages
K6023	Knowledge of Intrusion Prevention System (IPS) tools and techniques for ICS/OT environments

TABLE 10: KNOWLEDGE DESCRIPTIONS

Skill ID	Skill Description	Technical?
S0001	Skill in conducting vulnerability scans	Yes
S0002	Skill in identifying malware	Yes
S0003	Skill in applying information technologies into proposed solutions	Yes
S0004	Skill in applying core cybersecurity principles	Yes
S0005	Skill in applying host access controls	Yes
S0006	Skill in developing digital signatures	Yes
S0008	Skill in designing the integration of hardware and software solutions	Yes
S0009	Skill in detecting host-based and network-based intrusions	Yes
S0011	Skill in developing network infrastructure contingency and recovery plans	Yes
S0012	Skill in evaluating cybersecurity system designs	Yes
S0013	Skill in preserving digital evidence integrity	Yes
S0014	Skill in configuring network sensors	Yes
S0015	Skill in using protocol analyzer tools	Yes
S0016	Skill in configuring encrypted network communications	Yes
S0017	Skill in writing code in a currently supported programming language	Yes
S0018	Skill in solving problems	No
S0019	Skill in maintaining virtual machines	Yes

Skill ID	Skill Description	Technical?
S0020	Skill in performing digital forensics analysis	Yes
S0021	Skill in configuring and utilizing computer protection tools	Yes
S0022	Skill in securing network communications	Yes
S0023	Skill in categorizing types of vulnerabilities	Yes
S0025	Skill in performing damage assessments	Yes
S0026	Skill in performing network data analysis	Yes
S0027	Skill in configuring network protection components	Yes
S0028	Skill in conducting cybersecurity audits or reviews of technical systems	Yes
S0029	Skill in using binary analysis tools	Yes
S0030	Skill in implementing one-way hash functions	Yes
S0031	Skill in reading Hexadecimal data	Yes
S0032	Skill in identifying common encoding techniques	Yes
S0033	Skill in reading digital signatures	Yes
S0034	Skill in developing learning activities	No
S0035	Skill in applying hardening techniques	Yes
S0036	Skill in designing cybersecurity test plans	Yes
S0037	Skill in conducting application vulnerability assessments	Yes
S0038	Skill in implementing public key infrastructure (PKI) encryption	Yes

Skill ID	Skill Description	Technical?
S0039	Skill in applying cybersecurity models	Yes
S0040	Skill in assessing cybersecurity controls	Yes
S0041	Skill in performing packet-level analysis	Yes
S0044	Skill in performing risk assessments	Yes
S0045	Skill in applying secure coding techniques.	Yes
S0046	Skill in performing event correlation	Yes
S0047	Skill in using code analysis tools	Yes
S0048	Skill in performing root cause analysis	Yes
S0049	Skill in safely and effectively conducting research using deep web	Yes
S0050	Skill in performing target system analysis	Yes
S0051	Skill in preparing briefings	No
S0052	Skill in recognizing abnormal network activity in traffic	Yes
S0053	Skill in performing reverse engineering of software	Yes
S0054	Skill in analyzing tools, techniques, and procedures used by adversaries remotely to exploit and establish persistence on a target	Yes
S0055	Skill in incorporating feedback	No
S0056	Skill in performing threat analysis	Yes
S0057	Skill in bridging the gap between threat intelligence and strategy effectiveness	No
S0058	Skill in communicating effectively	No

Skill ID	Skill Description	Technical?
S0059	Skill in identifying cybersecurity threats	Yes
S0060	Skill in responding effectively to cyber incidents in cloud environment	Yes
S0061	Skill in applying confidentiality, integrity, and availability (CIA) principles	Yes
S0062	Skill in using risk management techniques	Yes
S0063	Skill in utilizing cyber defense service providers	Yes
S0064	Skill in identifying cybersecurity issues in the organization's supply chain	Yes
S0065	Skill in designing cyber processes and solutions	Yes
S0066	Skill in high-level programming	Yes
S0067	Skill in low-level programming	Yes
S0068	Skill in analyzing software configurations	Yes
S0069	Skill in performing network data flow analysis	Yes
S0070	Skill in identifying cybersecurity related coding flaws	Yes
S0071	Skill in designing secure network architectures	Yes
S0072	Skill in applying systems design tools, methods and techniques	Yes
S0073	Skill in integrating cybersecurity requirements in the acquisitions process	No
S0074	Skill in designing secure architectures	Yes
S0075	Skill in designing frameworks	No
S0076	Skill in mitigating deception in reporting and analysis	No

Skill ID	Skill Description	Technical?
S0077	Skill in applying critical thinking	No
S0078	Skill in establishing priorities	No
S0079	Skill in creating a risk management program	No
S0080	Skill in creating a risk management strategy	No
S0081	Skill in creating an internal information sharing program	No
S0082	Skill in identifying critical information systems	Yes
S0083	Skill in installing system and component upgrades	Yes
S0084	Skill in optimizing system performance	Yes
S0085	Skill in testing backup and recovery plans	Yes
S0086	Skill in communicating cybersecurity concepts and practices effectively	No
S0087	Skill in developing cybersecurity strategy	No
S0088	Skill in creating cybersecurity policies	No
S0089	Skill in applying risk management strategy and practices	Yes
S0090	Skill in sharing best practices across organizations	No
S0091	Skill in working with security logs	Yes
S0092	Skill in identifying vulnerabilities in security systems	Yes
S0093	Skill in capturing malware	Yes
S0094	Skill in containing malware	Yes

Skill ID	Skill Description	Technical?
S0095	Skill in reporting malware	Yes
S0096	Skill in applying network access controls	Yes
S0097	Skill in deploying digital signatures	Yes
S0098	Skill in testing network infrastructure contingency and recovery plans	Yes
S0099	Skill in implementing network infrastructure contingency and recovery plans	Yes
S0100	Skill in using one-way hash functions	Yes
S0101	Skill in interpreting digital signatures	Yes
S0102	Skill in reading application vulnerability assessment reports	Yes
S0103	Skill in presenting to an audience	No
S0104	Skill in interpreting abnormal network activity in traffic	Yes
S0106	Skill in integrating cyber processes and solutions	Yes
S0501	Skill in performing design modeling	Yes
S0503	Skill in designing multi-tier security solutions	Yes
S0504	Skill in the use of design methods	Yes
S0505	Skill in translating operational requirements into security controls	Yes
S0506	Skill in implementing network segregation	Yes
S0507	Skill in performing cybersecurity architecture analysis	Yes
S0508	Skill in performing user needs analysis	No

Skill ID	Skill Description	Technical?
S0509	Skill in analyzing an organization's enterprise information technology architecture	Yes
S0510	Skill in building use cases	Yes
S0511	Skill in designing cross-domain solutions	Yes
S1000	Skill in developing algorithms	Yes
S1001	Skill in debugging software	Yes
S1002	Skill in creating mathematical models	Yes
S1003	Skill in implementing input validation	Yes
S1004	Skill in designing cybersecurity controls	Yes
S1005	Skill in developing data dictionaries	Yes
S1006	Skill in developing data models	Yes
S1007	Skill in developing cybersecurity system controls	Yes
S1008	Skill in identifying the protection needs of information systems and networks	Yes
S1009	Skill in preparing reports	No
S1010	Skill in applying software testing methods	Yes
S1012	Skill in performing data preprocessing	Yes
S1013	Skill in identifying hidden patterns or relationships	Yes
S1014	Skill in performing format conversions	Yes
S1015	Skill in performing sensitivity analysis	Yes

Skill ID	Skill Description	Technical?
S1016	Skill in developing machine understandable semantic ontologies	Yes
S1017	Skill in performing regression analysis	Yes
S1018	Skill in performing transformation analytics	Yes
S1019	Skill in applying descriptive statistics	Yes
S1020	Skill in performing data analysis	Yes
S1021	Skill in performing data mapping	Yes
S1022	Skill in using outlier identification and removal techniques	Yes
S1023	Skill in writing computer scripts to automate tasks	Yes
S1024	Skill in performing systems engineering	Yes
S1026	Skill in implementing error handling in applications	Yes
S1028	Skill in performing open source intelligence (OSINT) research	Yes
S1029	Skill in mining data	Yes
S1030	Skill in assessing an organization's data assets	Yes
S1031	Skill in designing object-oriented systems	Yes
S1032	Skill in using version control systems	Yes
S1034	Skill in designing automated analytics systems	Yes
S1035	Skill in conducting research	No
S1036	Skill in developing machine learning models	Yes

Skill ID	Skill Description	Technical?
S1038	Skill in identifying forensic digital footprints	Yes
S1039	Skill in performing static code analysis	Yes
S1040	Skill in conducting customer interviews	No
S1041	Skill in caching data	Yes
S1042	Skill in cataloging data	Yes
S1043	Skill in compiling data	Yes
S1044	Skill in distributing data	Yes
S1045	Skill in retrieving data	Yes
S1046	Skill in designing data storage solutions	Yes
S1047	Skill in implementing data storage solutions	Yes
S1048	Skill in performing quantitative analysis	Yes
S1049	Skill in performing gap analysis	No
S1050	Skill in creating complex data structures	Yes
S1051	Skill in using data visualization tools	Yes
S1052	Skill in deploying software securely	Yes
S1053	Skill in configuring security logging	Yes
S1054	Skill in performing data structure analysis	Yes
S1055	Skill in creating statistical models	Yes

Skill ID	Skill Description	Technical?
S1056	Skill in using mathematical models	Yes
S1057	Skill in using statistical models	Yes
S1058	Skill in performing data mining analysis	Yes
S1059	Skill in developing object-oriented systems	Yes
S1060	Skill in developing automated analytics systems	Yes
S1500	Skill in creating system security policies	Yes
S1501	Skill in evaluating third-party supplier trustworthiness	No
S1502	Skill in continually identifying new technologies and their potential impact on cybersecurity requirements	Yes
S1504	Skill in collaborating with internal and external stakeholders	No
S1505	Skill in integrating cybersecurity requirements into procurement processes	No
S1506	Skill in identifying organization's cybersecurity-related technological challenges	No
S1507	Skill in identifying organization's cybersecurity-related business challenges	No
S1508	Skill in designing and managing a Security Fusion Center	No
S1509	Skill in designing and managing a Security Operations Center (SOC)	No
S1510	Skill in evaluating third-party product trustworthiness	Yes
S1511	Skill in performing cost/benefit analysis	Yes
S2001	Skill in using Knowledge management technologies	Yes
S2002	Skill in performing network traffic analysis	Yes

Skill ID	Skill Description	Technical?
S2003	Skill in developing curricula	No
S2004	Skill in identifying gaps in technical capabilities	No
S2006	Skill in applying technologies for instructional purposes	Yes
S2008	Skill in developing position qualification requirements	No
S2010	Skill in performing technical writing	No
S2011	Skill in deploying virtual machines	Yes
S2012	Skill in assessing learner comprehension	No
S2013	Skill in providing effective feedback to trainees	No
S2014	Skill in developing instructional materials	No
S2015	Skill in assessing and forecasting staffing requirements	No
S2016	Skill in developing career paths	No
S2017	Skill in evaluating workforce trends	No
S2018	Skill in executing command line tools	Yes
S2019	Skill in using electronic communication systems	Yes
S2020	Skill in conducting a training needs assessment	No
S2021	Skill in adapting teaching methods to accommodate diverse learning styles, abilities, and cultural backgrounds	No
S2022	Skill in establishing a respectful and inclusive classroom atmosphere that encourages learners to participate and succeed	No
S2023	Skill in teaching training programs	No

Skill ID	Skill Description	Technical?
S2024	Skill in developing training programs	No
S2025	Skill in developing cybersecurity awareness content tailored to specific user roles and risk profiles	Yes
S2026	Skill in configuring and executing phishing simulation campaigns	Yes
S2027	Skill in designing gamified awareness activities	Yes
S2028	Skill in interpreting feedback and assessment data to improve awareness training	No
S2029	Skill in communicating cybersecurity awareness concepts to non-technical audiences	No
S2500	Skill in monitoring system performance	Yes
S2501	Skill in applying cybersecurity controls	Yes
S2502	Skill in identifying Test and Evaluation Strategies (TES) infrastructure requirements	Yes
S2504	Skill in managing test assets	Yes
S2506	Skill in reviewing logs	Yes
S2507	Skill in troubleshooting cyber defense infrastructure anomalies	Yes
S2509	Skill in conducting system reviews from a cybersecurity perspective	Yes
S2512	Skill in applying policies that meet system security objectives	Yes
S2513	Skill in performing administrative planning activities	No
S2516	Skill in auditing network devices	Yes
S2517	Skill in identifying intelligence gaps and limitations	Yes
S2520	Skill in identifying threats' regional languages and dialects	No

Skill ID	Skill Description	Technical?
S2521	Skill in identifying devices that work at each level of protocol models	Yes
S2522	Skill in performing geospatial data analysis	Yes
S2523	Skill in prioritizing information	No
S2524	Skill in interpreting compiled programming languages	Yes
S2525	Skill in interpreting and evaluating metadata	Yes
S2526	Skill in interpreting traceroute results	Yes
S2527	Skill in interpreting vulnerability scanner results	Yes
S2529	Skill in managing client relationships	No
S2530	Skill in preparing plans	No
S2533	Skill in analyzing reports and recommending actions to be taken	No
S2537	Skill in performing intelligence collection analysis	Yes
S2540	Skill in accessing information relating to current internal and external cybersecurity resources and their current utilization and priorities	No
S2541	Skill in using databases	Yes
S2542	Skill in reviewing corporate strategies or applicable legal, regulatory or policy documents to identify issues requiring clarification or action	No
S2543	Skill in developing appropriate and effective requirements to inform selection of cyber threat intelligence sources or monitoring activity	No
S2544	Skill in interpreting readiness reporting	No
S2546	Skill in analyzing internal and external reports	No
S2547	Skill in designing Test and Evaluation Strategies (TES)	Yes

Skill ID	Skill Description	Technical?
S2548	Skill in facilitating group discussions	No
S2549	Skill in developing cybersecurity assessments	No
S2550	Skill in functioning effectively in a dynamic, fast-paced environment	No
S2551	Skill in identifying external partners	No
S2552	Skill in mitigating cognitive biases	No
S2553	Skill in applying supply chain risk management standards	Yes
S2554	Skill in performing big data analysis	Yes
S2555	Skill in defining and actively managing cyber risk appetite and risk profile	Yes
S2556	Skill in configuring systems for performance enhancement	Yes
S2557	Skill in identifying evidence of past intrusions	Yes
S2558	Skill in interpreting interpretive programming languages	Yes
S3000	Skill in creating data protection policies	Yes
S3001	Skill in negotiating vendor agreements	No
S3002	Skill in evaluating vendor data protection practices	No
S3003	Skill in evaluating cybersecurity laws	No
S3004	Skill in evaluating cybersecurity regulations	No
S3005	Skill in identifying the need for legal action after cybersecurity incidents	Yes
S3500	Skill in using incident handling methodologies	Yes

Skill ID	Skill Description	Technical?
S3501	Skill in collecting data from a variety of cybersecurity resources	Yes
S3502	Skill in conducting trend analysis	Yes
S4000	Skill in conducting information searches	No
S4001	Skill in assessing the application of cryptographic standards	Yes
S4002	Skill in analyzing cipher strength and breaking ciphers	Yes
S4003	Skill in applying cryptographic algorithms	Yes
S4004	Skill in determining asset availability, capabilities, and limitations	Yes
S4005	Skill in managing account access rights	Yes
S4006	Skill in collecting network data	Yes
S4007	Skill in deploying user credential management systems	Yes
S4008	Skill in implementing user credential management systems	Yes
S4009	Skill in implementing symmetric encryption	Yes
S4501	Skill in developing operations-based testing scenarios	Yes
S4502	Skill in performing threat modeling	Yes
S4503	Skill in testing the security of integrated systems	Yes
S4504	Skill in using penetration testing tools and techniques	Yes
S4505	Skill in performing social engineering	No
S4506	Skill in implementing network infrastructure business continuity and disaster recovery plans	Yes

Skill ID	Skill Description	Technical?
S4507	Skill in assessing an organization's threat environment	Yes
S4509	Skill in writing custom code to bypass security controls	Yes
S4510	Skill in implementing adversary Tactics, Techniques and Procedures	Yes
S4512	Skill in testing network infrastructure business continuity and disaster recovery plans	Yes
S5000	Skill in performing memory dump analysis	Yes
S5001	Skill in identifying forensics data in diverse media	Yes
S5002	Skill in manipulating operating system components	Yes
S5003	Skill in collecting digital evidence	Yes
S5004	Skill in setting up a forensic workstation	Yes
S5005	Skill in using digital forensic tools	Yes
S5006	Skill in disassembling PCs	Yes
S5008	Skill in performing source code analysis	Yes
S5009	Skill in performing volatile data analysis	Yes
S5010	Skill in identifying obfuscation techniques	No
S5011	Skill in interpreting debugger results	Yes
S5012	Skill in performing malware analysis	Yes
S5013	Skill in performing bit-level analysis	Yes
S5014	Skill in processing digital evidence	Yes

Skill ID	Skill Description	Technical?
S5015	Skill in writing Linux kernel scripts	Yes
S5018	Skill in identifying anomalous activity	Yes
S5019	Skill in performing file system forensic analysis	Yes
S5020	Skill in extracting information from packet captures	Yes
S5021	Skill in performing dynamic analysis	Yes
S5022	Skill in decrypting information	Yes
S5023	Skill in navigating the dark web	Yes
S5024	Skill in examining digital media	Yes
S5025	Skill in navigating system files	Yes
S5026	Skill in identifying filename extension abuse	Yes
S5027	Skill in recognizing digital forensics data	Yes
S5028	Skill in tracing low-level programming	Yes
S5029	Skill in using deployable forensics toolkits	Yes
S5030	Skill in extracting forensics data in diverse media	Yes
S5031	Skill in performing digital evidence analysis	Yes
S5032	Skill in transporting digital evidence	Yes
S5033	Skill in storing digital evidence	Yes
S5034	Skill in creating digital evidence copies	Yes

Skill ID	Skill Description	Technical?
S5500	Skill in conducting non-attributable research	No
S5501	Skill in defining an operational environment	Yes
S5502	Skill in developing or recommending analytic approaches in situations where information is incomplete or for which no precedent exists	No
S5503	Skill in evaluating potential sources of information for their value to a cyber investigation	Yes
S5504	Skill in evaluating information quality	No
S5511	Skill in recognizing network, operating system and application denial of Service (DoS) techniques	Yes
S5515	Skill in analyzing threat intelligence products	Yes
S5516	Skill in performing data queries	Yes
S5517	Skill in using data analytics tools	Yes
S5518	Skill in conducting open-source searches	Yes
S5519	Skill in using network analysis and reconstruction tools	Yes
S5520	Skill in using virtual collaborative workspace tools	Yes
S5523	Skill in monitoring threat or vulnerability situation and environmental factors	Yes
S5524	Skill in assessing the implication of cyber attacks on third parties	Yes
S5525	Skill in performing intrusion data analysis	Yes
S5526	Skill in evaluating security products	Yes
S5527	Skill in extracting metadata	Yes
S5528	Skill in performing threat emulation tactics	Yes

Skill ID	Skill Description	Technical?
S5529	Skill in performing nodal analysis	Yes
S5530	Skill in converting intelligence requirements into intelligence production tasks	Yes
S5531	Skill in thinking like threat actors	No
S5532	Skill in identifying advance persistent threats (APTs)	Yes
S5533	Skill in threat hunting	Yes
S5534	Skill in recognizing network, operating system and application deception techniques	Yes
S6000	Skill in performing design modeling in ICS/OT environments	Yes
S6001	Skill in creating test plans for ICS/OT environments	Yes
S6002	Skill in designing multi-level security solutions applicable to ICS/OT environments	Yes
S6003	Skill in implementing design methods in an IT and ICS/OT environments	Yes
S6004	Skill in translating operational requirements into security controls in ICS/OT environments	Yes
S6005	Skill in implementing network segregation in ICS/OT environments	Yes
S6006	Skill in assessing security controls of ICS/OT environments	Yes
S6007	Skill in protecting an ICS/OT environment against cyber threats	Yes
S6008	Skill in configuring ICS/OT systems for performance enhancement	Yes
S6009	Skill in using intrusion detection tools in ICS/OT environments	Yes
S6010	Skill in performing incident responses in ICS/OT environments	Yes
S6011	Skill in reading and interpreting technical diagrams relating to systems and networks in ICS/OT environments	Yes

Skill ID	Skill Description	Technical?
S6012	Skill in building use cases in ICS/OT environments	Yes
S6013	Skill in designing cross-domain solutions applicable to ICS/OT environments	Yes

TABLE 11: SKILLS DESCRIPTIONS

3.3 Appendix C: List of competency areas

The table below outlines the competency areas introduced in this version of SCyWF to address critical domains within cybersecurity. Each competency area provides a description of the specific capabilities required to perform specialized cybersecurity functions.

CA ID	CA Name	Description
CA001	Identity and Access Management	This Competency Area describes the learner's capabilities in managing digital identities, roles, and access controls to ensure secure and compliant access to protected resources. It includes authentication, authorization, identity lifecycle management, and applying access control principles to safeguard data integrity and enforce authorized access
CA002	Cloud Security	This Competency Area describes a learner's capabilities to protect cloud data, applications, and infrastructure from internal and external threats
CA003	Communications Security	This Competency Area describes a learner's capabilities to secure the operation, control, and communication over various network infrastructures, addressing the unique security challenges of wireless, analog, and digital telecommunications. It encompasses essential Knowledge of networking, secure communication protocols, and techniques to protect transmissions and broadcasting effectively
CA004	Cryptography	This Competency Area describes a learner's capabilities to transform data using cryptographic processes to ensure it can only be read by the person who is authorized to access it
CA005	Operating Systems Security	This Competency Area describes a learner's capabilities to install, administer, troubleshoot, backup, and conduct recovery of Operating Systems (OS), including in simulated environments
CA006	Supply Chain Security	This Competency Area describes a learner's capabilities to analyze and control digital and physical risks presented by technology products or services purchased from parties outside your organization
CA007	Data Security and Administration	This Competency Area describes the learner's capabilities to secure data across its entire lifecycle, focusing on data integrity, secure database management, access control, and lifecycle management of data security. It includes technical measures to protect data from unauthorized access, modification, and loss, as well as ensuring data security standards are met across storage, access, and disposal stages
CA008	Security Risk Analysis	This Competency Area describes a learner's capabilities related to assessing, identifying, and evaluating potential risks to information systems and organizational assets. It includes analyzing threats, vulnerabilities, and the potential impact of risks, as well as recommending risk mitigation strategies
CA009	Digital Forensics	This Competency Area describes a learner's capabilities related to the recovery and investigation of material found in digital devices. It includes the techniques for analyzing digital evidence to support investigations, incident responses, or legal processes

CA010	Penetration Testing	This Competency Area describes a learner's capabilities related to testing and assessing the security of information systems by simulating real-world attacks. It includes vulnerability discovery, exploitation techniques, and reporting findings to improve the security posture
CA011	Incident Management	This Competency Area describes the learner's capabilities to identify, respond to, and manage cybersecurity incidents. It includes Knowledge of incident detection and response protocols, tools for analyzing incidents, and strategies to contain, mitigate, and recover from cyber threats
CA012	Security Program Management	This Competency Area describes a learner's capabilities related to the management and execution of security programs within an organization, including resource allocation, risk management, and program performance evaluation
CA013	Vulnerability Management	This Competency Area describes a learner's capabilities related to identifying, assessing, and mitigating vulnerabilities in systems and networks. It includes using tools and techniques to evaluate security posture and recommend countermeasures
CA014	Secure Software Development	This Competency Area describes a learner's capabilities to develop and secure software by incorporating security practices throughout the software development lifecycle. It includes secure design principles, secure coding practices, application-layer security controls, code reviews, application vulnerability assessments, and integration of security into modern development pipelines (e.g., DevSecOps)
CA015	Artificial Intelligence (AI) Security	This Competency Area describes the learner's capabilities to secure AI systems, including understanding and mitigating risks specific to machine learning models, data integrity in AI applications, and the secure development of AI-driven cybersecurity tools. It covers securing AI pipelines and ensuring the reliability of AI systems used in cybersecurity operations
CA016	Hardware and Firmware Security	This Competency Area describes the learner's capabilities to secure hardware and firmware components against unauthorized access and tampering. This includes implementing security measures at the hardware level, reverse engineering, and safeguarding against physical attacks
CA017	Cybersecurity Design and Architecture	This Competency Area describes the learner's capabilities to design and architect secure information systems and networks. It includes applying secure design principles, developing resilient architectures, and implementing security controls that align with organizational goals and regulatory requirements
CA018	Industrial and IoT Security	This Competency Area describes the learner's capabilities to secure embedded systems, IoT devices, and Industrial Control Systems (ICS). It includes securing communication protocols, monitoring ICS environments, and ensuring robust protection for IoT and wireless sensor networks
CA019	Cyber Threat Intelligence	This Competency Area describes the learner's capabilities to identify, analyze, and defend against cyber threats using threat intelligence tools and defensive strategies. It includes network defense, understanding cyber threat landscapes, and utilizing analytical tools to monitor, assess, and mitigate security risks in real-time
CA020	Cybersecurity Training and Awareness	This Competency Area describes the learner's capabilities to design, develop, and deliver effective cybersecurity training and awareness programs. It encompasses creating engaging and accessible content, selecting suitable instructional methods, crafting impactful materials to enhance awareness, and evaluating the effectiveness of training efforts to ensure learners' progress and understanding

CA021	Cybersecurity Regulations and Compliance	This Competency Area describes the learner's capabilities to interpret, apply, and ensure compliance with cybersecurity laws, regulations, and ethical standards within an organization. It includes understanding relevant legal frameworks, managing regulatory compliance, advising on legal issues in cybersecurity, and ensuring adherence to cybersecurity policies and standards
CA022	Data Protection	This Competency Area describes the learner's capabilities to manage data protection risks, ensure compliance with data protection laws, and safeguard organizational data, including Personally Identifiable Information (PII). It includes implementing data protection-specific controls, managing data classification and access, and fostering organizational awareness of data protection responsibilities
CA023	Business Continuity and Disaster Recovery	This Competency Area describes the learner's capabilities to plan, implement, and manage cybersecurity-focused Business Continuity and Disaster Recovery (Cyber BCM/DR) strategies. It includes developing resilient systems, creating cyber-specific recovery protocols, and ensuring the continuity of essential cybersecurity functions during and after disruptions or cyber incidents
CA024	Cybersecurity Testing	This Competency Area describes the learner's capabilities to systematically evaluate the security posture of systems, networks, and applications through structured testing methodologies. It emphasizes testing the integration and security of systems, including functional testing, compliance-driven testing, fuzzing, and exploratory testing

TABLE 12: COMPETENCY AREAS DESCRIPTIONS

3.4 Appendix D: Updates in this version of SCyWF

This version (v1.5) of the Saudi Cybersecurity Workforce Framework (SCyWF) introduces several important updates aimed at improving alignment with international standards, and usability for stakeholders. The key changes include:

1- **Introduction of Supplementary Career Progression document:** This update introduces the *Saudi Cybersecurity Workforce Framework – Career Progression (SCyWF-CP)*, a supplemental document that defines structured pathways for professional growth within the cybersecurity field. It outlines clear progression routes, required qualifications, and recommended experience levels for each job role, helping individuals and organizations plan and navigate cybersecurity careers more effectively.

2- **Removal of Abilities**: Abilities have been removed and replaced with skills. This change aligns with the approach used in global best practices.

3- **Introduction of Competency Areas**: Competency Areas have been introduced in this version (Appendix C) to address critical cybersecurity needs and to provide a foundational framework for stakeholders.

4- **Revision of TKS Statements**: All Tasks, Knowledge, and Skills (TKS) statements have been reviewed, rephrased, and, where necessary, removed or split into more specific and distinct components to align with the most recent updates to global best practices.

5- **Refinement of TKS mapping to Job Role Details**: Each job role has been updated by revising the related TKS, including additions and removals, to better reflect the requirements of the role and align with evolving cybersecurity demands.

6- **Classification of Skills Statements**: Skills statements have been categorized as technical or non-technical, providing a clearer understanding of the nature of each skill and aiding in the development of role-specific training and assessment programs.

7- **Updates to the job role descriptions**: Minor updates were done to the names and/or descriptions of the Data Protection Officer, Cybersecurity Instructor and Cybersecurity Instructional Curriculum Developer job roles.

These updates collectively enhance the SCyWF's relevance and usability, ensuring it remains a comprehensive and effective tool for building and managing the national cybersecurity workforce.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority