الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

KINGDOM OF SAUDI ARABIA

THE SAUDI CYBERSECURITY WORKFORCE FRAMEWORK (SCyWF)

SCyWF - 1 : 2020

Sharing Indicator: White, Document Classification: Unclassified

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

Traffic Light Protocol (TLP):

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

Red – Personal, Confidential and for Intended Recipient Only

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

Amber – Restricted Sharing

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

Green – Sharing within the Same Community

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

White – No Restriction

Table of Contents

List of Tables

List of Figures

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 the national cybersecurity workforce, participating in the development of education and training programs, preparing professional standards and frameworks and developing and running tests to assess cybersecurity professionals. The NCA has developed the Saudi Cybersecurity Workforce Framework (SCyWF) as a foundational step towards carrying out that mandate.

1.1 An 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, skills and abilities (TKSAs).

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, skills and abilities (KSAs) 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.

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 is developed in alignment with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework from the U.S. National Institute of Standards and Technology (NIST)[1]. The SCyWF uses the methodology of the NICE framework. It organizes cybersecurity work in a hierarchical structure composed of categories, specialty areas and job roles

1 NIST Special Publication 800-181, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework", 2017. https://doi.org/10.6028/NIST.SP.800-181

in line with the NICE approach. However, the SCyWF categories, specialty areas and job roles are different from those in the NICE framework and have been developed to address the cybersecurity workforce demand in Saudi Arabia. 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 KSAs required to perform those tasks. All SCyWF job roles are listed in Appendix A.

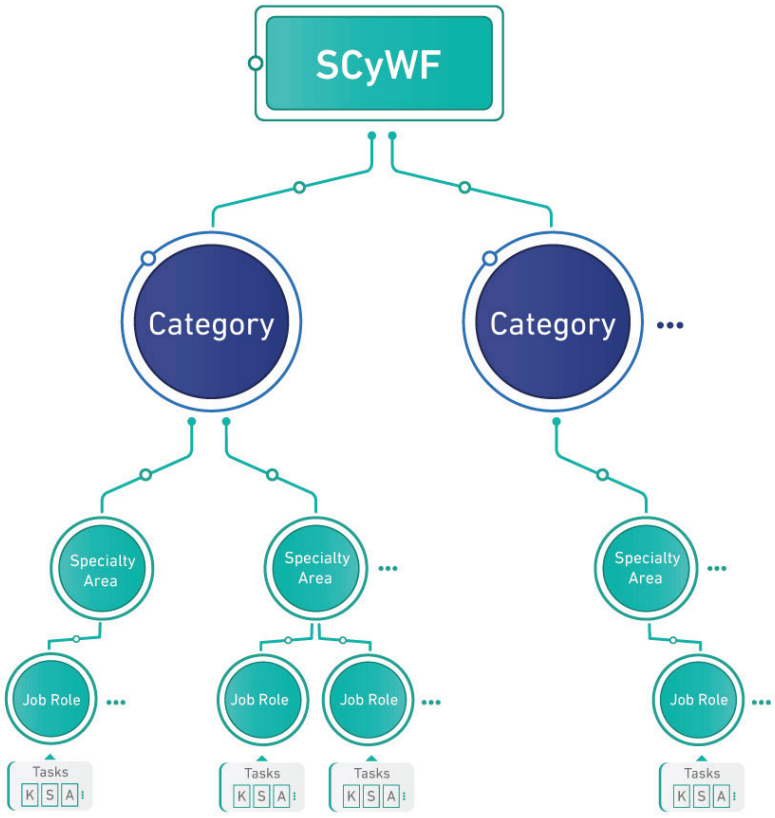
A **specialty area** is a group of job roles that serve a cybersecurity function and share common TKSAs.

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 KSAs. 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 Taxonomy

The SCyWF has five cybersecurity work categories, twelve specialty areas and forty job roles. These are defined in a brief description summarizing the work performed in that specific category, specialty area or job role. Each job role is associated with a set of tasks to be performed within that job role and a list of KSAs required to perform those tasks.

A **Knowledge** is defined as the set of data, facts, information, theories, concepts, issues and trends related to a particular subject.

A **Skill** is defined as the capability to apply knowledge and to use tools and methods to carry out a task.

An **Ability** is defined as the behavior-based competence that is necessary to perform the work in a particular field.

A **Task** is defined as a set of activities that need to be completed as part of a particular job role.

The TKSAs for the job roles in the SCyWF have been developed using the long list of TKSAs in the NICE framework with the necessary changes being made to address the cybersecurity workforce demand in Saudi Arabia. Appendix B gives a complete list of the SCyWF's TKSAs.

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

Figure 2: The SCyWF Taxonomy

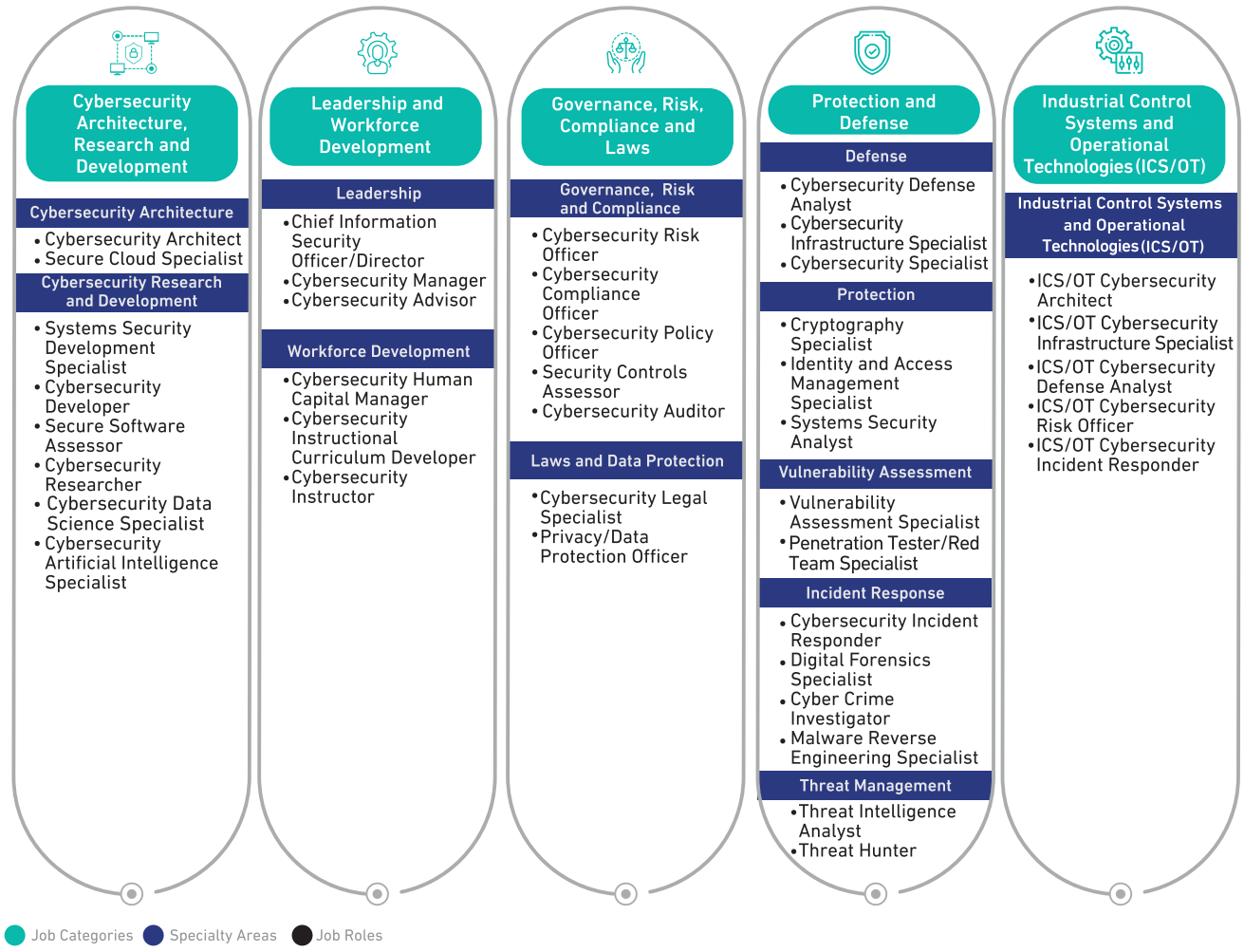


Table 1 describes the SCyWF categories. Each category has a unique identifier (ID) composed of the first characters of the category's name (e.g. PD for Protection and Defense). This forms part of the full job role ID for the job roles under each category as described in Appendix A.

Table 1: SCyWF Categories

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 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.

Table 2: SCyWF Specialty Areas

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.

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

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

Table 3: Cybersecurity Architecture, Research and Development (CARD) Job Roles

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.

2.2 Leadership and Workforce Development (LWD) Job Roles

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

Table 4: Leadership and Workforce Development (LWD) Job Roles

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 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.

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

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

Table 5: Governance, Risk, Compliance and Laws (GRCL) Job Roles

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		**Privacy/Data Protection Officer**	**GRCL-LDP-002**	Studies personal data schemes and the applicable privacy laws and regulations. Analyzes privacy risks. Develops and oversees the implementation of an organization's privacy and data protection compliance program and internal policies. Supports organizational response to a privacy or data protection incident.

2.4 Protection and Defense (PD) Job Roles

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

Table 6: Protection and Defense (PD) Job Roles

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.
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.

No	Specialty Area	Job Role	Job Role ID	Description
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.

2.5 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.

Table 7: Industrial Control Systems and Operational Technologies (ICS/OT) Job Roles

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.

For the KSAs 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.
Tasks	T0036, T0043, T0507, T0508, T0509, T0510, T0511, T0512, T0514, T0515, T0516, T0517, T0518, T0519, T0520, T0523, T0524, T0525, T0526, T0527, T0528, T0529, T0530, T0531, T2511, T4502
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0016, K0017, K0020, K0021, K0022, K0023, K0025, K0026, K0027, K0028, K0034, K0035, K0040, K0041, K0042, K0044, K0045, K0046, K0048, K0053, K0057, K0058, K0061, K0062, K0074, K0093, K0101, K0109, K0111, K0112, K0116, K0120, K0124, K0125, K0126, K0129, K0131, K0133, K0146, K0148, K0149, K0151, K0503, K0504, K0505, K0506, K0507, K0508, K0509, K0510, K0511, K0512, K0513, K0514, K0515, K1015, K1036, K1505, K4000, K5503
Skills	S0003, S0007, S0008, S0010, S0016, S0021, S0027, S0038, S0039, S0061, S0064, S0065, S0501, S0502, S0503, S0504, S0505, S0506, S1008
Abilities	A0003, A0009, A0010, A0011, A0013, A0035, A0043, A0044, A0500, A0502, A0503, A0504, A2504

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.
Tasks	T0134, T0500, T0501, T0502, T0503, T0504, T0505, T0506, T0521, T0522
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0019, K0025, K0044, K0045, K0046, K0048, K0071, K0074, K0084, K0085, K0106, K0121, K0132, K0500, K0502, K1011, K2001
Skills	S0012, S0019, S0060, S0500
Abilities	A0009, A0034, A0501

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.
Tasks	T0004, T0006, T0007, T0012, T0013, T0022, T0039, T0043, T0096, T0105, T0506, T0508, T1004, T1007, T1008, T1015, T1016, T1017, T1018, T1021, T1022, T1026, T1027, T1031, T1033, T1034, T1038, T1042, T1044, T1047, T1048, T1049, T1053, T1056, T1063, T1079, T1084, T1087, T1088, T1089, T1090, T2512
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0020, K0022, K0023, K0026, K0027, K0035, K0038, K0040, K0041, K0042, K0045, K0046, K0048, K0049, K0050, K0056, K0057, K0058, K0062, K0073, K0074, K0076, K0092, K0093, K0100, K0101, K0111, K0113, K0124, K0125, K0126, K0130, K0133, K0136, K0140, K0146, K0148, K0149, K0151, K1004, K1006, K1007, K1008, K1009, K1011, K1014, K1015, K1017, K1018, K1036, K1504, K5503
Skills	S0001, S0007, S0008, S0012, S0028, S0061, S1004, S1007, S1008, S1027, S2512
Abilities	A0001, A0002, A0003, A0005, A0009, A0010, A0011, A0012, A0013, A0019, A0032, A0035, A0044, A0500, A1005, A2503, A2507, A2511, A2513, A2524

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.
Tasks	T0035, T0039, T0040, T0091, T0114, T1002, T1003, T1005, T1006, T1009, T1010, T1011, T1013, T1014, T1023, T1030, T1031, T1035, T1036, T1040, T1043, T1054, T1055, T1071, T1075, T1078, T1080, T1085, T1092, T5060
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0022, K0030, K0035, K0039, K0045, K0050, K0051, K0052, K0074, K0076, K0083, K0093, K0100, K0110, K0112, K0124, K0125, K0126, K0127, K0146, K0147, K1000, K1004, K1008, K1011, K1012, K1013, K1014, K1015, K1017, K1018, K1019, K1021, K1022, K1023, K1039, K1040, K5503
Skills	S0001, S0007, S0017, S0036, S0038, S0047, S0048, S0061, S1001, S1002, S1003, S1007, S1008, S1026, S1031, S1034
Abilities	A0035, A0044, A1000, A1001, A1004

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.
Tasks	T0039, T0040, T0077, T1005, T1006, T1009, T1012, T1013, T1024, T1030, T1031, T1035, T1040, T1041, T1043, T1046, T1054, T1055, T1076, T1077, T1078, T1081, T1082, T1086, T1092, T1104
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0022, K0030, K0035, K0039, K0045, K0050, K0051, K0052, K0074, K0076, K0083, K0093, K0100, K0110, K0112, K0124, K0125, K0126, K0127, K0146, K0153, K0168, K1000, K1004, K1008, K1011, K1012, K1013, K1014, K1015, K1017, K1018, K1019, K1021, K1022, K1023, K1024, K1037, K5503
Skills	S0001, S0007, S0036, S0038, S0047, S0048, S0061, S1007, S1008, S1010
Abilities	A0035, A0044, A1001

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.
Tasks	T0052, T0089, T0090, T1019, T1045, T1050, T1051, T1057, T1058, T1073, T1074, T1091, T1093
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0017, K0044, K0056, K0073, K0074, K0092, K0093, K0094, K0095, K0096, K0097, K0098, K0100, K0112, K0114, K0128, K0135, K0143, K0153, K0159, K1026, K1029, K1030, K1031, K1032, K1033, K1034, K1035, K1038
Skills	S0003, S0018, S0045, S1002, S1024, S1025, S1028
Abilities	A0001, A0004, A0005, A0044

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.
Tasks	T0080, T0083, T0084, T1000, T1001, T1020, T1034, T1037, T1039, T1059, T1060, T1061, T1062, T1064, T1065, T1066, T1067, T1068, T1069, T1070, T1071, T1072, T1083, T1103
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0015, K0018, K0039, K0040, K0042, K0045, K0049, K0051, K0059, K0074, K0076, K0105, K0108, K0156, K1001, K1002, K1003, K1005, K1010, K1016, K1020, K1021, K1025, K1027, K1028, K1036
Skills	S0017, S0029, S0030, S0031, S0032, S1000, S1002, S1005, S1006, S1009, S1011, S1012, S1013, S1014, S1015, S1016, S1017, S1018, S1019, S1020, S1021, S1022, S1023, S1027, S1029, S1030, S1034
Abilities	A0008, A0014, A1002, A1003, A2509

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.
Tasks	T0134, T1071, T1072, T1094, T1095, T1096, T1097, T1098, T1099, T1100, T1101, T1103
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0074, K0119, K1039, K1040, K1041, K1042, K1043, K1044, K1046, K1047
Skills	S1031, S1032, S1033, S1034, S1035, S1036, S1037
Abilities	A1006, A1007, A1008

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.
Tasks	T0002, T0008, T0059, T0077, T0081, T0085, T0093, T0095, T0105, T0126, T0127, T0128, T0137, T1500, T1501, T1503, T1511, T1515, T1525, T1526, T1528, T1529, T1531, T1534, T1535, T1536, T1541, T2000, T2003, T2007, T2008, T2009
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0021, K0052, K0054, K0064, K0073, K0074, K0080, K0082, K0092, K0093, K0135, K0143, K0153, K0168, K2021, K5503
Skills	S0010, S0058, S0059, S1500, S1501, S1502, S1503, S3001
Abilities	A0006, A0015, A0017, A0021, A0024, A0025, A0029, A0030, A0031, A0032, A1500, A1501

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.
Tasks	T0001, T0002, T0008, T0016, T0020, T0023, T0048, T0053, T0059, T0061, T0063, T0115, T0137, T1500, T1502, T1503, T1504, T1505, T1506, T1507, T1508, T1509, T1510, T1511, T1512, T1514, T1515, T1516, T1517, T1518, T1519, T1520, T1521, T1522, T1523, T1524, T1525, T1526, T1527, T1528, T1529, T1530, T1531, T1532, T1533, T1534, T1542, T2000, T2001, T2007, T2008, T2009, T2510, T2514
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0016, K0019, K0021, K0024, K0029, K0031, K0033, K0034, K0036, K0037, K0043, K0044, K0046, K0052, K0056, K0061, K0064, K0073, K0074, K0082, K0090, K0091, K0092, K0093, K0100, K0101, K0110, K0118, K0124, K0125, K0126, K0128, K0133, K0148, K0150, K0153, K0168, K0169, K1500, K1501, K1502, K1503, K1504, K1505, K1506, K1507, K1509, K1511, K2501, K5503, S3001
Skills	S0010, S1500, S1501, S3001
Abilities	A0036, A0044, A1502

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.
Tasks	T0001, T0002, T0093, T1501, T1503, T1511, T1515, T1525, T1528, T1529, T1537, T1538, T1539, T1540, T2001, T2003, T2052
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0016, K0019, K0021, K0029, K0031, K0033, K0034, K0036, K0037, K0044, K0046, K0052, K0056, K0061, K0064, K0073, K0074, K0082, K0090, K0091, K0092, K0093, K0100, K0101, K0110, K0118, K0124, K0128, K0133, K0148, K0150, K0153, K0169, K1500, K1501, K1502, K1503, K1504, K1505, K1506, K1507, K1509, K1510, K1511, K5503
Skills	S0058, S1500, S1501, S1502, S1503
Abilities	A0006, A0015, A0017, A0021, A0024, A0025, A0029, A0030, A0031, A0032, A0043, A1500, A1501

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.
Tasks	T0002, T0008, T0017, T0020, T0045, T0046, T0078, T0081, T0082, T0085, T0086, T0088, T0092, T0093, T0095, T0099, T0103, T0104, T0108, T0109, T0110, T1500, T1503, T2006, T2022, T2023, T2025, T2026, T2027, T2028, T2030, T2031, T2032, T2033, T2034, T2035, T2037, T2038, T2039, T2040, T2047, T2052, T2053
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0061, K0074, K0079, K0080, K0091, K0092, K0118, K0141, K0142, K0150, K1501, K2002, K2011, K2013, K2014, K2019
Skills	S2008, S2508
Abilities	A0006, A2006, A2008, A2009, A2506, A2510

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 and education programs, courses, contents, methods and techniques based on instructional needs.
Tasks	T0052, T1528, T2011, T2012, T2021, T2022, T2024, T2028, T2029, T2036, T2040, T2041, T2044, T2045, T2050, T2052, T2054
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0044, K0074, K0079, K0080, K0133, K2000, K2002, K2003, K2004, K2006, K2007, K2009, K2012, K2014, K2015, K2016, K2018, K2021
Skills	S0055, S2003, S2004, S2005, S2007, S2009
Abilities	A0002, A0003, A0004, A0005, A0015, A0016, A0019, A0024, A0025, A0027, A0028, A0031, A0032, A2004, A2005, A2007, A2010, A2011, A2013, A2014, A2015

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.
Tasks	T0083, T0084, T0087, T2002, T2004, T2005, T2010, T2011, T2012, T2013, T2014, T2015, T2016, T2017, T2018, T2019, T2020, T2022, T2028, T2029, T2042, T2043, T2045, T2046, T2048, T2049, T2051, T2052, T2054
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0044, K0071, K0074, K0079, K0080, K0133, K2000, K2001, K2002, K2003, K2004, K2006, K2007, K2008, K2009, K2010, K2012, K2014, K2015, K2016, K2018, K2019, K2020, K2021
Skills	S0001, S0004, S0015, S0017, S0019, S0020, S0021, S0026, S0027, S0034, S0035, S0041, S0058, S1502, S2000, S2001, S2002, S2003, S2005, S2006, S2010, S2501, S2515, S2534, S2539, S4504, S4505, S4508, S5012, S5017
Abilities	A0002, A0003, A0004, A0005, A0014, A0015, A0016, A0019, A0024, A0025, A0027, A0028, A0031, A0032, A2001, A2002, A2003, A2004, A2005, A2007, A2011, A2013, A2014, A2015, A2502, A2503, A2504, A2505, A2506

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.
Tasks	T0001, T0006, T0012, T0013, T0014, T0020, T0039, T0043, T0053, T0105, T0128, T0129, T0130, T0131, T0132, T0133, T2500, T2513
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0029, K0037, K0073, K0074 ,K0080, K0081, K0082, K0083, K0089, K0092, K0107, K0127, K0160, K0162, K0166, K0167, K0508, K5503
Skills	S0044, S0057, S0062
Abilities	A0033, A0037, A0038, A0039, A0040, A0041, A0042, A0045, A2501

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.
Tasks	T0003, T0019, T0022, T0023, T0063, T0111, T2500, T2501, T2502, T2504, T2506, T2509, T2514, T2518, T2519, T3052
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0074, K0091, K0165, K0118, K2508, K5503
Skills	S0058, S0061
Abilities	A0006, A0007, A0023, A0024, A0026, A2005

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.
Tasks	T0011, T0017, T0045, T0046, T0078, T0082, T0085, T0086, T0088, T0092, T0093, T0095, T0099, T0103, T0104, T0108, T0109, T0110
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0052, K0074, K0079, K0091, K0118, K0122, K0141, K0142, K0150, K0168, K2019, K2503, K5503
Skills	S2513, S2530
Abilities	A0006, A2500, A2510

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.
Tasks	T0036, T0037, T0039, T0043, T0050, T0053, T0059, T0061, T0074, T0079, T2503, T2505, T2507, T2508, T2509, T2510, T2511, T2512, T2514, T2516
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0013, K0016, K0017, K0019, K0020, K0021, K0022, K0028, K0029, K0031, K0035, K0037, K0038, K0042, K0044, K0052, K0055, K0060, K0061, K0073, K0074, K0079, K0091, K0092, K0093, K0100, K0110, K0113, K0118, K0124, K0125, K0126, K0128, K0133, K0146, K0153, K0168, K0169, K1004, K1017, K1511, K2500, K2501, K2502, K5503
Skills	S0001, S0004, S0010, S0019, S0023, S0034, S0036, S0037, S0038, S0040, S0044, S0045, S0046, S0047, S0048, S0050, S0051, S0055, S0061, S0063, S0064, S1008, S2500, S2501, S2502, S2503, S2504, S2505, S2506, S2507, S2508, S2509, S2510, S2511, S2512, S2513, S2514, S2515, S2516, S2517, S2521, S2523, S2524, S2525, S2527, S2528, S2529, S2530, S2531, S2532, S2533, S2534, S2535, S2536, S2539, S2540, S2541, S2542, S2543
Abilities	A0001, A0002, A0003, A0004, A0005, A0008, A0012, A0015, A0016, A0017, A0018, A0019, A0021, A0025, A0027, A0028, A0029, A0030, A0031, A0032, A0035, A0044, A2502, A2503, A2504, A2505, A2506, A2507, A2508, A2509, A2511, A2512, A2513, A2514, A2515, A2516, A2517, A2518, A2519, A2520, A2521, A2523, A2524, A2525, A2526, A2527

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.
Tasks	T0024, T0038, T0039, T0041, T0048, T0059, T0060, T0109, T2502, T2508, T2509, T2510, T2512, T2515, T2520
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0013, K0021, K0022, K0028, K0035, K0038, K0056, K0074, K0079, K0109, K0133, K0144, K1004, K2500, K2501, K2504, K2505, K2506, K2507, K5503
Skills	S0004, S0010, S0023, S0028, S0036, S0040, S0046, S0047, S0048, S0051, S0055, S1008, S2500, S2501, S2502, S2503, S2504, S2505, S2506, S2507, S2508, S2509, S2510, S2511, S2512, S2513, S2514, S2515, S2516, S2519, S2521, S2523, S2524, S2525, S2526, S2527, S2528, S2529, S2532, S2533, S2534, S2536, S2539, S2540, S2541, S2545, S2546
Abilities	A0001, A0002, A0004, A0005, A0015, A0016, A0017, A0019, A0021, A0022, A0025, A0027, A0028, A0029, A0030, A0031, A0032, A0035, A0044, A2502, A2503, A2504, A2505, A2506, A2507, A2508, A2509, A2510, A2511, A2512, A2513, A2514, A2515, A2516, A2517, A2519, A2520, A2521, A2523, A2524, A2525, A2526, A2527, A2528, A2529, A2530

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.
Tasks	T0019, T0038, T1501, T3000, T3001, T3002, T3003, T3004, T3005, T3006, T3007, T3008, T3009, T3010, T3052
Knowledge	K0002, K0003, K0004, K0005, K0006, K0044, K0065, K0074, K0084, K0125, K0126, K0128, K3000, K3001, K3002, K3004, K5503
Skills	S0058
Abilities	A3000

Job Role Details	
Job Role Name	Privacy/Data Protection Officer
Job Role ID	GRCL-LDP-002
Category	Governance, Risk, Compliance and Laws
Specialty Area	Laws and Data Protection
Job Role Description	Studies personal data schemes and the applicable privacy laws and regulations. Analyzes privacy risks. Develops and oversees the implementation of an organization's privacy and data protection compliance program and internal policies. Supports organizational response to a privacy or data protection incident.
Tasks	T0007, T0126, T0127, T3011, T3012, T3013, T3014, T3015, T3016, T3017, T3018, T3019, T3020, T3021, T3022, T3023, T3024, T3025, T3026, T3027, T3028, T3029, T3030, T3031, T3032, T3033, T3034, T3035, T3036, T3037, T3038, T3039, T3040, T3041, T3042, T3043, T3044, T3045, T3046, T3047, T3048, T3049, T3050, T3051, T3052, T3053
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0029, K0030, K0035, K0050, K0074, K3004, K3005, K3006, K5503
Skills	S0058, S0061, S0064, S3000, S3002
Abilities	A0006, A0007, A0023, A0024, A0026, A0027, A0035, A2005, A2526, A2527, A3001, A3002

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.
Tasks	T0009, T0015, T0025, T0028, T0029, T0037, T0040, T0044, T0054, T0055, T0056, T0064, T0065, T0066, T0067, T0068, T0069, T0070, T0071, T0072, T0073, T0075, T0076, T0097, T0098, T0100, T0101, T0102, T0107, T0111, T3500, T3501, T3503, T3504
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0014, K0016, K0017, K0020, K0024, K0031, K0033, K0035, K0036, K0038, K0042, K0043, K0044, K0045, K0046, K0049, K0052, K0053, K0054, K0058, K0060, K0063, K0064, K0065, K0067, K0068, K0069, K0070, K0072, K0074, K0076, K0077, K0078, K0084, K0086, K0087, K0088, K0090, K0091, K0099, K0100, K0101, K0102, K0103, K0104, K0113, K0117, K0118, K0124, K0125, K0126, K0134, K0136, K0137, K0138, K0139, K0145, K0146, K0147, K0148, K0152, K0153, K0168 , K5503
Skills	S0006, S0009, S0010, S0012, S0015, S0023, S0033, S0040, S0041, S0042, S0046, S0048, S0057, S0061, S0063, S2002, S2514, S2534, S2543, S3500, S3501, S3502, S5524
Abilities	A0003, A0014, A0035, A0036, A3500, A3501

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.
Tasks	T0005, T0038, T0057, T0114, T3502, T3505, T3506, T3507, T3508, T3509, T3510, T3511, T3512, T4023
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0019, K0024, K0033, K0035, K0043, K0046, K0055, K0063, K0064, K0074, K0084, K0100, K0104, K0119, K0147, K0148, K1022, K3500, K3501, K3502, K3503, K3504, K5012
Skills	S0005, S0008, S0014, S0016, S0021, S0022, S0024, S0035, S0038, S0061, S0065, S1007, S2507, S3500
Abilities	A0001, A0035, A0044

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.
Tasks	T0005, T0009, T0026, T0028, T0102, T0113, T0136, T3500, T3501, T3503, T3504
Knowledge	K0001, K0004, K0005, K0006, K0007, K0009, K0013, K0014, K0017, K0019, K0020, K0024, K0031, K0033, K0035, K0038, K0043, K0045, K0051, K0053, K0055, K0063, K0068, K0074, K0084, K0104, K0115, K0119, K0152, K3504, K3505
Skills	S0002, S0009, S0010, S0012, S0019, S0021, S0022, S0023, S0027, S0028, S0035, S0042, S0062, S3501, S3502
Abilities	A0001, A0003, A0036, A3501

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.
Tasks	T0010, T0016, T0090, T0091, T0096, T0114, T4000, T4008, T4012, T4021, T4022
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0010, K0014, K0015, K0016, K0017, K0018, K0024, K0028, K0029, K0030, K0035, K0038, K0039, K0040, K0042, K0044, K0046, K0050, K0051, K0053, K0074, K0102, K0112, K0113, K0116, K0131, K0140, K0155, K0157, K0158, K0163, K1000, K1011, K4000, K4009, K4010, K4011, K4013, K4014, K4015, K4017
Skills	S0004, S0016, S0038, S0039, S0061, S1002, S1028, S4001, S4002, S4003
Abilities	A0035, A1001, A4000, A4001, A5000

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.
Tasks	T0100, T0114, T1049, T3508, T4016, T4017, T4018, T4019, T4020, T4024, T4025, T4026, T4027, T4028, T4029
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0024, K0028, K0035, K0042, K0049, K0059, K0074, K0079, K0085, K0106, K0107, K0108, K0112, K0124, K0125, K0126, K0132, K0133, K0144, K0151, K0156, K1019, K3505, K4000, K4001, K4002, K4004, K4012, K4016, K4018, K5503
Skills	S0005, S0061, S1007, S4000
Abilities	A0035, A4002, A4003

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.
Tasks	T0004, T0005, T0015, T0036, T0040, T0043, T0050, T0074, T0079, T0097, T0098, T0100, T0102, T0107, T0111, T1026, T4000, T4001, T4002, T4003, T4004, T4005, T4006, T4007, T4009, T4010, T4011, T4012, T4013, T4014, T4015, T4023
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0017, K0020, K0026, K0027, K0031, K0035, K0038, K0040, K0042, K0045, K0046, K0048, K0054, K0058, K0062, K0074, K0100, K0101, K0111, K0113, K0120, K0124, K0125, K0126, K0127, K0128, K0129, K0130, K0133, K0134, K0136, K0146, K0149, K0152, K1015, K4006, K4007, K4008, K4009 , K5503
Skills	S0008, S0010, S0012, S0017, S0040, S0042, S0061, S1007, S2511
Abilities	A0003, A0035

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.
Tasks	T0003, T0009, T0024, T0041, T0113, T0133, T2502, T4500, T4501, T4502, T4507, T4518
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0017, K0019, K0024, K0035, K0042, K0046, K0051, K0052, K0055, K0064, K0074, K0076, K0087, K0088, K0090, K0099, K0100, K0113, K0115, K0119, K0133, K0138, K0140, K0148, K0153, K0154, K0163, K0168, K4500, K4501, K5503
Skills	S0001, S0009, S0026, S0037, S0044, S0061, S1023, S2506, S2515, S2527, S2545, S4500, S4502, S4504, S4505, S4507, S4508
Abilities	A0001, A0033, A0035

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.
Tasks	T4500, T4503, T4504, T4505, T4506, T4507, T4508, T4509, T4510, T4511, T4512, T4513, T4514, T4515, T4516, T4517, T5545
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0038, K0054, K0057, K0074, K0075, K0080, K0134, K0140, K0153, K0158, K0161, K0163, K1013, K4502, K4503, K4504, K4505, K4506, K4507, K4508, K4509, K4510, K5503
Skills	S0011, S0027, S2514, S2515, S4501, S4503, S4504, S4505, S4506, S4508, S4509, S4510, S4511, S5002, S5015, S5016, S5502, S5509, S5510
Abilities	A0001, A0003, A0008, A4501, A4502, A4503, A4504, A4505

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.
Tasks	T0009, T0026, T0027, T0028, T0031, T0034, T0044, T0047, T0051, T0058, T0062, T0087, T0101, T0106, T5003, T5025, T5031, T5040, T5054
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0019, K0021, K0024, K0025, K0032, K0033, K0036, K0043, K0047, K0052, K0064, K0074, K0084, K0087, K0088, K0090, K0099, K0100, K0117, K0121, K0123, K0133, K0148, K0168, K0169, K5503
Skills	S0002, S0004, S0006, S0009, S0010, S0011, S0012, S0013, S0014, S0015, S0018, S0019, S0020, S0022, S0023, S0024, S0025, S0026, S0027, S0033, S0035, S0041, S0044, S0046, S0048, S0051, S0052, S0054, S0060, S1022, S1023, S1033, S1503, S2000, S2002, S2506, S2523, S2526, S2532, S2533, S2535, S2538, S3500, S3501, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5007, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5017, S5501, S5502, S5503, S5504, S5505, S5506, S5507, S5508, S5509, S5510, S5511, S5512, S5513, S5514
Abilities	A0034, A0036

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.
Tasks	T0010, T0030, T0032, T0033, T0034, T0049, T5000, T5002, T5004, T5006, T5007, T5010, T5013, T5014, T5015, T5016, T5017, T5019, T5020, T5022, T5023, T5024, T5025, T5026, T5027, T5028, T5029, T5030, T5031, T5036, T5037, T5038, T5039, T5040, T5041, T5044, T5050, T5051, T5059, T5062, T5534
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0016, K0019, K0033, K0045, K0052, K0066, K0074, K0075, K0090, K0091, K0100, K0119, K0138, K0168, K1503, K5000, K5002, K5003, K5005, K5006, K5007, K5008, K5009, K5010, K5011, K5014, K5016, K5017, K5018, K5019, K5020, K5021, K5022, K5023, K5024, K5028, K5029, K5030, K5031, K5503
Skills	S0011, S0013, S0019, S0020, S0029, S0030, S0041, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5007, S5008, S5009, S5010, S5011, S5012, S5013, S5014
Abilities	A5000, A5001

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.
Tasks	T0018, T0021, T5001, T5005, T5008, T5009, T5010, T5011, T5012, T5018, T5021, T5023, T5033, T5034, T5035, T5040, T5042, T5043, T5046, T5047, T5048, T5049, T5054, T5059, T5061
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0052, K0065, K0067, K0074, K0091, K0168, K5001, K5003, K5006, K5007, K5008, K5013, K5016, K5025, K5026, K5032 , K5503
Skills	S0013, S0018, S1501, S5003
Abilities	A5002, A5003

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.
Tasks	T0089, T0135, T5016, T5052, T5055, T5057, T5058, T5510, T5519, T5525, T5534, T5535, T5536, T5537, T5538, T5539, T5540, T5541, T5542, T5544, T5545
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0039, K0043, K0047, K0067, K0074, K0094, K0095, K0096, K0097, K0098, K0099, K0100, K0101, K0102, K0103, K0104, K0105, K5017, K5018, K5019, K5020, K5021, K5022, K5023, K5024
Skills	S0001, S0029, S0030, S0031, S0032, S0048, S0049, S0052, S0053, S1503, S5007, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5015, S5016, S5017
Abilities	A0001, A0025, A0046, A3500, A5000, A5004, A5502

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.
Tasks	T5056, T5502, T5503, T5504, T5505, T5506, T5507, T5508, T5510, T5515, T5517, T5519, T5524, T5525, T5526, T5527, T5528, T5529, T5530, T5531, T5535, T5536, T5537, T5538, T5539, T5540, T5541, T5542, T5543, T5544
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0027, K0043, K0066, K0074, K0099, K0155, K0157, K0159, K0161, K0163, K0165, K5500, K5501, K5502, K5503, K5504, K5506, K5507, K5508, K5509, K5511, K5512, K5513, K5514, K5515, K5516, K5517, K5518, K5519, K5520, K5523, K5524, K5527, K5528, K5530, K5532, K5533
Skills	S0049, S0051, S0055, S2536, S5500, S5501, S5502, S5504, S5507, S5509, S5510, S5516, S5517, S5518, S5520, S5521
Abilities	A0002, A0014, A0016, A0018, A0019, A0020, A0022, A0025, A2513, A2514, A2516, A2523, A2525, A5500, A5501, A5502

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.
Tasks	T0009, T0017, T0018, T0021, T0026, T0027, T0028, T0030, T0032, T0033, T0034, T0035, T0049, T0054, T0055, T0056, T0057, T0060, T0069, T0080, T0089, T0109, T0135, T0136, T1528, T5010, T5016, T5023, T5500, T5501, T5507, T5509, T5510, T5511, T5512, T5513, T5514, T5515, T5517, T5518, T5519, T5520, T5521, T5523, T5524, T5525, T5532, T5533, T5534, T5536,T5544
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0014, K0016, K0028, K0031, K0032, K0033, K0034, K0035, K0043, K0044, K0047, K0050, K0064, K0065, K0067, K0068, K0074, K0086, K0088, K0107, K0116, K0154, K5503, K5519, K5521, K5522, K5525, K5526, K5530, K5534
Skills	S0001, S0029, S0030, S0031, S0032, S0050, S0051, S0052, S0059, S0062, S2525, S2526, S2527, S2532, S4508, S5007, S5008, S5009, S5010, S5011, S5503, S5505, S5506, S5511, S5512, S5513, S5514, S5515, S5519, S5522, S5523, S5524
Abilities	A0001, A0025, A0033, A0046, A3500, A5000, A5502

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.
Tasks	T0036, T0043, T0507, T0508, T0509, T0510, T0511, T0512, T0514, T0515, T0516, T0517, T0518, T0519, T0520, T2511, T4502, T6000, T6001, T6002, T6003, T6004, T6009, T6010, T6011, T6012, T6013
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0016, K0017, K0020, K0021, K0022, K0023, K0025, K0026, K0027, K0028, K0034, K0035, K0040, K0041, K0042, K0044, K0045, K0046, K0048, K0053, K0057, K0058, K0062, K0074, K0093, K0101, K0109, K0111, K0112, K0116, K0120, K0124, K0125, K0126, K0129, K0131, K0133, K0146, K0148, K0149, K0151, K1015, K1036, K1505, K4000, K5503, K6000, K6001, K6002, K6003, K6004, K6005, K6006, K6007, K6008, K6009, K6010, K6011, K6012, K6013, K6014, K6015, K6016, K6017, K6018, K6019, K6020
Skills	S0003, S0007, S0008, S0010, S0016, S0021, S0027, S0038, S0039, S0061, S0064, S0065, S1008, S6000, S6001, S6002, S6003, S6004, S6005, S6006, S6007
Abilities	A0003, A0009, A0010, A0011, A0013, A0035, A0043, A0044, A0500, A2504, A6000, A6001, A6002, A6004

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.
Tasks	T0005, T0038, T0057, T0114, T3502, T3505, T3506, T3507, T3508, T3509, T3510, T3511, T3512, T4023, T6007, T6008, T6012
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0019, K0024, K0033, K0035, K0043, K0046, K0055, K0063, K0064, K0074, K0084, K0100, K0104, K0119, K0147, K0148, K1022, K3500, K3501, K3502, K3503, K3504, K5012, K6001, K6012, K6014, K6015, K6016, K6017, K6018, K6019, K6020
Skills	S0005, S0008, S0009, S0014, S0016, S0021, S0022, S0024, S0035, S0038, S0061, S0065, S1007, S2507, S3500, S6004, S6005, S6007
Abilities	A0001, A0035, A0044

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 environmenst to detect and mitigate cybersecurity threats.
Tasks	T0009, T0015, T0025, T0028, T0029, T0037, T0040, T0044, T0054, T0055, T0056, T0058, T0064, T0065, T0066, T0067, T0068, T0069, T0070, T0071, T0072, T0073, T0075, T0076, T0097, T0098, T0100, T0101, T0102, T0107, T0111, T3500, T3501, T3503, T3504
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0014, K0016, K0017, K0020, K0024, K0031, K0033, K0035, K0036, K0038, K0042, K0043, K0044, K0045, K0046, K0049, K0052, K0053, K0054, K0058, K0060, K0063, K0064, K0065, K0067, K0068, K0069, K0070, K0072, K0074, K0076, K0077, K0078, K0084, K0086, K0087, K0088, K0090, K0091, K0099, K0100, K0101, K0102, K0103, K0104, K0113, K0117, K0118, K0124, K0125, K0126, K0134, K0136, K0137, K0138, K0139, K0145, K0146, K0147, K0148, K0152, K0153, K0168, K5503, K6001, K6012, K6014, K6015, K6016, K6017, K6018, K6019, K6020
Skills	S0006, S0009, S0010, S0012, S0015, S0023, S0033, S0040, S0041, S0042, S0046, S0048, S0057, S0061, S0063, S2002, S2534, S3500, S3501, S3502, S6004, S6005, S6006, S6007
Abilities	A0003, A0014, A0035, A0036, A3500, A3501, A6004, A6005

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.
Tasks	T0001, T0006, T0012, T0013, T0014, T0020, T0034, T0039, T0043, T0053, T0105, T0109, T0128, T0129, T0130, T0131, T0132, T0133, T0136, T2500, T6014, T6016
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0029, K0037, K0073, K0074, K0080, K0081, K0082, K0083, K0089, K0092, K0107, K0127, K0160, K0162, K0166, K0167, K5503, K6001, K6003, K6005, K6012, K6014, K6015, K6016, K6017, K6018, K6019, K6020
Skills	S0044, S0057, S0062, S6006, S6007
Abilities	A0033, A0037, A0038, A0039, A0040, A0041, A0042, A0045, A2501, A6004, A6005

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.
Tasks	T0009, T0026, T0027, T0028, T0031, T0044, T0047, T0051, T0058, T0062, T0087, T0101, T0106, T5025, T5031, T6014, T6015
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0019, K0021, K0024, K0025, K0032, K0033, K0036, K0043, K0047, K0052, K0064, K0074, K0084, K0087, K0088, K0090, K0099, K0100, K0117, K0121, K0123, K0133, K0148, K0168, K5503, K6001, K6012, K6014, K6015, K6016, K6017, K6018, K6019, K6020
Skills	S0002, S0004, S0006, S0009, S0010, S0011, S0012, S0013, S0014, S0015, S0018, S0019, S0020, S0022, S0023, S0024, S0025, S0026, S0027, S0033, S0035, S0041, S0044, S0046, S0048, S0051, S0052, S0054, S0060, S1022, S1023, S1033, S1034, S1503, S2000, S2002, S2506, S2523, S2526, S2532, S2533, S2535, S2538, S3500, S3501, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5007, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5017, S5501, S5502, S5503, S5504, S5505, S5506, S5507, S5508, S5509, S5510, S5511, S5512, S5513, S5514, S6001, S6004, S6006, S6007
Abilities	A6004, A6005, A6006

3.2 Appendix B: List of Tasks, Knowledge, Skills and Abilities

As stated before, the SCyWF is developed using the methodology of the NIST's NICE framework. However, the SCyWF categories, specialty areas and job roles are different from those in the NICE framework and have been developed to address the cybersecurity workforce demand in Saudi Arabia.

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

TKSAs in the SCyWF are numbered as shown in Table 8. Tables 9, 10, 11 and 12 show the descriptions of tasks, knowledge, skills and abilities, respectively.

Table 8: SCyWF Numbering Scheme of TKSAs

Category	Specialty Area	Numbering Range for TKSA
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 9: Tasks Descriptions

Task ID	Task Description
T0001	Effectively communicate cybersecurity risks and posture to senior management.
T0002	Effectively communicate financial aspects of cybersecurity related activities to senior management.
T0003	Analyze organization's cybersecurity defense policies and configurations to evaluate compliance with regulations and organizational directives.
T0004	Apply security policies to applications that interface with one another.
T0005	Apply security policies to meet system security objectives.
T0006	Develop security risk profiles of computer systems by assessing threats to, and vulnerabilities of, those systems.
T0007	Conduct Privacy Impact Assessments (PIAs) to ensure that Personally Identifiable Information (PII) is appropriately protected.
T0008	Collaborate with stakeholders to ensure business continuity and disaster recovery programs meet organizational requirements.
T0009	Correlate incident data to identify vulnerabilities.
T0010	Perform technical decryption of seized data.
T0011	Develop cybersecurity policies and related documentation.
T0012	Develop risk mitigation strategies to effectively manage risk in accordance with organizational risk appetite.
T0013	Develop specific cybersecurity countermeasures and risk mitigation strategies.
T0014	Develop statements of preliminary or residual cybersecurity risks for system operation.
T0015	Use cybersecurity products and security control technologies to reduce identified risk to an acceptable level.
T0016	Ensure that protection and detection capabilities are aligned with the organization's cybersecurity strategy, policies and other related documentation.
T0017	Establish and maintain appropriate communication channels with stakeholders.
T0018	Build relationships between the incident response team and internal and external partners.
T0019	Evaluate cybersecurity aspects of contracts to ensure compliance with financial, contractual, legal and regulatory requirements.

Task ID	Task Description
T0020	Ensure that decisions relating to cybersecurity are based on sound risk management principles.
T0021	Identify data which will add value to investigations.
T0022	Ensure that any products implemented to manage cybersecurity risks have been effectively evaluated and authorized for use.
T0023	Recognize patterns of non-compliance with cybersecurity policies and related documentation to identify ways to improve the documentation.
T0024	Maintain a deployable cyber defense audit toolkit based on industry best practice to support cyber defense audits.
T0025	Document and escalate incidents that may cause immediate or ongoing impact.
T0026	Analyze log files from multiple sources to identify possible threats to network security.
T0027	Triage incidents to identify specific vulnerability, determine scope, urgency and potential impact, make recommendations that enable expeditious remediation.
T0028	Analyze and report cyber defense trends.
T0029	Correlate information from multiple sources to understand situation and determine the effectiveness of an observed attack.
T0030	Perform file signature analysis.
T0031	Perform initial collection of images to relevant forensic standards; inspect to evaluate possible mitigation and remediation measures.
T0032	Perform real-time forensic analysis.
T0033	Perform timeline analysis.
T0034	Perform incident response tasks to support deployable incident response teams including forensic collection, intrusion correlation, tracking, threat analysis and system remediation.
T0035	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.
T0036	Perform cybersecurity reviews and identify gaps in security architecture, to develop cybersecurity risk management plans.
T0037	Perform cybersecurity reviews and identify security gaps in security architecture to inform risk mitigation strategies.
T0038	Perform system administration on specialized cybersecurity applications and systems.

Task ID	Task Description
T0039	Perform risk analysis whenever an application or system undergoes a major change.
T0040	Analyze exercise results and system environment to plan and recommend modifications and adjustments.
T0041	Prepare cybersecurity assessment and audit reports that identify technical and procedural findings, and include recommended remediation strategies and solutions.
T0042	Provide cybersecurity related guidance to inform business continuity and data protection plans.
T0043	Provide input to the risk management framework and related documentation.
T0044	Analyze network alerts from multiple sources to determine possible causes.
T0045	Review existing and proposed policies and related documentation with stakeholders.
T0046	Provide cybersecurity expertise on organizational and sectoral policy boards.
T0047	Track and document cyber incidents from initial detection to final resolution.
T0048	Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
T0049	Capture and analyze network traffic associated with malicious activities using network monitoring tools.
T0050	Review, update and maintain cybersecurity related documentation reflecting system design.
T0051	Write and publish cyber defense techniques, guidance and post incident reports to appropriate constituencies.
T0052	Research current technology to understand cyber defense capability required by systems or networks.
T0053	Ensure cybersecurity risks are identified and managed appropriately through the organization's risk governance process.
T0054	Provide timely detection, identification and alerting of possible attacks, anomalous activities and misuse activities and distinguish them from benign activities.
T0055	Use cyber defense tools to monitor and analyze system activity continuously to identify malicious activity.
T0056	Analyze malicious activity to determine vulnerabilities exploited, exploitation methods and effects on system and information.
T0057	Identify, prioritize and coordinate the protection of critical cyber defense infrastructure and resources.

Task ID	Task Description
T0058	Employ defense-in-depth principles and practices in line with organizational policies.
T0059	Effectively manage vulnerability remediation.
T0060	Ensure an audit log of evidence of security measures is maintained.
T0061	Ensure the organization's cybersecurity requirements are considered in mergers, acquisitions, outsourcing and other operations involving third parties.
T0062	Collect intrusion artefacts and use discovered data to mitigate potential cybersecurity incidents within the organization.
T0063	Periodically review cybersecurity strategy, policies and related documents to maintain compliance with applicable legislation and regulation.
T0064	Determine Tactics, Techniques, and Procedures (TTP) for intrusion sets.
T0065	Examine network topologies to understand data flows through the network.
T0066	Recommend vulnerability corrections for the environment.
T0067	Use metadata to identify and analyze anomalies in network traffic.
T0068	Identify indications and warnings through research, analysis and correlation across multiple data sets.
T0069	Use packet analysis tools to validate intrusion detection system alerts.
T0070	Isolate and remove malware.
T0071	Use network traffic to identify a network device's applications and operating systems.
T0072	Use network traffic to reconstruct malicious activity.
T0073	Identify network mapping and operating system fingerprinting activities.
T0074	Assess the effectiveness of cybersecurity controls.
T0075	Assist in the construction of signatures for implementation on cybersecurity network tools to respond to new or observed threats within the environment.
T0076	Report suspected cyber incidents in line with the organization's cyber incident response plan.

Task ID	Task Description
T0077	Supervise and effectively assign work to staff working on cybersecurity related tasks.
T0078	Ensure that appropriate funding for cybersecurity training resources is made available.
T0079	Assess the configuration management process.
T0080	Collect metrics and trending data.
T0081	Allocate resources to cybersecurity roles.
T0082	Ensure that cybersecurity workforce management policies and processes 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 cyber policy and strategy as appropriate among the organization's management.
T0086	Review and assess cybersecurity staff effectiveness to identify skills gaps and training requirements.
T0087	Write and publish reviews to learn and promulgate lessons from cybersecurity events.
T0088	Interpret and apply applicable laws, statutes and regulatory documents to ensure they are reflected in the cybersecurity policies.
T0089	Identify and develop reverse engineering tools to enhance capabilities and detect vulnerabilities.
T0090	Develop secure data management capabilities to support a mobile workforce.
T0091	Enable applications with public keying, using existing public key infrastructure libraries and incorporating certificate management and encryption when appropriate.
T0092	Analyze an organization's cybersecurity policy.
T0093	Work with stakeholders to develop cybersecurity policies and associated documentation in alignment with the organization's cybersecurity strategy.
T0094	Define and integrate current and future mission environments to maintain consistency and reduce administrative overheads.
T0095	Align the organization's cybersecurity strategy with its business strategy.

Task ID	Task Description
T0096	Design, develop, integrate and update system security measures that provide confidentiality, integrity, availability, authentication and non-repudiation.
T0097	Analyze and report on trends in the organization's security posture.
T0098	Analyze and report on trends in the systems' security posture.
T0099	Create and publish the organization's cybersecurity policy.
T0100	Assess the adequacy of access controls against organizational policies.
T0101	Monitor external data sources to keep understanding of currency of cybersecurity threats up to date and determine which security issues may have an impact on the organization.
T0102	Assess and monitor the cybersecurity of the organization's system implementation and testing practices.
T0103	Monitor how effectively cybersecurity policies, principles and practices are implemented in the delivery of planning and management services.
T0104	Seek consensus on proposed cybersecurity policy changes from stakeholders.
T0105	Carry out a cybersecurity risk assessment.
T0106	Coordinate incident response functions.
T0107	Make cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
T0108	Provide policy guidance to cybersecurity management, staff and users.
T0109	Review, conduct, or participate in audits of cyber programs and projects.
T0110	Support the Chief Information Officer (CIO) in the formulation of cybersecurity policies.
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.
T0114	Apply cybersecurity functions (e.g., encryption, access control and identity management) to reduce exploitation opportunities.

Task ID	Task Description
T0115	Maintain knowledge of cybersecurity threats to the organization.
T0116	Conduct in-depth research and analysis into cybersecurity threats.
T0117	Develop information sources required to answer the organization's requests for cybersecurity information.
T0118	Generate requests for cybersecurity information.
T0119	Produce timely, relevant cyber threat intelligence reports fusing information from multiple sources.
T0120	Provide up to date cyber threat intelligence to support key stakeholders in responding to cybersecurity threats and incidents.
T0121	Provide evaluation and feedback to cyber threat intelligence sources to improve the quality of their intelligence.
T0122	Provide timely notice of imminent or hostile intentions or activities which may impact the organization's objectives, resources, or capabilities.
T0123	Work closely with stakeholders to ensure the cyber threat intelligence available to the organization is relevant, accurate and up-to-date.
T0124	Identify the tactics and methodologies of cyber threats relevant to the organization.
T0125	Identify foreign language terminology within computer programs.
T0126	Work with others on policies, processes and procedures relating to cybersecurity and privacy.
T0127	Ensure that appropriate controls are in place to effectively mitigate risk and address privacy concerns during a risk assessment process.
T0128	Work with others to implement and maintain a cybersecurity risk management program.
T0129	Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.
T0130	Establish a risk management strategy for the organization that includes a determination of risk tolerance.
T0131	Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis.
T0132	Work with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels.
T0133	Use continuous monitoring tools to assess risk on an ongoing basis.
T0134	Develop security architecture elements to mitigate threats as they emerge.

Task ID	Task Description
T0135	Review and analyze cybersecurity threats to provide stakeholders with information needed to respond to threats.
T0136	Make recommendations to enable effective remediation of vulnerabilities.
T0137	Ensure sound principles are reflected in the organization's mission, vision and goals.
T0500	Deliver secure cloud solutions to development teams, ensure security of cloud migrations and cloud application development.
T0501	Work within and across multi-disciplinary teams as a domain expert in cloud security architecture standards and methodologies.
T0502	Evaluate and determine the adequacy of security architectures and designs.
T0503	Develop and implement secure cloud strategy in conjunction with enterprise architecture.
T0504	Develop and enforce secure designs for technology teams to consume cloud services.
T0505	Build solutions to identify existing organizational data within cloud environments.
T0506	Provide subject matter expertise to develop and architect the next generation of organizational cybersecurity.
T0507	Employ secure configuration management processes.
T0508	Identify and prioritize critical business functions in collaboration with organizational stakeholders.
T0509	Provide advice on project costs, design concepts, or design changes.
T0510	Advise on security requirements to be included in procurement documents.
T0511	Analyze candidate architectures, allocate security services and select security mechanisms.
T0512	Define system security context, concept of operations and baseline requirements in line with applicable cybersecurity policies.
T0513	Evaluate security architectures and designs proposed in procurement documents.
T0514	Write detailed functional specifications that document the architecture development process.
T0515	Analyze user needs and requirements to plan architecture.

Task ID	Task Description
T0516	Develop enterprise architecture or system components required to meet user needs.
T0517	Document and update as necessary all definition and architecture activities.
T0518	Determine security controls for information systems and networks and document appropriately.
T0519	Assess and design cybersecurity management functions.
T0520	Define appropriate availability levels for critical system functions and disaster recovery and continuity of operations requirements to deliver them.
T0521	Build the security controls in place to properly monitor and protect information held in cloud environments.
T0522	Serves as a subject matter expert for security cloud architecture, including networking, storage, databases, provisioning and management.
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 systems and networks with multilevel security requirements.
T0525	Document and address organization's security architecture, and systems security engineering requirements throughout the acquisition life cycle.
T0526	Ensure that acquired or developed systems and architectures are consistent with organization's cybersecurity architecture guidelines.
T0527	Translate proposed capabilities into technical requirements.
T0528	Work with agile team members to conduct fast prototyping, feasibility studies and evaluation of new technologies.
T0529	Design systems and solutions to support successful proofs-of-concept and pilot projects in emerging technology areas.
T0530	Read and interpret technical diagrams, specifications, drawings, blueprints and schematics relating to systems and networks.
T0531	Determine and document security controls for systems and networks.
T1000	Analyze and define data requirements and specifications.
T1001	Analyze and plan for anticipated changes in data capacity requirements.
T1002	Analyze information to determine, recommend and plan the development of a new application or modification of an existing application.

Task ID	Task Description
T1003	Assess how user needs and software requirements can be met in line with cybersecurity policies and determine feasibility of design within time and cost constraints.
T1004	Analyze design constraints and trade-offs in detailed system cybersecurity design and consider life cycle support.
T1005	Apply coding and testing security standards.
T1006	Apply secure code documentation.
T1007	Assess the effectiveness of systems' cybersecurity measures.
T1008	Build, test and modify product prototypes to demonstrate compliance with cybersecurity requirements using working or theoretical models.
T1009	Integrate cybersecurity into the requirements process by defining and capturing security controls.
T1010	Ensure program development and revisions are fully documented and can be understood by others by using comments in the coded instructions.
T1011	Determine project limitations and capabilities, performance requirements and interfaces.
T1012	Develop threat model based on customer interviews and requirements.
T1013	Evaluate interface between hardware and software, in consultation with engineering staff.
T1014	Ensure that desired results are produced by rechecking the program and correct errors by making appropriate changes.
T1015	Design and develop cybersecurity or cybersecurity-enabled products.
T1016	Design hardware, operating systems and software applications to address cybersecurity requirements.
T1017	Design or integrate appropriate secure system backup and protected storage of back up data capabilities into designs.
T1018	Develop and direct procedures and documentation for system testing and validation.
T1019	Review and validate data mining and data warehousing programs, processes and requirements.
T1020	Develop data standards, policies and procedures.

Task ID	Task Description
T1021	Develop detailed security design documentation for component and interface specifications to support system design and development.
T1022	Develop and test disaster recovery and continuity of operations plans for systems under development prior to systems entering a production environment.
T1023	Develop secure code and error handling processes and documentation.
T1024	Inform hardware configuration through evaluation of cost constraints and security restrictions.
T1025	Examine recovered data for information relevant to cybersecurity events and incidents.
T1026	Identify and allocate security functions to components and describe the relationships between them.
T1027	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems.
T1028	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.
T1029	Identify, at a high level, basic common coding errors.
T1030	Apply methodologies to correct common coding errors with security implications to ensure development of secure software.
T1031	Ensure that cybersecurity is built into software development, maintenance and decommissioning processes.
T1032	Ensure that cybersecurity is incorporated into system design.
T1033	Ensure that alerting on vulnerabilities is built into system designs.
T1034	Manage the compilation, cataloging, caching, distribution and retrieval of data.
T1035	Perform integrated quality assurance testing of security systems' functionality and resilience.
T1036	Prepare detailed workflow charts and diagrams that describe input, output and logical operation of security systems.
T1037	Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.
T1038	Provide guidelines for implementing developed systems to customers or installation teams.

Task ID	Task Description
T1039	Provide recommendations on new database technologies and architectures.
T1040	Address security implications in the software acceptance phase.
T1041	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
T1042	Support security certification test and evaluation activities.
T1043	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling and defining any specific security criteria.
T1044	Utilize models and simulations to analyze or predict system performance under different operating conditions.
T1045	Identify cybersecurity capability strategies for custom hardware and software development based on organization's requirements.
T1046	Ensure penetration testing is carried out when required for new or updated applications.
T1047	Design and develop key cybersecurity management functions.
T1048	Analyze user needs and requirements to plan and conduct system security development.
T1049	Develop cybersecurity designs to meet operational needs and environmental factors.
T1050	Collaborate with stakeholders to identify appropriate cybersecurity solutions technology.
T1051	Design and develop new 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 cybersecurity systems design and maintenance.
T1055	Direct cybersecurity software programming and development of documentation.
T1056	Employ configuration management processes when implementing cybersecurity systems.
T1057	Evaluate network infrastructure vulnerabilities.

Task ID	Task Description
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	Assess the validity of source data and subsequent findings.
T1061	Conduct hypothesis testing using statistical processes.
T1062	Confer with systems analysts, engineers, programmers and others to design cybersecurity applications.
T1063	Design, implement, test and evaluate secure interfaces between information systems, physical systems and embedded technologies.
T1064	Develop and facilitate data-gathering methods.
T1065	Develop strategic insights from large data sets.
T1066	Program custom algorithms.
T1067	Provide stakeholders with actionable recommendations derived from data analysis and findings.
T1068	Utilize technical documentation or resources to implement new mathematical, data science, or computer science methodologies.
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.
T1073	Troubleshoot prototype design and process issues throughout the product design, development and pre-launch phases.
T1074	Find opportunities to develop new capability to address vulnerabilities.
T1075	Identify and leverage enterprise-wide security processes and services while designing and developing secure applications.
T1076	Analyze and provide information to stakeholders to support the development or modification of security applications.

Task ID	Task Description
T1077	Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.
T1078	Conduct trial runs of programs and software applications to ensure that the desired information is produced, and instructions and security levels are correct.
T1079	Design to security requirements to ensure requirements are met for all systems and applications.
T1080	Develop software testing and validation procedures, programming and documentation.
T1081	Develop secure software testing and validation procedures.
T1082	Develop system testing and validation procedures, programming and documentation.
T1083	Develop and implement data mining and data warehousing programs.
T1084	Develop mitigation strategies to address cost, schedule, performance and security risks.
T1085	Modify and maintain existing software to correct errors, adapt to new hardware, or upgrade interfaces and improve performance.
T1086	Perform secure program testing, review and assessment to identify potential flaws in codes and mitigate vulnerabilities.
T1087	Perform security reviews and identify security gaps in architecture.
T1088	Provide input to information systems security implementation plans and standard operating procedures.
T1089	Trace system requirements to design components and perform gap analysis.
T1090	Verify stability, interoperability, portability and scalability of system architecture.
T1091	Research and evaluate available technologies and standards to meet customer requirements.
T1092	Determine and document software patches or the extent of releases that would leave software vulnerable.
T1093	Review, approve, prioritize and submit operational requirements for research, development and acquisition of cyber capabilities.
T1094	Develop world class automated processes and artificial intelligence solutions.
T1095	Define and develop automated computational solutions, including analytic and algorithmic solutions.

Task ID	Task Description
T1096	Leverage statistical and machine learning techniques for trend identification and predictive analysis.
T1097	Apply knowledge of machine learning, computer vision, remote sensing and big data processing to important problems by developing software to measure the feasibility of algorithms and approaches.
T1098	Analyze data and conduct quantitative data analysis using a variety of datasets to identify, monitor and explore operations.
T1099	Keep current with computer vision and machine learning research to replicate and baseline new techniques.
T1100	Use visualization tools to visualize data and create dashboards to communicate results.
T1101	Perform data profiling, statistical and machine learning analysis.
T1102	Convert detailed workflow charts and diagrams for security systems into a series of instructions coded in a computer language.
T1103	Use quantitative techniques.
T1104	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.
T1500	Obtain resources to develop and implement effective processes to meet strategic cybersecurity goals.
T1501	Understand and communicate an organization's cybersecurity status during legal and regulatory scrutiny.
T1502	Ensure appropriate data is collected and maintained to meet defined cybersecurity reporting requirements.
T1503	Promote and demonstrate the value of cybersecurity to stakeholders within an organization.
T1504	Ensure that cybersecurity improvement actions are evaluated, implemented and reviewed as required.
T1505	Ensure that cybersecurity inspections, tests and reviews are coordinated for the network environment.
T1506	Ensure that cybersecurity requirements are included in all business continuity and disaster recovery planning operations.
T1507	Ensure that cybersecurity architecture design is aligned with the organization's cybersecurity strategy.
T1508	Evaluate development of new systems and processes to ensure that appropriate security controls are implemented.
T1509	Identify alternative cybersecurity strategies to address organizational security objective.

Task ID	Task Description
T1510	Identify the implications of new technologies and upgrades on cybersecurity across the organization.
T1511	Communicate effectively with third parties in the event of a cybersecurity incident.
T1512	Review and, if appropriate, approve cybersecurity capabilities of proposed new technologies prior to organizational adoption.
T1513	Ensure that organizational situational awareness is maintained from a cybersecurity perspective.
T1514	Ensure that information relating to the organization's cybersecurity is appropriately managed, evaluated and shared.
T1515	Review the effectiveness of the organization's cybersecurity controls against its strategic goals.
T1516	Ensure that cybersecurity training and awareness programs are carried out on a regular basis.
T1517	Participate in cybersecurity risk assessment as required.
T1518	Participate in the development or modification of cybersecurity program plans and requirements.
T1519	Ensure that all documentation relating to network security is developed, issued and maintained.
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	Manage the regular review and maintenance of the organization's cybersecurity policy and associated documentation.
T1526	Ensure that appropriate actions are taken to mitigate the risk in the event of a cybersecurity incident.
T1527	Use internationally available documentation relating to cybersecurity implementation to inform and enhance organizational documentation.

Task ID	Task Description
T1528	Advocate cybersecurity related topics with senior management, to ensure the organization's strategic goals include cybersecurity.
T1529	Ensure that organizational cybersecurity strategy is effectively addressed by cybersecurity policies and related documents.
T1530	Review the effectiveness and efficiency of the procurement function in ensuring that cybersecurity requirements and supply chain risks are addressed as necessary and make improvements where necessary.
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.
T1533	Ensure that appropriate cybersecurity resource are always available.
T1534	Develop and maintain appropriate cybersecurity policies and related documentation to ensure the organization's critical infrastructure is appropriately protected.
T1535	Collaborate with stakeholders in the organization and with third parties when identifying future cybersecurity strategy requirements.
T1536	Identify and recruit appropriately skilled resources to address cybersecurity activities within the organization.
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 and present at international cybersecurity events.
T1542	Ensure that cybersecurity assumptions are reviewed on a regular basis.
T2000	Obtain relevant resource to implement and maintain the cybersecurity aspects of an effective business continuity plan.
T2001	Communicate relevant changes in the organization's cybersecurity posture to senior management.
T2002	Conduct interactive training exercises to create an effective learning environment.

Task ID	Task Description
T2003	Develop and maintain a cybersecurity strategy that aligns to the organization's business strategy.
T2004	Develop or identify awareness training materials that are appropriate for intended audiences.
T2005	Evaluate the effectiveness and comprehensiveness of training programs.
T2006	Identify organizational policy stakeholders.
T2007	Ensure that 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	Support the design and execution of exercise scenarios.
T2012	Write instructional materials to provide detailed guidance to the organization's staff or units.
T2013	Develop or assist in the development of computer-based training modules or classes.
T2014	Develop or assist in the development of course assignments.
T2015	Develop or assist in the development of course evaluations.
T2016	Develop or assist in the development of grading and proficiency standards.
T2017	Develop or assist in the development of individual or collective learning and development, training and skills or knowledge gap remediation plans.
T2018	Develop or assist in the development of learning objectives and goals.
T2019	Develop or assist in the development of on-the-job training materials or programs.
T2020	Develop or assist in the development of written tests for measuring and assessing learner proficiency.
T2021	Assess the effectiveness and efficiency of instruction against different performance indicators.

Task ID	Task Description
T2022	Conduct learning needs assessments and identify requirements.
T2023	Work with subject matter experts to ensure qualification standards reflect organizational functional requirements and industry standards.
T2024	Develop interactive learning exercises and an effective learning environment.
T2025	Develop and implement standardized position descriptions based on established cybersecurity workforce roles.
T2026	Develop and review recruiting, hiring and retention procedures in accordance with current HR policies.
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 or assist in the development of training policies and protocols for cybersecurity training.
T2029	Develop the goals and objectives for an organizational cybersecurity training curriculum.
T2030	Ensure that cybersecurity careers are managed in accordance with organizational HR policies and directives.
T2031	Establish and collect metrics to monitor and validate cybersecurity workforce capacity, capability and readiness.
T2032	Establish and oversee requirements, qualifications and processes for cyber career entry.
T2033	Establish cyber career paths to allow career progression, development and growth within and between cyber career fields.
T2034	Establish data requirements to support cyber workforce management and reporting requirements.
T2035	Establish, resource, implement and assess cyber workforce management programs in accordance with organizational requirements.
T2036	Evaluate instructional strategy and delivery options in conjunction with educators and trainers to develop the most effective organizational learning and development plan.
T2037	Review and apply cyber career qualification standards.
T2038	Review and apply organizational policies related to or influencing the cyber workforce.
T2039	Support integration of qualified cyber workforce personnel into information systems life cycle development processes.

Task ID	Task Description
T2040	Correlate training and learning to business or mission requirements.
T2041	Create training courses tailored to the audience and physical or virtual environments.
T2042	Deliver training courses tailored to the audience and physical or virtual environments.
T2043	Apply concepts, procedures, software, equipment and technology applications to students.
T2044	Design training curriculum and course content based on the organization and workforce requirements.
T2045	Assist the development of training curriculum and course content.
T2046	Ensure that training meets cybersecurity training, education, or awareness goals and objectives.
T2047	Identify and address cyber workforce planning and management issues including recruitment, retention and training.
T2048	Plan and coordinate the delivery of classroom techniques and formats for the most effective learning environment.
T2049	Plan non-classroom educational techniques and formats.
T2050	Conduct periodic reviews and revisions of course content for accuracy, completeness, alignment and currency.
T2051	Recommend revisions to curriculum and course content based on feedback from previous training sessions.
T2052	Serve as an internal consultant and advisor in own area of expertise.
T2053	Review and approve training supplier selection and management policies.
T2054	Develop or assist with the development of training materials to increase workforce understanding of organizational cybersecurity, data protection and privacy policies, including legal obligations.
T2500	Develop methods to effectively monitor and measure risk, compliance and assurance efforts.
T2501	Develop specifications to ensure that risk, compliance and assurance efforts conform with cybersecurity requirements.
T2502	Maintain knowledge of applicable cybersecurity defense policies, regulations and compliance documents as they pertain to cybersecurity defense auditing.
T2503	Manage and approve agreed accreditation packages.

Task ID	Task Description
T2504	Monitor and evaluate a system's compliance with cybersecurity, resilience and dependability requirements.
T2505	Plan and conduct cybersecurity authorization reviews and assurance case development for initial installation of systems and networks.
T2506	Provide an accurate technical evaluation of software applications, systems, or networks and document their compliance with agreed cybersecurity requirements.
T2507	Review risk registers or other similar documents to confirm that the level of risk is within acceptable limits for each software application, system and network.
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 and audits for services provided by third parties.
T2510	Regularly review and ensure that cybersecurity policies and related documentation are aligned with the organization's stated business objectives and strategy.
T2511	Define and document the effect of implementation of a new system or new interfaces between systems on the security posture of the existing environment.
T2512	Ensure that security design and cybersecurity development activities are appropriately documented.
T2513	Determine and document supply chain risks for critical system elements, where they exist.
T2514	Provide support to compliance activities as necessary.
T2515	Ensure that 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.
T2517	Verify accreditation packages.
T2518	Maintain knowledge of applicable legislation, regulation and accreditation standards and regularly review these to ensure continued organizational compliance.
T2519	Cooperate with relevant regulatory agencies and other legal entities in any compliance reviews or investigations.
T2520	Develop processes with any external auditors on information sharing in a secure manner.
T3000	Evaluate the effectiveness of policies, standards, or procedures against the organization's strategy.

Task ID	Task Description
T3001	Interpret and apply laws, regulations, policies, standards, or procedures as necessary.
T3002	Resolve conflicts in policies, standards, or procedures where they contradict applicable laws or regulations.
T3003	Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures etc.
T3004	Provide cybersecurity expertise to the framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.
T3005	Develop guidelines for implementation of relevant cybersecurity controls.
T3006	Provide cybersecurity guidance to oversight and compliance personnel regarding compliance with cybersecurity policies and relevant legal and regulatory requirements.
T3007	Evaluate the impact of changes in laws and regulations on an organization's cybersecurity policies and related documentation.
T3008	Provide cybersecurity related guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.
T3009	Assist with the implementation of new or revised laws, regulations, executive orders etc. as they relate to cybersecurity policies and other documentation.
T3010	Provide cybersecurity related guidance in the preparation of legal and other relevant documents.
T3011	Work with the organization's legal advisers and relevant third parties to ensure that all services comply with privacy and data security requirements.
T3012	Work with the organization's legal advisers, management and other stakeholders to ensure the organization has and maintains appropriate privacy and confidentiality documentation.
T3013	Work with stakeholders to develop relationships with regulators and government departments responsible for privacy and data security issues.
T3014	Ensure all processing and data source are registered with the relevant privacy and data protection authorities where required.
T3015	Work with business teams and senior management to ensure awareness of best practices relating to information privacy and data security.
T3016	Work with senior management to establish a committee responsible for the oversight of data privacy.
T3017	Provide leadership on the committee responsible for the oversight of data privacy.
T3018	Develop and document procedures for reporting self-disclosures of any evidence of privacy violations.

Task ID	Task Description
T3019	Serve as the information privacy liaison for users of technology systems, reporting breaches to senior management.
T3020	Develop training materials and other communications to increase employees understanding of company privacy policies, data handling practices and legal obligations.
T3021	Oversee, direct and ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties.
T3022	Ensure that privacy training and awareness activities are delivered on a regular basis.
T3023	Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues.
T3024	Work with organization administration, legal advisers and other related parties to represent the organization's information privacy interests with external parties.
T3025	Report on a periodic basis regarding the status of the privacy program to senior management and other responsible individuals or committees.
T3026	Provide leadership for the organization's privacy program.
T3027	Direct and oversee privacy specialists and coordinate privacy and data security programs with senior management to ensure consistency across the organization.
T3028	Ensure compliance with privacy practices across the organization.
T3029	Work with legal and HR teams to develop appropriate sanctions for failure to comply with the organization's privacy policies and procedures.
T3030	Resolve allegations of noncompliance with organizational privacy policies or notice of information practices in a timely manner.
T3031	Establish and maintain a risk management and compliance framework for privacy.
T3032	Review the organization's data and privacy projects to ensure that they are compliant with the organization's privacy and data security policies.
T3033	Establish a process for managing all aspects of complaints concerning the organization's privacy policies and procedures.
T3034	Provide leadership in the planning, design and evaluation of privacy and cybersecurity related projects.
T3035	Establish and maintain an internal privacy audit program.
T3036	Periodically review and update the privacy program to incorporate changes in laws, regulations or organizational policy.

Task ID	Task Description
T3037	Provide development guidance and assistance relating to the organization's information privacy policies and procedures.
T3038	Ensure that the use of technologies maintains and does not erode, privacy protections on use, collection and disclosure of personal information.
T3039	Monitor systems development and operations to ensure compliance with cybersecurity and privacy policies.
T3040	Conduct privacy impact assessments of proposed rules on the privacy of personal information.
T3041	Review all cybersecurity plans to ensure alignment between cybersecurity and privacy practices.
T3042	Develop and manage procedures for vetting and auditing vendors for compliance with appropriate privacy, data security, legislative and regulatory requirements.
T3043	Ensure all complaints concerning the organization's privacy policies and related documentation are addressed in a timely manner by appropriate resource.
T3044	Identify and remediate areas where the organization is not fully compliant with privacy requirements.
T3045	Coordinate with the Chief Information Security Officer (or equivalent) to ensure alignment between cybersecurity and privacy practices.
T3046	Develop and maintain appropriate communications and training to promote and educate all employees including senior management regarding privacy compliance and the consequences of noncompliance.
T3047	Ensure that privacy compliance monitoring activities are carried out on an ongoing basis.
T3048	Ensure that appropriate technologies are used to maintain compliance with privacy requirements.
T3049	Develop strategic plans with senior management to ensure that personal information is processed accordance with applicable privacy requirements.
T3050	Develop and maintain enterprise-wide procedures to ensure that new products and services are developed in accordance with organizational privacy policies and legal obligations.
T3051	Work with the Chief Information Security Officer, legal counsel and senior management to manage privacy incidents and breaches in accordance with legal and regulatory requirements.
T3052	Maintain awareness of applicable privacy laws, regulations and accreditation standards.
T3053	Manage company participation in public events related to privacy and data security.
T3500	Develop cyber defense tools.

Task ID	Task Description
T3501	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
T3502	Manage and administer the updating of rules and signatures for cyber defense applications.
T3503	Coordinate with other cyber defense staff to validate network alerts.
T3504	Provide summary reports of network events and other cybersecurity-relevant activities in line with organizational policies and requirements.
T3505	Build, install, configure, patch and test dedicated cyber defense hardware and software.
T3506	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.
T3507	Administer test beds and test and evaluate applications, hardware infrastructure, rules, signatures, access controls and configurations of platforms managed by service providers.
T3508	Create, edit and manage network access control lists on specialized cyber defense systems.
T3509	Identify and report potential conflicts with implementation of any cyber defense tools.
T3510	Implement risk management framework and security assessment and authorization requirements for dedicated cyber defense systems within the organization and document and maintain records for them.
T3511	Select the security controls for a system and document the functional description of the planned control implementations in a security plan.
T3512	Implement the security controls specified in a security plan or other system documentation.
T4000	Apply service-oriented security architecture principles to meet the organization's confidentiality, integrity and availability requirements.
T4001	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.
T4002	Apply security patches to commercial products in accordance with the timelines dictated by the management authority for the intended operational environment.
T4003	Implement specific cybersecurity countermeasures for systems and applications.
T4004	Integrate automated capabilities for updating or patching system software where practical.
T4005	Ensure cybersecurity testing of developed applications and systems.
T4006	Document and update systems security implementation, operations and maintenance activities.

Task ID	Task Description
T4007	Provide cybersecurity guidance to leadership.
T4008	Detect and analyze encrypted and concealed data.
T4009	Develop and test procedures to transfer system operations to an alternate site.
T4010	Execute business continuity and disaster recovery procedures.
T4011	Implement security measures to system or system components to resolve vulnerabilities, mitigate risks and recommend security changes.
T4012	Implement system security measures in accordance with established procedures.
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	Verify minimum security requirements are in place for all applications.
T4016	Work with other teams to design, develop and provide identity access management solutions.
T4017	Work with cybersecurity architect to develop the identity access management strategy.
T4018	Ensure identity access management implementations follow organization's standards and policies.
T4019	Work with stakeholders to identify and address gaps in the identity access management implementation.
T4020	Mentor and advise team members on identity access management systems and processes.
T4021	Develop, design and implement cryptographic algorithms to meet organization's requirements.
T4022	Analyze cryptographic algorithms to find weaknesses and break ciphers.
T4023	Develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.
T4024	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
T4025	Manage accounts, network rights, and access to systems and equipment.

Task ID	Task Description
T4026	Design and develop systems administration and management functionality for privileged access users.
T4027	Administer accounts, network rights and access to systems and equipment.
T4028	Establish continuous monitoring tools and technologies access control process and procedures.
T4029	Ensure that continuous monitoring tools and technologies access control is managed adequately.
T4500	Conduct or support authorized penetration testing of infrastructure and assets.
T4501	Conduct required reviews, including reviews of defensive measures, according to the organization's policies.
T4502	Recommend cost-effective security controls to mitigate risks identified through testing and review.
T4503	Gather information about network topography and usage through technical analysis and open source research and document findings.
T4504	Mimic malicious social engineering techniques that an attacker would use to attempt a system breach to uncover security gaps and vulnerabilities.
T4505	Identify methods that attackers could use to exploit system and network vulnerabilities.
T4506	Include business considerations in security strategies and recommendations.
T4507	Carry out vulnerability scanning on systems and assets.
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 remote testing of a network to expose weaknesses in security.
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.

Task ID	Task Description
T4515	Explain business impact of vulnerabilities identified through testing to make case for addressing them.
T4516	Conduct physical security assessments of servers, systems and network devices.
T4517	Test for vulnerabilities in web applications, client applications and standard applications.
T4518	Use security testing and code scanning tools to conduct code reviews.
T5000	Analyze log files, evidence and other information to determine best methods for identifying perpetrators of a network intrusion.
T5001	Interview victims of a possible cybercrime and witnesses.
T5002	Confirm what is known about an intrusion and seek to discover new information.
T5003	Provide expert technical support to resolve cyber defense incidents.
T5004	Create a forensically sound duplicate of the evidence to use for data recovery and analysis processes, in line with national or organizational policies as applicable.
T5005	Develop a plan to investigate alleged cybercrime, violation, or suspicious activity.
T5006	Provide technical summary of findings in accordance with established reporting procedures.
T5007	Ensure that chain of custody is followed for all acquired digital media in accordance with national law or organizational policies as applicable.
T5008	Fuse results from analysis of networks, infrastructure and digital evidence with results from other criminal investigations and operations.
T5009	Determine whether a cybersecurity incident may be a violation of law requiring specific legal action.
T5010	Identify digital evidence for examination and analysis.
T5011	Identify evidence that can prove that a cybercrime took place.
T5012	Identify, collect and seize documentary or physical evidence associated with cyber intrusion incidents, investigations and operations.
T5013	Perform dynamic analysis to boot an “image” of a drive - with or without the original - to see the intrusion as the user may have seen it, in a native environment.
T5014	Perform hash comparison against databases required by organizational policies.

Task ID	Task Description
T5015	Perform static media analysis.
T5016	Perform tier 1, 2 and 3 malware analysis.
T5017	Ensuring data integrity when preparing digital media for imaging.
T5018	Process crime scenes.
T5019	Provide technical assistance in acquiring, securing, handling or analyzing digital evidence.
T5020	Recognize and report forensic artifacts in line with reporting policies.
T5021	Secure electronic devices and information sources required for analysis.
T5022	Extract data from devices.
T5023	Use specialized equipment and techniques to perform forensic tasks in line with policy.
T5024	Conduct cursory binary analysis.
T5025	Work as a technical expert in support of law enforcement, explaining incident details and forensic analysis as required.
T5026	Perform virus scanning on digital media.
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.
T5030	Utilize deployable forensics toolkits to support operations.
T5031	Coordinate with threat intelligence analysts to correlate threat assessment data.
T5032	Take necessary steps to mitigate potential risks from the incident to people, assets and resources.
T5033	Assess and report on actions and behaviors relevant to the investigation of victims, witnesses, or suspects.

Task ID	Task Description
T5034	Determine the extent of threats and risks arising from them and recommend courses of action or countermeasures to mitigate them.
T5035	Provide criminal investigative support to legal authorities during the judicial process.
T5036	Process image with tools appropriate to the investigation's objectives.
T5037	Perform Windows registry analysis.
T5038	Perform file and registry monitoring on the running system after identifying intrusion.
T5039	Enter information for acquired digital media into tracking database.
T5040	Report cyber incidents to inform cyber defense.
T5041	Build and maintain a deployable cybersecurity incident response toolkit.
T5042	Analyze material from cybersecurity incidents for evidence of hostile foreign actor or criminal activity.
T5043	Gather and preserve evidence that could be used to prosecute perpetrators of the cybercrime.
T5044	Use results from analysis of intrusion artefacts to inform advice on the mitigation of potential cyber defense incidents.
T5045	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.
T5046	Identify and develop leads and sources of information to assist identification or prosecution of those responsible for a cybercrime.
T5047	Document original condition of digital and associated evidence in line with national or organizational policies.
T5048	Analyze IT systems and digital media to solve, investigate and prosecute cybercrimes.
T5049	Document the investigation in line with legal standards and requirements.
T5050	Review forensic images, volatile data and other data sources to recover potentially relevant information.
T5051	Write and publish recommendations and reports on incident findings to appropriate constituencies.
T5052	Review gathered information for validity and relevance to the investigation in line with organizational policies.

Task ID	Task Description
T5053	Reconstruct networks in diagram and report format.
T5054	Identify and select most effective sources of information to assist with incident investigation.
T5055	Sanitize reports to protect proprietary, commercial, personal or otherwise sensitive or confidential data or methods.
T5056	Track status of requests for information in line with the organization's policies.
T5057	Document lessons learned from the outcome of events or exercises.
T5058	Identify potential malicious activity from memory dumps, logs and packet captures.
T5059	Examine recovered data for information of relevance to the issue at hand.
T5060	Devise creative and custom exploits, solutions and techniques to discover vulnerabilities and exploitability of the targets.
T5061	Interview those suspected of having committed a cybercrime.
T5062	Identify intrusion via dynamic analysis.
T5500	Use reviews to recommend new or revised security, resilience and dependability measures.
T5501	Analyze the results of software, hardware, or interoperability testing to identify cost-effective improvements that can reduce identified risks.
T5502	Answer requests for information in line with the organization's policies.
T5503	Use knowledge of threat actors and activities to build common understanding of organization's current risk profile.
T5504	Use knowledge of threat actors and activities to inform organization's response to a cyber incident.
T5505	Coordinate, validate and manage the organization's cyber threat intelligence sources and feeds.
T5506	Identify information gaps in threat intelligence and assess their implications for the organization.
T5507	Prepare and deliver briefs on specific threats to the organization.
T5508	Work collaboratively and share information with threat intelligence analysts working in related fields.

Task ID	Task Description
T5509	Conduct network scouting and analyze vulnerabilities of systems within a network.
T5510	Conduct nodal analysis.
T5511	Detect exploits against networks and hosts of interest to inform understanding of threat actor activity.
T5512	Determine what technologies are used by threat actors of interest.
T5513	Develop information sources to deepen understanding of threat actors of interest.
T5514	Apply analytic techniques to gain information about threats actors of interest.
T5515	Evaluate threat decision-making processes.
T5516	Identify threat behaviors and vulnerabilities.
T5517	Identify the principal threats to the organization's known vulnerabilities.
T5518	Evaluate available capabilities to combat likely threat activities to recommend efficient solutions.
T5519	Identify threat tactics and methodologies.
T5520	Identify and evaluate threat critical capabilities, requirements and vulnerabilities.
T5521	Identify the threat actor's structure and components.
T5522	Identify intelligence gaps and shortfalls.
T5523	Provide input to or develop courses of action based on understanding of threat.
T5524	Monitor and report changes in threat dispositions, activities, tactics, capabilities and objectives.
T5525	Monitor and report on validated threat activities.
T5526	Monitor open source websites for hostile content directed towards organizational or partner interests.
T5527	Monitor and report on threat actor activities to fulfil organization's threat intelligence and reporting requirements.

Task ID	Task Description
T5528	Use expertise on threat actors and activities to support activities to plan and develop the organization's cybersecurity strategy and resources.
T5529	Provide information and assessments of threat actors to assist stakeholders in planning and executing cybersecurity activities.
T5530	Provide real-time cyber threat intelligence analysis and support during cybersecurity incidents and exercises.
T5531	Monitor cyber threat intelligence feeds and report significant network events and intrusions.
T5532	Perform incident handling, event triage, network analysis, threat detection, trend analysis, metric development and vulnerability information dissemination.
T5533	Support threat and vulnerability analysis and cybersecurity advisory services and recommendations.
T5534	Perform tier 1 and 2 malware analysis.
T5535	Maintain a common intelligence picture.
T5536	Conduct in-depth research and analysis.
T5537	Develop information requirements necessary for answering priority information requests.
T5538	Generate requests for information.
T5539	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).
T5540	Provide current intelligence support to critical internal/external stakeholders as appropriate.
T5541	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements and operations.
T5542	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.
T5543	Work closely with planners, intelligence analysts and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.
T5544	Identify cyber threat tactics and methodologies.
T5545	Identify foreign language terminology within computer programs (e.g., comments, variable names).
T6000	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event in IT and ICS/OT environments.

Task ID	Task Description
T6001	Develop and integrate cybersecurity designs for systems and networks with multilevel security requirements in IT and ICS/OT environments.
T6002	Document and address organization's security, architecture and systems security engineering requirements throughout the acquisition life cycle in IT and ICS/OT environments.
T6003	Ensure that acquired or developed systems and architectures are consistent with organization's cybersecurity architecture guidelines in IT and ICS/OT environments.
T6004	Translate proposed capabilities into technical requirements in IT and ICS/OT environments.
T6005	Conduct analysis of physical and logical digital technologies in IT and ICS/OT enviroments to identify potential avenues of access.
T6006	Research emerging communications technology trends to inform organizational design and security policies in IT and ICS/OT environments.
T6007	Select the security controls for a system and document the functional description of the planned control implementations in a security plan in IT and ICS/OT environments.
T6008	Implement the security controls specified in a security plan or other system documentation in IT and ICS/OT environments.
T6009	Work with agile team members to conduct fast prototyping, feasibility studies and evaluation of new technologies in IT and ICS/OT environments.
T6010	Design systems and solutions to support successful proofs-of-concept and pilot projects in emerging technology areas in IT and ICS/OT environments.
T6011	Read and interpret technical diagrams, specifications, drawings, blueprints and schematics relating to systems and networks in IT and ICS/OT environments..
T6012	Understand and troubleshoot fault areas in industrial automation and communication systems.
T6013	Determine and document security controls for systems and networks in IT and ICS/OT environments.
T6014	Coordinate and provide expert technical support to the organization's cybersecurity team to resolve ICS/OT cybersecurity incidents.
T6015	Perform real-time cybersecurity incident handling tasks in ICS/OT environment to support deployed incident response team.
T6016	Perform risk analysis for ICS/OT environments whenever an application or a system undergoes a change.

Table 10: Knowledge Descriptions

KSA ID	KSA Description
K0001	Knowledge of network components, their operation and appropriate network security controls and methods.
K0002	Knowledge and understanding of risk assessment, mitigation and management methods.
K0003	Knowledge of relevant cybersecurity aspects of legislative and regulatory requirements, relating to ethics and privacy.
K0004	Knowledge of the principles of cybersecurity and privacy.
K0005	Knowledge of cybersecurity related threats and vulnerabilities.
K0006	Knowledge of the likely operational impact on an organization of cybersecurity breaches.
K0007	Knowledge of cybersecurity authentication, authorization and access control methods.
K0008	Knowledge of business practices within organizations.
K0009	Knowledge of vulnerabilities in applications and their likely impact.
K0010	Knowledge of cybersecurity communication methods, principles and concepts that support the network infrastructure.
K0011	Knowledge of capabilities and applications of network equipment.
K0012	Knowledge of how to analyze capabilities and requirements.
K0013	Knowledge of cybersecurity defense and vulnerability assessment tools and their capabilities.
K0014	Knowledge of computer algorithms.
K0015	Knowledge of computer programming principles.
K0016	Knowledge of encryption algorithms, their relative strengths and weaknesses and appropriate selection criteria.
K0017	Knowledge of cryptography and cryptographic key management concepts.
K0018	Knowledge of data administration and data standardization policies.
K0019	Knowledge of appropriate data backup and recovery methods and solutions, including testing.
K0020	Knowledge of cybersecurity considerations for database systems.

KSA ID	KSA Description
K0021	Knowledge of cybersecurity aspects of business continuity and disaster recovery planning and including testing.
K0022	Knowledge of the organization's enterprise cybersecurity architecture.
K0023	Knowledge of electrical engineering required for computer architecture.
K0024	Knowledge of host and network access control mechanisms.
K0025	Knowledge of how network services and protocols interact to provide network communications.
K0026	Knowledge of installation, integration and optimization of system components.
K0027	Knowledge of human-computer interaction principles.
K0028	Knowledge of cybersecurity assessment and authorization processes.
K0029	Knowledge of cybersecurity controls and privacy requirements for the management of risks relating to data.
K0030	Knowledge of cybersecurity and privacy principles as they apply to software development.
K0031	Knowledge of sources of information relating to the identification and effective treatment of vulnerabilities.
K0032	Knowledge of incident categories, incident responses and timelines for responses.
K0033	Knowledge of best practices for incident response and incident management.
K0034	Knowledge of best practice analysis principles and methods.
K0035	Knowledge of cybersecurity and privacy principles and organizational requirements.
K0036	Knowledge of host-based and network-based intrusion detection methodologies and techniques.
K0037	Knowledge of the organization's risk management processes and procedures.
K0038	Knowledge of IT security principles and methods.
K0039	Knowledge of low-level computer languages required for role.

KSA ID	KSA Description
K0040	Knowledge of mathematics required for role.
K0041	Knowledge of microprocessors.
K0042	Knowledge of network access, identity and access management.
K0043	Knowledge of best practice network traffic analysis methods.
K0044	Knowledge and understanding of new technologies and solutions from a cybersecurity perspective.
K0045	Knowledge of operating systems.
K0046	Knowledge of network traffic protocols, methods and management.
K0047	Knowledge of packet-level analysis.
K0048	Knowledge of parallel and distributed computing concepts.
K0049	Knowledge of policy-based and risk adaptive access controls.
K0050	Knowledge of how to carry out privacy impact assessments.
K0051	Knowledge of programming language structures and logic.
K0052	Knowledge of system and application security threats and vulnerabilities.
K0053	Knowledge of key security management concepts.
K0054	Knowledge of security system design tools, methods and techniques.
K0055	Knowledge of industry standard systems diagnostic tools and fault identification techniques.
K0056	Knowledge of all aspects of system lifecycle management.
K0057	Knowledge of systems testing and evaluation methods.
K0058	Knowledge of telecommunications concepts relevant to role.

KSA ID	KSA Description
K0059	Knowledge of the capabilities and functionality of technologies for organizing and managing information.
K0060	Knowledge of the process for reporting cybersecurity incidents.
K0061	Knowledge of the organization's IT strategy and objectives.
K0062	Knowledge of the systems engineering process.
K0063	Knowledge of Virtual Private Network (VPN) security.
K0064	Knowledge of the components of a network attack and their relationship to threats and vulnerabilities.
K0065	Knowledge of appropriate processes, reporting and investigative tools relating to insider threat investigations, including laws and regulations where relevant.
K0066	Knowledge of physical computer components and peripherals' architectures and functions.
K0067	Knowledge of attackers' relevant to the organization's tactics, techniques and procedures.
K0068	Knowledge of network tools.
K0069	Knowledge of defense-in-depth principles and network security architecture.
K0070	Knowledge of different types of network communication.
K0071	Knowledge of technology that can be exploited.
K0072	Knowledge of file extensions.
K0073	Knowledge of best practices for supply chain risk management.
K0074	Knowledge of the national cybersecurity regulations and requirements relevant to the organization.
K0075	Knowledge of types of digital forensics data and how to recognize them.
K0076	Knowledge of interpreted and compiled computer languages.
K0077	Knowledge of threat intelligence sources, capabilities and limitations.

KSA ID	KSA Description
K0078	Knowledge of how threat intelligence sources collect intelligence.
K0079	Knowledge of the organization's core business processes and how cybersecurity affects them.
K0080	Knowledge of cybersecurity threats, risks and issues posed by new technologies and malicious actors.
K0081	Knowledge of import and export control regulations relevant to cybersecurity risk management activities, knowledge and technologies.
K0082	Knowledge of the organization's risk management processes.
K0083	Knowledge of supply chain risk management standards, processes and practices from a cybersecurity perspective.
K0084	Knowledge of cybersecurity policies, procedures and regulations.
K0085	Knowledge of the organization's IT user security policies.
K0086	Knowledge of the common network layer attack vectors.
K0087	Knowledge of different classes of cyberattacks.
K0088	Knowledge of different types of cyber attackers, their capabilities and objectives.
K0089	Knowledge of effective risk and threat assessment methods.
K0090	Knowledge of system administration, network management and operating system hardening methods.
K0091	Knowledge of relevant legislative and regulatory requirements.
K0092	Knowledge of cybersecurity best practices for IT supply chain management.
K0093	Knowledge of critical information systems that were designed with limited technical cybersecurity controls.
K0094	Knowledge of hardware reverse engineering techniques.
K0095	Knowledge of middleware relevant to role.
K0096	Knowledge of networking protocols.

KSA ID	KSA Description
K0097	Knowledge of software reverse engineering techniques.
K0098	Knowledge of Extensible Markup Language (XML) schemas.
K0099	Knowledge of the stages of a cyberattack.
K0100	Knowledge of network security architecture concepts including topology, protocols, components, and principles.
K0101	Knowledge of network systems management principles, models, methods and tools.
K0102	Knowledge of encryption methodologies.
K0103	Knowledge of the impact of signature implementation on viruses, malware and attacks.
K0104	Knowledge of Windows and Unix ports and services.
K0105	Knowledge of advanced data remediation security features in databases.
K0106	Knowledge of cloud-based knowledge management technologies and concepts applicable to security, governance, procurement and administration.
K0107	Knowledge of data classification standards and methodologies as they relate to the management of cybersecurity risk.
K0108	Knowledge of database access application programming interfaces.
K0109	Knowledge of organizational process improvement concepts and process maturity models.
K0110	Knowledge of cybersecurity architecture concepts and reference models.
K0111	Knowledge of service management concepts for networks and related standards.
K0112	Knowledge of application firewall concepts and functions.
K0113	Knowledge of industry standard security models and their effective application.
K0114	Knowledge of covert communication techniques.
K0115	Knowledge of data backup and restoration concepts.

KSA ID	KSA Description
K0116	Knowledge of confidentiality, integrity and availability requirements.
K0117	Knowledge of OSI model and underlying network protocols.
K0118	Knowledge of relevant laws, legal authorities, restrictions and regulations that govern and are applicable to cybersecurity activities.
K0119	Knowledge of system administration concepts for operating systems used by the organization.
K0120	Knowledge of types of computer architectures relevant to the organization.
K0121	Knowledge of cloud service models and how those models can limit incident response.
K0122	Knowledge of the full spectrum of defensive and offensive cybersecurity capabilities.
K0123	Knowledge of malware analysis concepts and methodologies.
K0124	Knowledge of data security standards relating to personally identifiable information.
K0125	Knowledge of Payment Card Industry Data Security Standards (PCI-DSS).
K0126	Knowledge of data security standards relating to the sector in which the organization operates.
K0127	Knowledge of best practice IT risk management methodologies.
K0128	Knowledge of legislation, regulations and other standards applicable to critical infrastructure cybersecurity.
K0129	Knowledge of configuration management techniques.
K0130	Knowledge of security management.
K0131	Knowledge of current and emerging data encryption security features in databases.
K0132	Knowledge of use-cases relating to cross-platform collaboration and content synchronization.
K0133	Knowledge of an organization's cybersecurity data classification requirement.
K0134	Knowledge of systems security testing and evaluation methods.

KSA ID	KSA Description
K0135	Knowledge of potential vulnerabilities in all network equipment and how it is used.
K0136	Knowledge of countermeasure design for identified security risks.
K0137	Knowledge of how to map networks and recreate network topologies.
K0138	Knowledge of packet-level analysis using appropriate tools.
K0139	Knowledge of the use of sub-netting tools.
K0140	Knowledge of cryptology.
K0141	Knowledge of emerging technologies and their potential for exploitation.
K0142	Knowledge of technology trends.
K0143	Knowledge of cybersecurity vulnerabilities across a range of industry standard technologies.
K0144	Knowledge of the principal methods, procedures and techniques for gathering, producing, reporting and sharing cybersecurity information.
K0145	Knowledge of operating system command-line tools.
K0146	Knowledge of embedded systems and how cybersecurity controls can be applied to them.
K0147	Knowledge of intrusion detection and prevention system tools and applications.
K0148	Knowledge of network protocols and directory services.
K0149	Knowledge of network design processes, including security objectives, operational objectives and trade-offs.
K0150	Knowledge of current and emerging cybersecurity technologies and associated threats.
K0151	Knowledge of access authentication methods.
K0152	Knowledge of how to use network analysis tools to identify vulnerabilities.
K0153	Knowledge of penetration testing and red teaming principles, tools and techniques.

KSA ID	KSA Description
K0154	Knowledge of an organization's threat environment.
K0155	Knowledge of data communications terminology.
K0156	Knowledge of database theory.
K0157	Knowledge of encryption algorithms.
K0158	Knowledge of network security at practitioner level.
K0159	Knowledge of IT operations security.
K0160	Knowledge of organizational objectives, leadership priorities and risk management methods.
K0161	Knowledge of physical and logical network devices and infrastructure.
K0162	Knowledge of cybersecurity risk management and mitigation strategies.
K0163	Knowledge of network security at fundamental level.
K0164	Knowledge of the common networking and routing protocols and how they interact to provide network communications.
K0165	Knowledge of what constitutes a threat to network security.
K0166	Knowledge of risk scoring as part of a risk management process.
K0167	Knowledge of risk assessment methodologies.
K0168	Knowledge of public sources detailing common application security risks and mitigations.
K0169	Knowledge of procedures for reporting compromise of data.
K0500	Knowledge of scripting.
K0501	Knowledge of TCP/IP networking protocols.
K0502	Knowledge of cloud technologies and cloud security.

KSA ID	KSA Description
K0503	Knowledge of network hardware devices and functions.
K0504	Knowledge of network technologies.
K0505	Knowledge of the capabilities and limitations of cybersecurity products.
K0506	Knowledge of best practice cybersecurity risk management methodologies.
K0507	Knowledge of multi-level security systems and cross domain solutions.
K0508	Knowledge of system protection planning measures.
K0509	Knowledge of N-tiered topologies.
K0510	Knowledge of the architectural concepts and patterns.
K0511	Knowledge of integrating the organization's goals and objectives into the system architecture.
K0512	Knowledge of organization's cybersecurity-relevant evaluation and validation criteria.
K0513	Knowledge of system fault tolerance methodologies.
K0514	Knowledge of demilitarized zones.
K0515	Knowledge of the structure, architecture and design of modern digital and telephony networks.
K1000	Knowledge of complex data structures.
K1001	Knowledge of data mining and data warehousing principles.
K1002	Knowledge of database management systems, query languages, table relationships and views.
K1003	Knowledge of digital rights management.
K1004	Knowledge of the organization's evaluation and validation requirements in relation to cybersecurity risk management.
K1005	Knowledge of enterprise messaging systems and associated software.

KSA ID	KSA Description
K1006	Knowledge of how to use resiliency and redundancy to mitigate cybersecurity risks.
K1007	Knowledge of cybersecurity systems engineering principles and standards used by the organization.
K1008	Knowledge of local and wide area networking principles and concepts including bandwidth management.
K1009	Knowledge of process engineering concepts.
K1010	Knowledge of query languages.
K1011	Knowledge of secure configuration management techniques.
K1012	Knowledge of software debugging principles.
K1013	Knowledge of software design tools, methods and techniques.
K1014	Knowledge of software development models.
K1015	Knowledge of software engineering.
K1016	Knowledge of the organization's data-sets sources, characteristics and uses.
K1017	Knowledge of structured analysis principles and methods.
K1018	Knowledge of system design tools, methods and techniques, including automated systems analysis and design tools.
K1019	Knowledge of web services.
K1020	Knowledge of command-line tools.
K1021	Knowledge of secure coding techniques.
K1022	Knowledge of software related IT security principles and methods.
K1023	Knowledge of software quality assurance process.
K1024	Knowledge of secure software deployment methodologies, tools and practices.

KSA ID	KSA Description
K1025	Knowledge of applications that can log errors, exceptions and application faults.
K1026	Knowledge of how to work with and use the output of R&D centers, think tanks, academic research and industry.
K1027	Knowledge of how to utilize technologies and tools to explore, analyze and represent data.
K1028	Knowledge of machine learning theory and principles.
K1029	Knowledge of forensic footprint identification.
K1030	Knowledge of mobile communications architecture.
K1031	Knowledge of operating system structures and internals.
K1032	Knowledge of network analysis tools used to identify software communications vulnerabilities.
K1033	Knowledge of industry standard security models.
K1034	Knowledge of hacking methodologies.
K1035	Knowledge of engineering concepts as applied to computer architecture and associated computer hardware/software.
K1036	Knowledge of information theory.
K1037	Knowledge of root cause analysis techniques.
K1038	Knowledge of research strategies and knowledge management.
K1039	Knowledge of developing software in high-level languages.
K1040	Knowledge of developing software for UNIX or Linux.
K1041	Knowledge of software integration or testing, including analyzing and implementing test plans and scripts.
K1042	Knowledge of statistical methods.
K1043	Knowledge of natural language processing.

KSA ID	KSA Description
K1044	Knowledge of automated log analysis.
K1045	Knowledge of Machine Learning algorithms.
K1046	Knowledge of how to develop underlying algorithms.
K1047	Knowledge of open-source technologies.
K1500	Knowledge of best practice measures or indicators of system performance and availability.
K1501	Knowledge of best practice resource management principles and techniques.
K1502	Knowledge of best practice server administration and systems engineering theories, concepts and methods.
K1503	Knowledge of server, client and mobile operating systems.
K1504	Knowledge of system software and organizational design standards, techniques and methods.
K1505	Knowledge of best practice technology integration processes where relevant for cybersecurity.
K1506	Knowledge of best practice program management and project management principles and techniques.
K1507	Knowledge of best practice incident response methods, roles and responsibilities.
K1508	Knowledge of current and emerging cybersecurity threats and threat vectors.
K1509	Knowledge of critical IT procurement considerations relating to cybersecurity.
K1510	Knowledge of industry standard continuous monitoring technologies and tools.
K1511	Knowledge of cybersecurity controls related to the use, processing, storage and transmission of data.
K2000	Knowledge of cognitive domains and the tools and methods applicable for learning in each domain.
K2001	Knowledge of virtualization technologies and virtual machine development and maintenance.
K2002	Knowledge of different learning assessment, test and evaluation techniques and how and when to use them.

KSA ID	KSA Description
K2003	Knowledge of developing computer-based training and e-learning courses.
K2004	Knowledge of instructional design and evaluation models.
K2005	Knowledge of training best practices.
K2006	Knowledge of learning levels.
K2007	Knowledge of Learning Management Systems and their use in managing learning.
K2008	Knowledge of learning styles and how to develop training to accommodate them.
K2009	Knowledge of modes of learning.
K2010	Knowledge of organizational training systems.
K2011	Knowledge of the Saudi cybersecurity workforce framework, job roles and associated tasks, knowledge, skills and abilities.
K2012	Knowledge of the uses of written, oral and visual media to support training and techniques for production, communication and dissemination of media.
K2013	Knowledge of the organization's human resource policies, processes and procedures.
K2014	Knowledge the organization's training and education policies, processes and procedures.
K2015	Knowledge of principles and processes for conducting training and education needs assessment.
K2016	Knowledge of concepts, procedures, software, equipment and technology applications relevant to cybersecurity training.
K2017	Knowledge of test and evaluation processes for learners.
K2018	Knowledge of methods for designing curricula, teaching and instruction for individuals and groups.
K2019	Knowledge of external organizations and academic institutions specializing in cybersecurity education and research and development.
K2020	Knowledge of technical delivery options for cybersecurity training and exercising and their limitations.
K2021	Knowledge of how capture the flag and other cybersecurity related exercises and competitions can assist in improving practical skills.

KSA ID	KSA Description
K2500	Knowledge of the organization's local and wide area network connections and the risks they pose to its cybersecurity.
K2501	Knowledge of best practices for reviewing and determining the suitability of technology solutions to meet cybersecurity requirements.
K2502	Knowledge of the organization's enterprise IT architecture and the risks it poses to its cybersecurity.
K2503	Knowledge of strategic theory and practice in relation to cybersecurity.
K2504	Knowledge of all-source reporting and appropriate dissemination procedures.
K2505	Knowledge of best practice auditing and logging procedures.
K2506	Knowledge of formats and best practice for issuing cybersecurity compliance reports to external partners.
K2507	Knowledge of the organization's formats for management and compliance reporting relating to cybersecurity risks, readiness and progress against plans.
K2508	Knowledge of who is developing the organization's strategies, policies and plans are, along with their contact details and their expectations.
K3000	Knowledge of concepts and practices of processing digital forensic data to ensure admissibility of evidence.
K3001	Knowledge of cyber threat intelligence gathering principles, policies and procedures including legal authority and restrictions.
K3002	Knowledge of the organization's policies and standard operating procedures relating to cybersecurity.
K3003	Knowledge of foreign disclosure policies and import/export control regulations in relation to cybersecurity.
K3004	Knowledge of how to produce cybersecurity privacy disclosure statements in line with applicable laws.
K3005	Knowledge of privacy enhancing technologies including their operation and reporting capabilities.
K3006	Knowledge of human-computer interaction and the principles of usable design, as they relate to cybersecurity.
K3500	Knowledge of basic system, network and OS hardening techniques.
K3501	Knowledge of test procedures, principles and methodologies relevant to developing and integrating cybersecurity capability.
K3502	Knowledge of transmission technologies and jamming techniques that enable and prevent transmission of undesirable information or prevent installed systems from operating correctly and the laws relating to their usage.

KSA ID	KSA Description
K3503	Knowledge of network traffic analysis tools, methodologies and processes.
K3504	Knowledge of networking and internet communications fundamentals.
K3505	Know how to analyze infrastructure build sheets, configuration management databases, vulnerability scans, access control lists and vendor documentation to understand software behaviors and interactions.
K4000	Knowledge of remote access technology processes, tools and capabilities and their implications for cybersecurity.
K4001	Knowledge of the capabilities, functionality and cybersecurity risks associated with content creation technologies.
K4002	Knowledge of the capabilities and functionality of collaborative technologies and their implications for cybersecurity.
K4003	Knowledge of import and export regulations related to cryptography.
K4004	Knowledge of taxonomy and semantic ontology theory.
K4005	Knowledge of remote access processes, tools, and capabilities related to customer support.
K4006	Knowledge of how to evaluate supplier and product trustworthiness including use of external sources of advice.
K4007	Knowledge of IT service catalogues.
K4008	Knowledge of developing and applying user credential management system.
K4009	Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.
K4010	Knowledge of confidentiality, integrity and availability principles.
K4011	Knowledge of data concealment techniques and how technologies can apply or counter them.
K4012	Knowledge of data mining techniques.
K4013	Knowledge of asset availability, capabilities and limitations.
K4014	Knowledge of cryptologic capabilities, limitations and contributions to cyber operations.
K4015	Knowledge of encryption algorithms and tools for wireless local area networks.

KSA ID	KSA Description
K4016	Knowledge of identification and reporting processes.
K4017	Knowledge of obfuscation techniques.
K4018	Knowledge of system administration concepts for organization's operating systems.
K4500	Knowledge of hacker methodologies.
K4501	Knowledge of the infrastructure that supports the safety, performance and reliability of IT.
K4502	Knowledge of penetration testing principles, techniques and best practice application.
K4503	Knowledge of computer programming concepts, including computer languages, programming, testing, debugging and file types.
K4504	Knowledge of using programming languages relevant to the systems and infrastructure to be tested.
K4505	Knowledge of using operating systems and their toolsets relevant to the systems being tested.
K4506	Knowledge of how to mimic the attacks a social engineer would use to attempt a system breach.
K4507	Knowledge of encryption cracking tools, password cracking tools and remote access methods.
K4508	Knowledge of using network servers and networking tools used by the organization or systems being tested.
K4509	Knowledge of using and selecting security tools and products.
K4510	Knowledge of using the tools and frameworks that are most readily available to hackers seeking to attack the organization.
K5000	Knowledge of server diagnostic tools and fault identification techniques.
K5001	Knowledge of the main types of electronic device, their vulnerabilities and how they store data.
K5002	Knowledge of file system implementations.
K5003	Knowledge of processes for seizing and preserving digital evidence.
K5004	Knowledge of hacker techniques and tools.

KSA ID	KSA Description
K5005	Knowledge of the investigative techniques required for hardware, operating systems and network technologies.
K5006	Knowledge of applicable laws and the organization's policies and procedures relating to the collection and admissibility of digital evidence.
K5007	Knowledge of processes for collecting, packaging, transporting and storing electronic evidence while maintaining chain of custody.
K5008	Knowledge of types of persistent data and how to collect them.
K5009	Knowledge of tools and techniques for webmail collection, searching and analysis.
K5010	Knowledge of the system files that contain relevant information and where to find them.
K5011	Knowledge of how to conduct deployed forensics operations and the tools that support them.
K5012	Knowledge of web filtering technologies.
K5013	Knowledge of the global social dynamics of the different cyber threat types.
K5014	Knowledge of security event correlation tools.
K5015	Knowledge of electronic evidence law.
K5016	Knowledge of national or applicable judicial and court procedure for cybercrime and fraud cases.
K5017	Knowledge of data carving tools and techniques.
K5018	Knowledge of malware reverse engineering concepts.
K5019	Knowledge of anti-forensics tactics, techniques and procedures.
K5020	Knowledge of forensics lab design configuration and support applications.
K5021	Knowledge of debugging procedures and tools.
K5022	Knowledge of how and why adversaries abuse file type.
K5023	Knowledge of malware analysis tools.

KSA ID	KSA Description
K5024	Knowledge of how malware evades virtual machine detection.
K5025	Knowledge of crisis management protocols, processes and techniques relevant to the organization's cybersecurity.
K5026	Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.
K5027	Knowledge of the judicial process, including the presentation of facts and evidence.
K5028	Knowledge of binary analysis.
K5029	Knowledge of network architecture concepts including topology, protocols and components.
K5030	Knowledge of concepts and practices of processing digital forensic data.
K5031	Knowledge and understanding of operational design.
K5032	Knowledge of statutes, laws, regulations and policies governing the collection of information using cybersecurity techniques.
K5500	Knowledge of concepts, terminology and operations of communications media.
K5501	Knowledge of website types, administration, functions and content management systems.
K5502	Knowledge of attack methods and techniques.
K5503	Knowledge of national and organizational document and information classification and marking standards, policies and procedures.
K5504	Knowledge of common computer and network infections and their methods.
K5505	Knowledge of computer networking fundamentals.
K5506	Knowledge of computer-based intrusion sets.
K5507	Knowledge of cyber threat intelligence sources and their respective capabilities.
K5508	Knowledge of cybersecurity operations concepts, terminology, principles, limitations and effects.
K5509	Knowledge of evolving and emerging communications technologies and their implications for cybersecurity.

KSA ID	KSA Description
K5510	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber-attack, cyber defense), principles, capabilities, limitations, and effects.
K5511	Knowledge of host-based security products and how those products reduce vulnerability to exploitation.
K5512	Knowledge of how internet communications applications work.
K5513	Knowledge of the risks digital telephony networks pose for an organization's cybersecurity.
K5514	Knowledge of the risks wireless networks pose for an organization's cybersecurity.
K5515	Knowledge of how to extract, analyze and use metadata.
K5516	Knowledge of different types of organization, team and people involved in cyber threat intelligence collection.
K5517	Knowledge of how to use cyber threat intelligence to inform the organization's cybersecurity planning.
K5518	Knowledge of how to use cyber threat intelligence to inform the organization's cybersecurity operations.
K5519	Knowledge of the tactics an organization can employ to anticipate and counter an attacker's capabilities and actions.
K5520	Knowledge of Internet network addressing.
K5521	Knowledge of which cyber threat actors are relevant to the organization.
K5522	Knowledge of the threat environment within which the organization is operating.
K5523	Knowledge of malware.
K5524	Knowledge of the organization's leadership, structure and cyber decision-making processes.
K5525	Knowledge of the structure, main capabilities and vulnerabilities of the threat actors relevant to the organization.
K5526	Knowledge of the tactics, techniques and procedures of the threat actors relevant to the organization.
K5527	Knowledge of telecommunications fundamentals.

KSA ID	KSA Description
K5528	Knowledge of the basic structure, architecture and design of modern digital and telephony networks.
K5529	Knowledge of the factors of threat that could impact collection operations.
K5530	Knowledge of how threat actors relevant to the organization use the internet and the targeting information they could learn about the organization from it.
K5531	Knowledge of threat systems.
K5532	Knowledge of virtualization products.
K5533	Knowledge of the basic structure, architecture and design of modern wireless communications systems.
K5534	Knowledge of the political, legal, commercial and other relevant options to use to deter threat actors threatening the organization.
K6000	Knowledge of network hardware devices and functions in IT and ICS/OT environments.
K6001	Knowledge of network technologies in IT and ICS/OT environments.
K6002	Knowledge of the capabilities and limitations of cybersecurity products designed for the IT and ICS/OT environments.
K6003	Knowledge of best practice cybersecurity risk management methodologies for the IT and ICS/OT domains.
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 IT and ICS/OT environments.
K6007	Knowledge of the organization's architectural concepts and patterns in IT and ICS/OT environments.
K6008	Knowledge of integrating the organization's goals and objectives into the system architecture in IT and ICS/OT environments.
K6009	Knowledge of organization's cybersecurity-relevant evaluation and validation criteria relevant to the IT and ICS/OT domains.
K6010	Knowledge of system fault tolerance methodologies in IT and ICS/OT environments.

KSA ID	KSA Description
K6011	Knowledge of demilitarized zones in IT and ICS/OT environments.
K6012	Knowledge of supervisory control and data acquisition system components.
K6013	Knowledge of the structure, architecture and design of modern digital and telephony networks in IT and ICS/OT environments.
K6014	Knowledge of ICS operating environments and functions.
K6015	Knowledge of ICS network architectures and communication protocols.
K6016	Knowledge of ICS devices and industrial programming languages.
K6017	Knowledge of the ICS threat landscape.
K6018	Knowledge of threats and vulnerabilities in ICS systems and environments.
K6019	Knowledge of intrusion detection methodologies and techniques for detecting ICS intrusions.
K6020	Knowledge of ICS security methodologies and technologies.

Table 11: Skills Descriptions

KSA ID	KSA Description
S0001	Skill in effectively conducting vulnerability scans and identifying vulnerabilities in security systems.
S0002	Skill of identifying, capturing, containing and reporting malware.
S0003	Skill in applying and incorporating information technologies into proposed solutions.
S0004	Skill in applying core cybersecurity principles.
S0005	Skill in applying host and network access controls.
S0006	Skill in developing and deploying signatures.
S0007	Skill in designing countermeasures to identified security risks.
S0008	Skill in designing the integration of hardware and software solutions.
S0009	Skill in using intrusion detection technologies to detect host and network-based intrusions.
S0010	Skill in determining the normal operational state for security systems and how that state is affected by change.
S0011	Skill in developing, testing and implementing network infrastructure contingency and recovery plans.
S0012	Skill in evaluating the adequacy of security designs.
S0013	Skill in preserving evidence integrity according to standard operating procedures or national standards.
S0014	Skill in tuning sensors.
S0015	Skill in using protocol analyzers.
S0016	Skill in using virtual private network devices and its encryption.
S0017	Skill in writing code in currently supported programming languages.
S0018	Skill in using scientific rules and methods to solve problems.
S0019	Skill in using virtual machines.
S0020	Skill in conducting forensic analyses in multiple operating system environments.
S0021	Skill in configuring and utilizing computer protection tools.

KSA ID	KSA Description
S0022	Skill in securing network communications.
S0023	Skill in effectively recognizing and categorizing types of vulnerabilities and associated attacks.
S0024	Skill in protecting a network against malware.
S0025	Skill in performing damage assessments.
S0026	Skill in using network analysis tools to identify vulnerabilities.
S0027	Skill in configuring and utilizing network protection components.
S0028	Skill in conducting cybersecurity audits or reviews of technical systems.
S0029	Skill in using binary analysis tools.
S0030	Skill in using one-way hash functions.
S0031	Skill in reading Hexadecimal data.
S0032	Skill in identifying common encoding techniques.
S0033	Skill in reading and interpreting signatures.
S0034	Skill in selecting or developing learning activities to provide the most appropriate material for learners.
S0035	Skill in system, network and OS hardening techniques.
S0036	Skill in designing appropriate cybersecurity test plans.
S0037	Skill in conducting application vulnerability assessments and understanding their results.
S0038	Skill in using public key infrastructure encryption and digital signature capabilities within applications.
S0039	Skill in applying security models.
S0040	Skill in assessing security controls based on cybersecurity principles and tenets.

KSA ID	KSA Description
S0041	Skill in performing packet-level analysis.
S0042	Skill in recognizing vulnerabilities in security systems.
S0043	Skill in configuring and utilizing computer network protection components.
S0044	Skill in performing cybersecurity related impact and risk assessments.
S0045	Skill in applying secure coding techniques effectively.
S0046	Skill in using security event correlation tools effectively.
S0047	Skill in using code analysis tools effectively.
S0048	Skill in effectively performing root cause analysis for cybersecurity issues.
S0049	Skill in safely and effectively conducting research using deep web.
S0050	Skill in effectively performing target system analysis.
S0051	Skill in effectively preparing and presenting briefings in a clear and concise manner.
S0052	Skill in recognizing and interpreting malicious network activity in traffic.
S0053	Skill in malware reverse engineering.
S0054	Skill in analyzing tools, techniques, and procedures used by adversaries remotely to exploit and establish persistence on a target.
S0055	Skill in utilizing feedback to improve cybersecurity processes, products and services.
S0056	Skill in analyzing threat sources of strength and drive.
S0057	Skill in communicating how gaps in knowledge from monitoring or threat intelligence impacts on effectiveness of cybersecurity strategy.
S0058	Skill in effectively communicating with all levels of staff.
S0059	Skill in identifying new cybersecurity threats in a timely manner.

KSA ID	KSA Description
S0060	Skill in responding effectively to cyber incidents in cloud environment.
S0061	Skill in applying cybersecurity and privacy principles to organizational requirements.
S0062	Skill in using risk scoring to inform performance-based and cost-effective approaches to help an organization manage its cybersecurity risk.
S0063	Skill in using cybersecurity service providers effectively as part of the organization's capability.
S0064	Skill in identifying cybersecurity and privacy issues relating to connections with internal and external third parties and their supply chain.
S0065	Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.
S0500	Skill in securing virtual machines.
S0501	Skill in design modeling and building use cases.
S0502	Skill in writing test plans.
S0503	Skill in designing multi-level and cross domain security solutions.
S0504	Skill in the use of design methods.
S0505	Skill in translating operational requirements into protection needs.
S0506	Skill in setting up physical or logical sub-networks that separate trusted and untrusted networks.
S1000	Skill in conducting queries and developing algorithms to analyze data structures.
S1001	Skill in conducting software debugging.
S1002	Skill in creating and utilizing mathematical or statistical models.
S1003	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables and input streams.
S1004	Skill in designing security controls based on cybersecurity principles and tenets.
S1005	Skill in developing data dictionaries.

KSA ID	KSA Description
S1006	Skill in developing data models.
S1007	Skill in developing and applying security system access controls.
S1008	Skill in determining the security control requirements of information systems and networks.
S1009	Skill in generating queries and reports.
S1010	Skill in integrating black box security testing tools into quality assurance process for software releases.
S1011	Skill in assessing the predictive power and subsequent generalizability of a model.
S1012	Skill in data pre-processing.
S1013	Skill in identifying hidden patterns or relationships.
S1014	Skill in performing format conversions to create a standard representation of the data.
S1015	Skill in performing sensitivity analysis.
S1016	Skill in developing semantic ontologies that are understandable by machines.
S1017	Skill in applying regression analysis techniques.
S1018	Skill in applying transformation analysis techniques.
S1019	Skill in using basic descriptive statistics and techniques.
S1020	Skill in using data analysis tools.
S1021	Skill in using data mapping tools.
S1022	Skill in using outlier identification and removal techniques.
S1023	Skill in writing scripts to automate organizational processes.
S1024	Skill in applying the organization's systems engineering process.

KSA ID	KSA Description
S1025	Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.
S1026	Skill in developing applications that can log and handle errors, exceptions and application faults and logging.
S1027	Skill in the use of design modeling.
S1028	Skill in conducting research using all available sources.
S1029	Skill in data mining and analysis techniques.
S1030	Skill in identifying the sources, characteristics and uses of the organization's data assets.
S1031	Skill in designing and developing object-oriented systems.
S1032	Skill in using version control systems.
S1033	Skill in activity modeling for knowledge capture.
S1034	Skill in designing and developing automated analytic software, techniques and algorithms.
S1035	Skill in carrying out research.
S1036	Skill in using machine learning frameworks.
S1037	Skill in using quantitative programming languages for database queries, data modeling and visualization tools.
S1500	Skill in developing policies which reflect the organization's business and cybersecurity strategic objectives.
S1501	Skill in evaluating the viability and legitimacy of suppliers and products.
S1502	Skill in continually identifying new technologies and their potential impact on cybersecurity requirements.
S1503	Skill in using critical thinking to recognize organizational challenges and relationships.
S2000	Skill in analyzing network traffic capacity and performance characteristics.
S2001	Skill in using knowledge management technologies.

KSA ID	KSA Description
S2002	Skill in using network management tools to analyze network traffic patterns.
S2003	Skill in developing and executing technical training programs and curricula.
S2004	Skill in identifying gaps in technical capabilities.
S2005	Skill in talking to others to convey information effectively.
S2006	Skill in utilizing technologies for instructional purposes.
S2007	Skill in developing technical delivery capabilities through training and exercising.
S2008	Skill in developing workforce specialty and role qualification standards.
S2009	Skill in identifying gaps in technical delivery capabilities.
S2010	Skill in writing about facts and ideas in a clear, convincing and organized manner.
S2500	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance as necessary.
S2501	Skill in applying appropriate cybersecurity controls.
S2502	Skill in identifying test and evaluation infrastructure requirements.
S2503	Skill in communicating with customers.
S2504	Skill in managing test assets and resources to ensure effective completion of test events.
S2505	Skill in preparing test and evaluation reports.
S2506	Skill in reviewing logs to identify evidence of intrusions and other suspicious behavior.
S2507	Skill in troubleshooting and diagnosing cybersecurity defense infrastructure anomalies and determining the root cause.
S2508	Skill in using HR IT systems.

KSA ID	KSA Description
S2509	Skill in conducting cybersecurity reviews of systems.
S2510	Skill in understanding network systems management principles, models, methods and tools.
S2511	Skill in assessing cybersecurity systems designs.
S2512	Skill in developing, deploying and integrating policies that meet organizational system cybersecurity objectives.
S2513	Skill in planning and carrying out administrative activities relating to cybersecurity.
S2514	Skill in analyzing an organization's communication networks through the eyes of an attacker.
S2515	Skill in analyzing traffic to identify network devices.
S2516	Skill in auditing firewalls, routers and intrusion detection systems.
S2517	Skill in identifying gaps and limitations in cyber threat intelligence provision.
S2518	Skill in identifying cybersecurity issues that may have an impact on the organization's objectives.
S2519	Skill in identifying potential leads that may assist in a cybercrime investigation.
S2520	Skill in identifying threats' regional languages and dialects.
S2521	Skill in identifying devices that work at each level of protocol models.
S2522	Skill in using geospatial analysis techniques to identify and locate threats' sources.
S2523	Skill in prioritizing information during a cybersecurity operation.
S2524	Skill in interpreting compiled and interpretive programming languages.
S2525	Skill in effectively and efficiently interpreting metadata.
S2526	Skill in effectively and efficiently interpreting the results from network analysis and reconstruction tools.
S2527	Skill in interpreting vulnerability scan results to identify vulnerabilities and their levels of criticality in relation to the organization.

KSA ID	KSA Description
S2528	Skill in knowledge management, including technical documentation techniques.
S2529	Skill in managing client relationships.
S2530	Skill in preparing plans and related documentation.
S2531	Skill in prioritizing foreign language material provided or obtained in support of a cyber investigation.
S2532	Skill in identifying and processing data for further analysis.
S2533	Skill in analyzing reports and recommending actions to be taken.
S2534	Skill in reviewing and editing cybersecurity assessment products.
S2535	Skill in reviewing and editing cybersecurity related plans.
S2536	Skill in tailoring analysis to the necessary levels based on organizational policies on data-handling and classification and distribution of sensitive material.
S2537	Skill in threat intelligence collecting operations.
S2538	Skill in identifying a network anomaly.
S2539	Skill in writing clear and concise technical documentation.
S2540	Skill in accessing information relating to current internal and external cybersecurity resources and their current utilization and priorities.
S2541	Skill in accessing databases where required documentation is maintained.
S2542	Skill in reviewing corporate strategies or applicable legal, regulatory or policy documents to identify issues requiring clarification or action.
S2543	Skill in developing appropriate and effective requirements to inform selection of cyber threat intelligence sources or monitoring activity.
S2544	Skill in interpreting readiness reporting, its operational relevance and intelligence collection impact.
S2545	Skill in preparing clear and concise reports, presentations and briefings.

KSA ID	KSA Description
S2546	Skill in analyzing and assessing reporting from internal and external partners.
S3000	Skill in creating and maintaining cybersecurity policies aligned with the organization's privacy objectives.
S3001	Skill in negotiating vendor agreements.
S3002	Skill in evaluating vendor privacy practices.
S3500	Skill in using incident handling methodologies.
S3501	Skill in collecting data from a variety of cybersecurity resources.
S3502	Skill in conducting trend analysis.
S4000	Skill in conducting information searches.
S4001	Skill in assessing the application of cryptographic standards.
S4002	Skill in analyzing cipher strength and breaking ciphers.
S4003	Skill in applying cryptography algorithms and techniques to protect data, systems and networks.
S4500	Skill in assessing the robustness of security systems and designs.
S4501	Skill in developing operations-based testing scenarios.
S4502	Skill in mimicking threat behaviors.
S4503	Skill in testing the security of integrated systems.
S4504	Skill in the use of penetration testing tools and techniques.
S4505	Skill in the use of social engineering techniques.
S4506	Skill in implementing and testing network infrastructure business continuity and disaster recovery plans.
S4507	Skill to develop insights about an organization's threat environment.

KSA ID	KSA Description
S4508	Skill in using tools, techniques and procedures to remotely exploit and establish persistence on a target.
S4509	Skill in writing custom code to bypass security controls.
S4510	Skill in implementing adversary Tactics, Techniques and Procedures.
S4511	Skill to carry out attack and defense operations for the purpose of exercises and vulnerability assessment and detection.
S5000	Skill in analyzing memory dumps to extract information.
S5001	Skill in identifying and extracting data of forensic interest in diverse media.
S5002	Skill in identifying, modifying and manipulating applicable operating system components.
S5003	Skill in collecting, processing, packaging, transporting and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.
S5004	Skill in setting up a forensic workstation.
S5005	Skill in using forensic tool suites.
S5006	Skill in physically disassembling PCs.
S5007	Skill in deep analysis of captured malicious code.
S5008	Skill in determining if anomalous code is malicious or benign.
S5009	Skill in analyzing volatile data.
S5010	Skill in identifying obfuscation techniques.
S5011	Skill in interpreting debugger results to ascertain attacker's tactics, techniques and procedures.
S5012	Skill in analyzing malware.
S5013	Skill in conducting bit-level analysis.
S5014	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.

KSA ID	KSA Description
S5015	Skill in C, low-level assembly and Linux kernel.
S5016	Skill in script-based languages.
S5017	Skill in reverse engineering to identify function and ownership of remote tools.
S5500	Skill in conducting non-attributable research.
S5501	Skill in defining and characterizing aspects of the operational environment relevant to its cybersecurity strategy.
S5502	Skill in developing or recommending analytic approaches in situations where information is incomplete or for which no precedent exists.
S5503	Skill in evaluating potential sources of information for their value to a cyber investigation.
S5504	Skill in evaluating information for reliability, validity and relevance.
S5505	Skill in determining relevance, priority and urgency of information.
S5506	Skill in identifying a network's characteristics when viewed through the eyes of an attacker.
S5507	Skill in identifying alternative analytical interpretations to minimize unanticipated outcomes.
S5508	Skill in identifying critical threat elements.
S5509	Skill in identifying cyber threats which may jeopardize the organization or its stakeholders' interests.
S5510	Skill in identifying and analyzing physical, functional, or behavioral relationships to develop understanding of attackers and their objectives.
S5511	Skill in recognizing denial and deception techniques when used by attackers or cybercriminals.
S5512	Skill in recognizing opportunities and information that will assist in developing a cyber strategy or investigation.
S5513	Skill in recognizing relevance of information to a cybersecurity strategy or investigation.
S5514	Skill in recognizing significant changes in an attacker or suspected cyber-criminal's communication patterns.

KSA ID	KSA Description
S5515	Skill in reviewing and editing cyber threat intelligence products from various sources to support decision-making on cybersecurity matters.
S5516	Skill in constructing simple and complex queries.
S5517	Skill in using multiple analytic tools, databases and techniques.
S5518	Skill in using multiple search engines and tools in conducting open-source searches.
S5519	Skill in using network analysis and reconstruction tools and interpreting their results.
S5520	Skill in utilizing virtual collaborative workspaces and tools in line with organizational cybersecurity policies.
S5521	Skill in writing, reviewing and editing cybersecurity assessment products using information derived from multiple sources.
S5522	Skill in prioritizing filling an organization's knowledge gaps in line with its cybersecurity strategy, vulnerabilities and main threats.
S5523	Skill to monitor a threat or vulnerability situation and environmental factors.
S5524	Skill in accurately assessing the implication of successful attacks on third parties including suppliers and others with similar environments or cybersecurity solutions.
S6000	Skill in design modeling and building use cases in IT and ICS/OT environments.
S6001	Skill in writing test plans for IT and ICS/OT environments.
S6002	Skill in designing multi-level and cross domain security solutions applicable to IT and ICS/OT environments.
S6003	Skill in the use of design methods in an IT and ICS/OT environments.
S6004	Skill in translating operational requirements into protection needs in an IT and ICS/OT environments.
S6005	Skill in setting up physical or logical sub-networks that separate trusted and untrusted networks in IT and ICS/OT environments..
S6006	Skill in assessing the cybersecurity controls of ICS/OT environments.
S6007	Skill in protecting an ICS/OT environment against cyber threats.

Table 12: Abilities Descriptions

KSA ID	KSA Description
A0001	Ability to analyze vulnerability and configuration data to identify cybersecurity issues.
A0002	Ability to communicate cybersecurity concepts and practices in an effective manner.
A0003	Ability to conduct vulnerability scans and determine vulnerabilities from the results.
A0004	Ability to prepare and present cybersecurity briefings to management and other staff.
A0005	Ability to produce technical documentation at an appropriate level for the audience.
A0006	Ability to develop strategy, policy and related documentation to support business strategy and maintain compliance with legislative, regulatory and contractual obligations.
A0007	Ability to develop, update and maintain cybersecurity related documentation.
A0008	Ability to identify basic and common cybersecurity related coding flaws at a high level.
A0009	Ability to apply network security architecture concepts including topology, protocols, components and principles.
A0010	Ability to apply secure system design tools, methods and techniques.
A0011	Ability to apply automated systems analysis and design tools.
A0012	Ability to ensure cybersecurity practices are applied at all stages in the acquisition or divestment process.
A0013	Ability to design architectures and frameworks in line with security policies.
A0014	Ability to source all data used in intelligence, assessment and planning activities.
A0015	Ability to demonstrate critical comprehension of documentation.
A0016	Ability to determine whether information is reliable, valid and relevant.
A0017	Ability to use experience to understand poorly written policies.
A0018	Ability to focus research efforts to address cybersecurity requirements and meet the organization's decision-making needs.
A0019	Ability to function in a collaborative environment to leverage analytical and technical expertise.
A0020	Ability to identify gaps in threat intelligence and other cybersecurity information gathering.
A0021	Ability to understand and relate legislative, regulatory and contractual requirements to the cybersecurity objectives of the organization.
A0022	Ability to recognize and mitigate deception in information obtained and provide appropriate reporting and analysis.
A0023	Ability to select appropriate mitigation techniques within the organization's goals and policies.

KSA ID	KSA Description
A0024	Ability to communicate technical and planning information at the same level as a stakeholder's understanding.
A0025	Ability to apply critical thinking.
A0026	Ability to use awareness of changes to information privacy laws to influence organizational adaptation and compliance.
A0027	Ability to maintain awareness of changes to information privacy technologies to influence organizational adaptation and compliance.
A0028	Ability to develop, identify or procure relevant training that delivers a topic at the appropriate level for the trainee.
A0029	Ability to effectively and efficiently prioritize cybersecurity resources.
A0030	Ability to align business and security strategies for the benefit of the organization.
A0031	Ability to recognize organizational challenges from a business, management and technological perspective.
A0032	Ability to relate basic cybersecurity concepts to the impact they may have on an organization.
A0033	Ability to effectively communicate insights relating to an organization's threat environment to improve its risk management posture.
A0034	Ability to assess and respond effectively to cyber incidents in cloud environment.
A0035	Ability to apply cybersecurity and privacy principles to organizational requirements.
A0036	Ability to use intrusion detection technologies to detect host-based and network-based intrusions.
A0037	Ability to work with the organization's leadership to provide a comprehensive, organization-wide approach to address cybersecurity risk.
A0038	Ability to work with the organization's leadership to develop a risk management strategy to address cybersecurity related risks.
A0039	Ability to work with the organization's leadership to share cybersecurity risk related information.
A0040	Ability to work with the organization's leadership to provide oversight for all cybersecurity risk management related activities.

KSA ID	KSA Description
A0041	Ability to bring required stakeholders into an organization-wide group to consider all cyber risks which may affect the organization.
A0042	Ability to work with the organization's leadership to determine the organization's risk posture based on the aggregated risk from its operations and its use of systems.
A0043	Ability to work with cybersecurity staff to provide effective advice and guidance to the organization's leadership on a range of cybersecurity matters.
A0044	Ability to identify critical information systems which have limited technical cybersecurity controls.
A0045	Ability to recognize how changes to systems, environment or cybersecurity controls change residual risks in relation to risk appetite.
A0046	Ability to perform advanced analysis and reverse engineering of suspect source code.
A0500	Ability to apply the organization's chosen framework for describing, analyzing and documenting its IT architecture.
A0501	Ability to employ best practice when implementing cybersecurity controls within a system.
A0502	Ability to develop and maintain architecture to support an organization's goals and objectives.
A0503	Ability to optimize systems to meet enterprise performance requirements.
A0504	Ability to work with enterprise architects, systems security engineers, system owners, control owners and system security officers to apply security controls as system specific, hybrid, or common controls.
A1000	Ability to tailor code analysis to assess application-specific concerns.
A1001	Ability to use and understand complex mathematical concepts.
A1002	Ability to build complex data structures and high-level programming languages.
A1003	Ability to use data visualization tools.
A1004	Ability to develop secure software according to secure software deployment methodologies, tools and practices.
A1005	Ability to collaborate effectively with others.
A1006	Ability to develop statistical and machine learning models.

KSA ID	KSA Description
A1007	Ability to develop algorithms to analyze text data.
A1008	Ability to design and develop object-oriented systems.
A1500	Ability to integrate cybersecurity management with strategic business and operational processes.
A1501	Ability to engage with the organization's leadership to ensure cybersecurity controls are applied in their areas of responsibility.
A1502	Ability to integrate cybersecurity requirements into procurement processes.
A2000	Ability to develop a curriculum that teaches cybersecurity topic at the appropriate level for the target audience.
A2001	Ability to prepare and deliver training to ensure that users understand why they should adhere to systems security policies and procedures.
A2002	Ability to gauge the understanding and knowledge level of trainees.
A2003	Ability to provide effective feedback to trainees to improve their learning.
A2004	Ability to apply principles of adult learning.
A2005	Ability to develop clear, concise and effective instructional materials.
A2006	Ability to assess and forecast staffing requirements to meet organizational objectives.
A2007	Ability to develop a curriculum for use within a virtual environment.
A2008	Ability to develop career paths relevant to organizational needs.
A2009	Ability to determine the validity of workforce trend data.
A2010	Ability to design training in line with organizational standards and policies.
A2011	Ability to operate common network tools.
A2012	Ability to tailor curriculum that covers cybersecurity topics at the appropriate level for the target audience.
A2013	Ability to execute OS command line.

KSA ID	KSA Description
A2014	Ability to operate different electronic communication systems and methods.
A2015	Ability to conduct training and education needs assessment.
A2500	Ability to determine and understand the validity of technology trend data.
A2501	Ability to implement supply chain risk management standards.
A2502	Ability to answer cybersecurity related questions in a clear and concise manner.
A2503	Ability to ask questions for clarification of cybersecurity matters.
A2504	Ability to communicate cybersecurity related material clearly and concisely when writing.
A2505	Ability to effectively and efficiently facilitate small group discussions.
A2506	Ability to design valid cybersecurity assessments.
A2507	Ability to competently analyze cybersecurity related test data.
A2508	Ability to collect, verify and validate cybersecurity related test data.
A2509	Ability to identify relationships between two or more cybersecurity related data sources that may initially appear unrelated.
A2510	Ability to leverage cybersecurity best practices from external organizations when dealing with cybersecurity incidents.
A2511	Ability to determine relevance and meaning of data and cybersecurity test results.
A2512	Ability to collaborate effectively with colleagues, partners and suppliers.
A2513	Ability to collaborate effectively within virtual teams and matrix management.
A2514	Ability to evaluate, analyze and synthesize large quantities of data into high quality, fused reports.
A2515	Ability to target and expand network access by conducting appropriate analysis and collection of relevant data.
A2516	Ability to function effectively in a dynamic, fast-paced environment which changes frequently.

KSA ID	KSA Description
A2517	Ability to identify external partners with common cybersecurity interests.
A2518	Ability to identify and describe an organization's cybersecurity vulnerabilities.
A2519	Ability to determine tools and methods through which an organization's vulnerabilities could be exploited.
A2520	Ability to interpret and translate stakeholder cybersecurity requirements into operational controls and actions.
A2521	Ability to interpret and understand complex and rapidly evolving environments.
A2522	Ability to participate as a member of virtual teams as necessary.
A2523	Ability to recognize and mitigate against cognitive biases which may adversely impact analysis.
A2524	Ability to understand organizational objectives and the effects of cybersecurity controls on those objectives.
A2525	Ability to utilize multiple information sources to inform cybersecurity related actions.
A2526	Ability to work across departments and business units to implement an organization's privacy principles and programs.
A2527	Ability to work across departments and business units to ensure an organization's privacy and cybersecurity objectives are aligned.
A2528	Ability to ensure cybersecurity related activities are reported to appropriate stakeholders within an organization.
A2529	Ability to recognize and explain the importance of auditing the application of cybersecurity policies.
A2530	Ability to effectively communicate complex technical problems from a cybersecurity perspective.
A3000	Ability to monitor and assess the potential impact of emerging technologies on legislation, regulations and cybersecurity policies and related documentation.
A3001	Ability to determine whether a cybersecurity incident violates a privacy principle or law which would require specific legal action.
A3002	Ability to author an appropriate privacy disclosure statement based on current laws.
A3500	Ability to analyze malware.

KSA ID	KSA Description
A3501	Ability to interpret the information collected by network tools.
A4000	Ability to perform network collection tactics, techniques and procedures.
A4001	Ability to perform wireless collection procedures.
A4002	Ability to ensure operational cybersecurity decisions taken by the organization's leadership take all known factors into account to ensure success.
A4003	Ability to ensure all relevant stakeholders are involved when an organization's leadership takes operational cybersecurity decisions.
A4500	Ability to apply programming language structures, including source code review and logic.
A4501	Ability to tailor a penetration test or vulnerability assessment according to an organization's role, operations, architecture and threats.
A4502	Ability to solve complex technical problems and articulate to non-IT personnel.
A4503	Ability to effectively provide technical risk assessment of all technologies used by the organization being assessed or tested.
A4504	Ability to conduct penetration testing in line with the organization's policies and best practice.
A4505	Ability to write technical reports that include an operational risk assessment and suggested resolution for identified problem areas.
A5000	Ability to decrypt digital data collections.
A5001	Ability to conduct forensic analysis in and for all operating systems used by an organization.
A5002	Ability to find and navigate the dark web to locate markets and forums.
A5003	Ability to examine digital media on all operating system platforms used by an organization.
A5004	Ability to read and understand assembly code.
A5500	Ability to clearly articulate cyber threat intelligence requirements into well-formulated research questions and data tracking variables for inquiry tracking purposes.
A5501	Ability to develop analytic approaches and solutions to problems where information is incomplete, or no precedent exists.

KSA ID	KSA Description
A5502	Ability to think like threat actors.
A6000	Ability to develop and maintain architecture to support an organization's goals and objectives in IT and ICS/OT environments.
A6001	Ability to optimize systems to meet enterprise performance requirements in IT and ICS/OT environments.
A6002	Ability to work with enterprise architects, systems security engineers, system owners, control owners and system security officers to apply security controls as system-specific, hybrid, or common controls in IT and ICS/OT environments.
A6003	Ability to set up physical or logical sub-networks that separates trusted and untrusted networks in IT and ICS/OT environments.
A6004	Ability to apply techniques and tools for protecting systems and networks against cyber threats in IT and ICS/OT environments.
A6005	Ability to apply techniques and tools for detecting intrusions in IT and ICS/OT environments.
A6006	Ability to apply techniques and tools for responding to incidents in IT and ICS/OT environments.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority