الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

The Saudi Cybersecurity Workforce Framework- Career Progression

(SCyWF-CP – 1: 2026)

TLP: Clear

Document Classification: Public

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

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

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

`

Traffic Light Protocol (TLP):

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

Red (Personal, Confidential, and for the Intended Recipient Only)
The recipient has no right to share the information classified in red with any person outside the defined range of recipients, either inside or outside the entity, beyond the scope specified for receipt.

Amber+ Strict (Sharing within the entity)
The recipient may share the information only with the intended recipients inside the entity.

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

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

Clear (No Restrictions)

Table of Contents

List of Figures

List of Tables

1. Introduction

The Saudi National Cybersecurity Authority (NCA) is leading the national effort to protect the country's cyber space. This mission requires a qualified national cybersecurity workforce capable of carrying out all types of cybersecurity work. The NCA's mandate was issued by Royal Order number 6801, dated October 31, 2017. It includes building 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. This document, the Saudi Cybersecurity Workforce Framework - Career Progression (SCyWF-CP), is an Appendix of the SCyWF 1.5 document and has been developed by the NCA to extend the Saudi Cybersecurity Workforce Framework (SCyWF). It defines structured pathways for career progression within cybersecurity roles, supporting the NCA's mandate to cultivate a skilled and capable national cybersecurity workforce.

1.1 Purpose

This document defines the promotion and progression pathways within cybersecurity job roles outlined in the Saudi Cybersecurity Workforce Framework (SCyWF). It builds on the SCyWF by detailing the required qualifications, experience, and career pathways while supporting national efforts to develop a robust cybersecurity workforce. For each level, it defines the required skill proficiency levels, educational qualifications, and experience needed. By linking roles to clear career pathways, this document ensures professionals can effectively grow their skills while addressing evolving cybersecurity challenges. Additionally, it provides an indication of possible roles an individual can pursue as they progress through their career.

1.2 Goals

The goal of this document is to establish minimum requirements and provide clear pathways for career progression within cybersecurity roles. Specifically, it aims to:

- Develop a dynamic framework to identify, recruit, and nurture cybersecurity talent by detailing job role levels, entry requirements, progression pathways, and proficiency expectations to align workforce development with the job expectations at different career levels.
- Develop and improve cybersecurity educational programs by providing a standardized terminology for academic institutions.
- Establish a standard to define and align cybersecurity roles, ensuring clarity in tasks, skills, and training requirements.
- Support alignment with national workforce objectives by offering structured pathways for talent development, helping professionals understand how to advance their positions or transition to new roles in their cybersecurity careers.

1.3 Scope of Applicability

This document complements the Saudi Cybersecurity Workforce Framework (SCyWF) by providing practical pathways for career progression within cybersecurity roles. It serves as a resource to guide individuals and organizations in aligning talent development with national cybersecurity goals. In addition, organizations can customize this framework to address their requirements. The SCyWF-CP applies to:

1. **Future cybersecurity professionals** seeking to understand the qualifications and requirements for entering and growing within the cybersecurity profession.
2. **Current cybersecurity professionals** aiming to develop their skills, gain proficiency, and progress through defined career pathways.
3. **Cybersecurity employers and educators** responsible for building a skilled workforce by aligning talent development strategies with organizational and national cybersecurity objectives.

1.4 Relationship with Other NCA publications

The SCyWF and its related documents (of which this Saudi Cybersecurity Workforce Framework - Career Progression (SCyWF-CP) is one) have been developed in alignment with international standards, frameworks and practice and are aligned with all relevant Saudi Arabian Laws and requirements such as but not limited to the Essential Cybersecurity Controls and the Data Cybersecurity Controls[1].

This document's approach to years of experience required at each level takes into account both user requirements and the minimum experience levels required for internationally recognized and frequently mandated certifications. The SCyWF-CP approach is aligned with the Job Classification Guide[2] by the Ministry of Human Resources and Social Development to ensure consistency in the way job levels were defined. Similarly, the approach to defining educational qualification requirements is aligned with the Saudi Cybersecurity Higher Education Framework (SCyber-Edu)[3].

1 See Essential Cybersecurity Controls (ECC – 2: 2024), 2024, https://nca.gov.sa/pages/legislation.html; and Data Cybersecurity Controls (DCC), https://nca.gov.sa/pages/legislation.html.

2 See the Job Classification Guide, MHRSD, https://eservices.masar.sa/UCG/

3 See The Saudi Cybersecurity Higher Education Framework (SCyber-Edu – 1: 2020), 2020, https://nca.gov.sa/ar/scyberedu_en.pdf

1.5 Minimum Academic Qualifications

Some roles accept entry-level candidates with an intermediate diploma or bachelor's degree, whereas others may require advanced qualifications, up to a doctoral degree. The table below shows the minimum academic qualifications, aligned with the Cyber-Edu framework.

Rank1	
QR1	An Intermediate Diploma in Cybersecurity or relevant diploma that covers the required knowledge units and required skills.
QR2	A bachelor's degree in Cybersecurity or in closely related fields such as Computer Science, Information Systems, Information Technology, Computer Engineering, Software Engineering or relevant bachelor's degree with Cybersecurity track that satisfy the required knowledge units1.
QR3	A previous qualification as QR2 and a high diploma in Cybersecurity or similarly relevant diploma that covers the required knowledge units1.
QR4	A previous qualification as QR2 and a master's degree in Cybersecurity or similarly relevant degree that covers the required knowledge units1.
QR5	A previous qualification as QR3 or QR4, and a Doctoral degree in Cybersecurity that covers the required knowledge in depth or relevant experience in the field.

TABLE 1: DEFINITION OF ACADEMIC QUALIFICATIONS AND THEIR RANKINGS

[1] QR = Qualification Rank

1.6 Job Role Levels

Each job role will have one or more levels. These levels are broadly defined in Table 2 below.

Role Level	Description
Level 1	Entry level role, usually described as a junior with a degree or relevant diploma (see Table 1), works as a trainee, team support or junior team member under close supervision of a practitioner, while developing the necessary skills to become a Practitioner.
Level 2	Carries out the core tasks of the job role effectively with minimum supervision. Can mentor or manage a junior team member.
Level 3	Carries out the core tasks at a larger scale or in more complex environments, as well as tasks which require more experience, and which can be more niche than those carried out by Level 2 staff. Can supervise, manage and mentor practitioners or teams of practitioners carrying out the core tasks of the job role. Can deputize for experts and may act as the team subject matter expert in some knowledge and skills areas.
Level 4	Carries out highly specialized, large scale, or complex tasks which require much higher levels of skill and experience relevant to the job role than is likely to be present in lower levels. May lead a team of Senior Practitioners and/or Practitioners. At this level, staff with strong management competencies may lead the team while others may act as the organization's subject matter experts on a range of skill and knowledge areas relevant to the job role. Staff members at this level are likely to represent the organization and present on behalf of the organization at external events.
Level 5	Fills, for example, Chief Information Security Officer/Director (CISO), Senior Cybersecurity Manager, Cybersecurity Advisor or Fellow roles in the largest and most complex organizations. At this level individuals may lead very large teams and bring very deep experience acquired over many years of work as a cybersecurity professional to develop organizational or national cybersecurity strategies and programs. Staff members at this level are likely to represent the organization and present on behalf of the organization at external events.

TABLE 2: DESCRIPTION OF JOB ROLE LEVELS

There are some additional terms which are used in the document but not mentioned in Table 2 above. Table 3 below describes some of these terms.

Term	Description
QR1 Entry Level Graduate	Graduates holding **QR1** qualifications (see Table 1) can typically enter a cybersecurity role at **Level 1**. They have **foundational** knowledge but may have limited practical experience, so they begin in an entry-level capacity. Over time, as they gain relevant cybersecurity experience (see Table 5), they may be eligible to advance to higher levels
QR2 Entry Level Graduate	Graduates with **QR2** qualifications (see Table 1) qualify for **Level 2** positions, provided they also possess relevant cybersecurity experience or equivalent higher qualifications (e.g., QR3, QR4, or QR5). Those aiming for **Level 3** roles should not only meet the QR2 minimum but also demonstrate more extensive experience (see Table 5). This combination of qualifications and experience positions them for mid-level cybersecurity responsibilities.
Other HR or Admin Role	The skills required for these roles fall out of the scope of this document because, unless indicated otherwise, most are related to organizational and administrative skills coupled with varying levels of capability in Human Capital Management. These will require the same abilities at each level as defined in Table 2.
Cybersecurity Technical Roles	This relates to any role within the Cybersecurity, Architecture and Research and Development (CARD), and Protection and Defense (PD) categories and Operational Technology (ICS/OT) job roles except for the ICS/OT Cybersecurity Risk Officer.
Core Cybersecurity Roles	This description applies to any role with the exception of the Cybersecurity Human Capital Manager and Cybersecurity Legal Specialist roles, because those two roles do not have any specific cybersecurity-related skills associated with them.

TABLE 3: DESCRIPTIONS OF ADDITIONAL TERMS

1.7 The Saudi Cybersecurity Workforce Framework Taxonomy

Figure 1 below shows the identified Categories, Specialties and Roles related to cybersecurity in the SCyWF by the NCA. These are referred to in the remainder of the document.

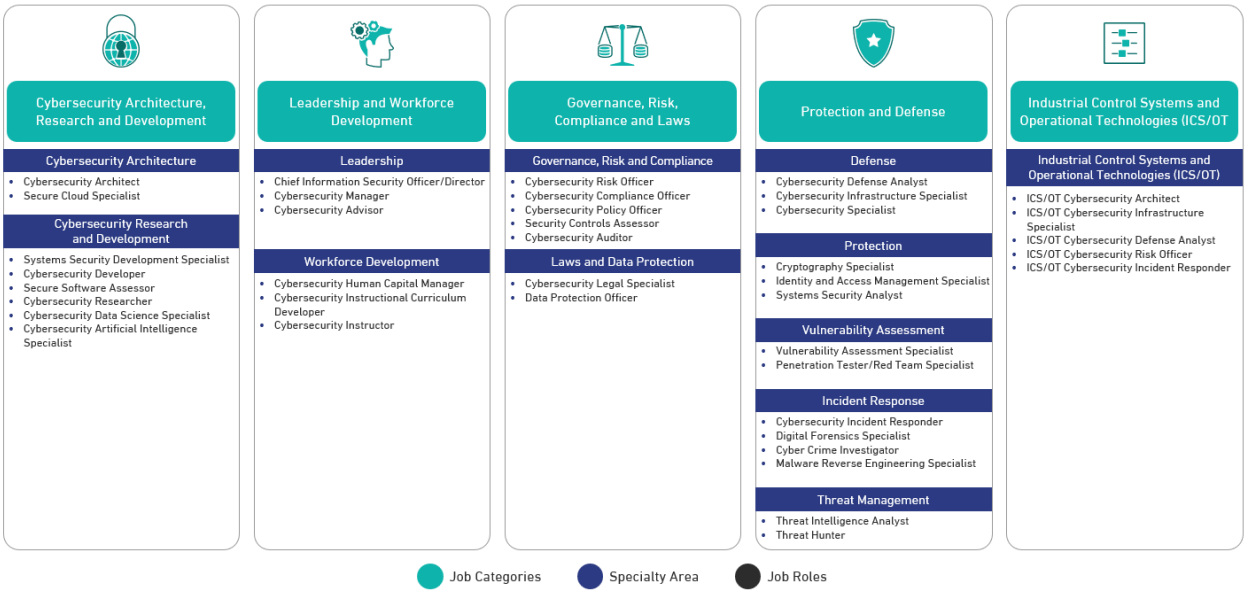

FIGURE 1: THE SAUDI CYBERSECURITY WORKFORCE FRAMEWORK

The job roles, specialty areas and categories are defined in SCyWF as follows:

- A *job role* is a set of cybersecurity tasks that need to be performed in a cybersecurity job. A job role is defined by a set of tasks to be performed within that job role and a list of Knowledge and Skills (KSs) required to perform those tasks.
- A *specialty area* is a group of related job roles that serve a cybersecurity function.
- A *category* is a group of related specialty areas and the job roles associated with them, that serve related cybersecurity functions.

1.8 Education, Experience, and Skill proficiency

Table 4 below outlines the required academic qualification for each job role level. It also explains that having an academic qualification that is higher than the minimum qualification requirement of a job role level could always be used as equivalent to some years of experience required at that level. In addition, Table 4 shows that education requirements for job roles from level 2 to level 5 are identical.

Role Level	Education Requirements
Level 1	The minimum educational qualification is QR1 (as described in Table 1). However, a QR2 qualification or higher can be used as an equivalent to some of the years of experience required for the level.
Level 2	The minimum educational qualification is QR2 (as described in Table 1). However, a QR3 qualification or higher can be used as an equivalent to some of the years of experience required for the level.
Level 3	The minimum educational qualification is QR2 (as described in Table 1). However, a QR3 qualification or higher can be used as an equivalent to some of the years of experience required for the level.
Level 4	The minimum educational qualification is QR2 (as described in Table 1). However, a QR3 qualification or higher can be used as an equivalent to some of the years of experience required for the level.
Level 5	The minimum educational qualification is QR2 (as described in Table 1). However, a QR3 qualification or higher can be used as an equivalent to some of the years of experience required for the level.

TABLE 4: JOB ROLE LEVELS EDUCATION REQUIREMENTS

Role Level	Minimum Years in Cybersecurity Profession	Typical no. of years spent at this level	Required skill proficiency level
Level 1	0	1 - 3	Foundational
Level 2	1	3 - 5	Foundational
Level 3	4	6 - 10	Intermediate
Level 4	10	5 - rest of career	Advanced
Level 5	15+	Rest of career	Advanced

TABLE 5: DESCRIPTION OF EXPERIENCE REQUIRED

Table 5 provides guidance on the minimum number of years' experience required at each role level that an individual would be expected to have gained in cybersecurity roles (as defined in the SCyWF) before being eligible for promotion or appointment to a job role at this level. Fresh graduates or staff changing careers with no experience in a cybersecurity job role can be appointed to Level 1 roles. A staff member would be expected to have at least 10 years' experience in cybersecurity job roles defined in the SCyWF before being eligible for a Level 4 role.

It also provides guidance on the typical number of years that a cybersecurity professional will spend at each level. A Level 1 joins with 0 years' experience and then typically spends one to three years at that level. Some may be promoted to Level 2 after one year, while others may take three years before they are promoted. Once at Level 2, they will typically spend between three and five years at that level. Most cybersecurity professionals spend most of their time working at Level 2 and Level 3 – up to 15 years (5 at Level 2, 10 at Level 3) as shown in this table – as these are the levels where most cybersecurity jobs are available and where they are usually most valuable to their organization. The vast majority of professionals are promoted to Level 4 after a minimum of 10 years, or a more likely 15 to 17 years in the profession, and then spend the rest of their career at Level 4.

It also provides the skill proficiency level required for each role, as described in Table 6 below. At Levels 1 and 2, individuals are expected to exhibit foundational proficiency, which involves a basic understanding of cybersecurity concepts and the ability to handle routine tasks under close supervision. At Level 3, intermediate proficiency is required, allowing individuals to independently manage both routine and moderately complex tasks with minimal supervision. At Levels 4 and 5, advanced proficiency is critical, requiring deep expertise, leadership capabilities, and the ability to manage complex challenges while providing strategic guidance with little to no supervision. In addition, organizations can use Table 6 to develop detailed matrices to measure the skill proficiency level.

Skill Proficiency Level	Description
Foundational	Skills are performed at basic level to perform routine tasks under close supervision
Intermediate	Skills are performed at moderate level to handle moderately complex tasks with minimum supervision
Advanced	Skills are performed at expert level to manage complex situation and provide strategic guidance with little or no supervision

TABLE 6: DESCRIPTION OF SKILL PROFICIENCY LEVELS

1.9 Rationale for lateral job role transitions

The lateral transitions outlined in this document (sections 2.1 onwards) were determined through insights from cybersecurity experts who observe how professionals realistically shift between roles. This practical perspective ensures the framework reflects genuine career pathways, rather than purely theoretical progressions. In addition, most of these lateral movements occur between roles that share some TKS similarity, making it more straightforward for professionals to adapt and succeed when changing job functions. For example, a Cybersecurity Defense Analyst can laterally transition into a Vulnerability Assessment Specialist role, as both share strong overlaps in threat detection, risk analysis, and security assessment TKS

1.10 Key for Roles

The following sections include career path maps for each role. To aid with the concepts, these have been color coded with the lightest colors at the lowest level roles, getting darker towards the more senior roles. The color codes are shown in Figure 2 below and should be referred to as necessary.

Table 7shows all roles and the relevant levels which apply to each role. A check mark (✓) indicates the levels

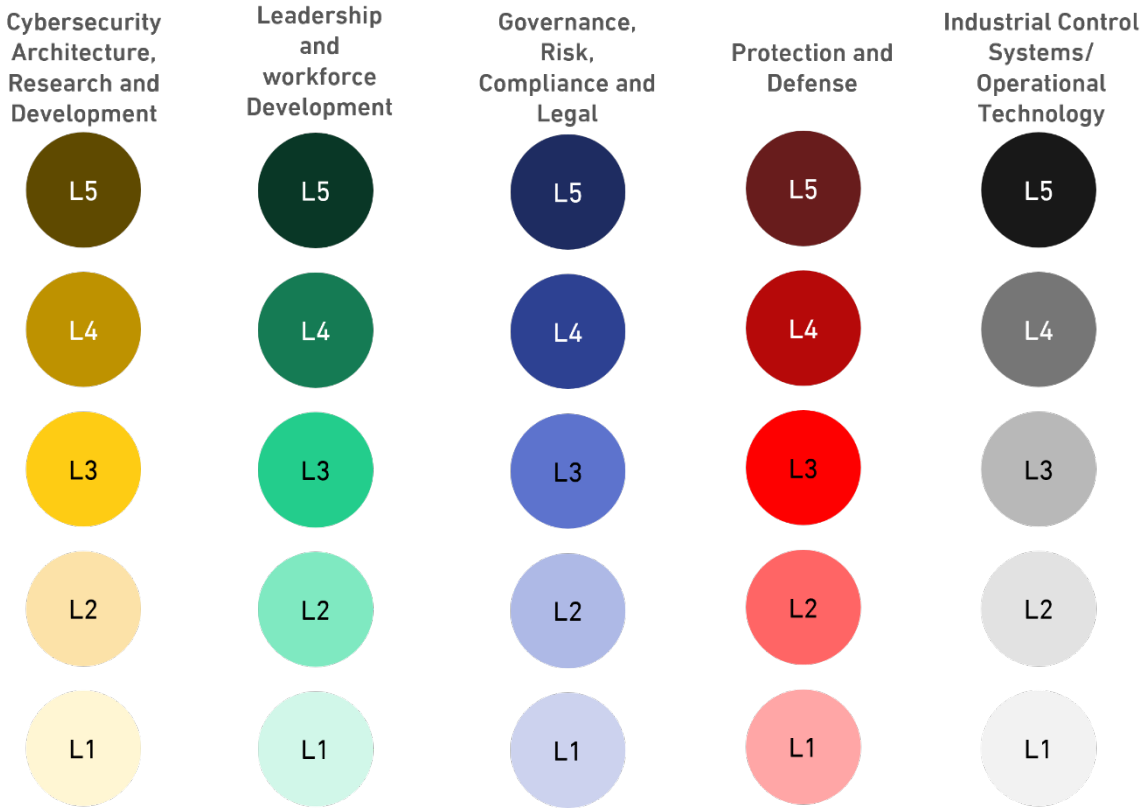

FIGURE 2: COLOR CODING FOR LEVELS

which exist for each role. The following points explain the rationale for how each role's starting level is determined:

- **Roles that start from Level 1** are **less advanced job roles** requiring no prior cybersecurity experience or in-depth domain knowledge. They suit individuals beginning their careers in the field.
- **Roles that start from Level 2** (with no Level 1 counterpart) serve as an **entry point** to cybersecurity, requiring **foundational** knowledge in a related domain (e.g., data science for a Cybersecurity Data Science Specialist). While prior cybersecurity experience is not mandatory, a basic understanding of the relevant industry is essential.
- **Roles that start from Level 3** (with no Levels 1 or 2) require an **intermediate level** of cybersecurity experience. Professionals in these positions should have a solid understanding and hands-on expertise in cybersecurity practices.

Category	Specialty	Roles	Levels				
			1	2	3	4	5
Cybersecurity Architecture, Research and Development	Cybersecurity Architecture	Cybersecurity Architect			✓	✓	
		Secure Cloud Specialist		✓	✓	✓	
	Cybersecurity Research and Development	Systems Security Development Specialist	✓	✓	✓	✓	
		Cybersecurity Developer	✓	✓	✓	✓	
		Secure Software Assessor	✓	✓	✓	✓	
		Cybersecurity Researcher	✓	✓	✓	✓	
		Cybersecurity Data Science Specialist		✓	✓	✓	
		Cybersecurity Artificial Intelligence Specialist		✓	✓	✓	
Leadership and Workforce Development	Leadership	Chief Information Security Officer/Director				✓	✓
		Cybersecurity Manager			✓	✓	✓
		Cybersecurity Advisor				✓	✓
	Workforce Development	Cybersecurity Human Capital Manager		✓	✓	✓	
		Cybersecurity Instructional Curriculum Developer	✓	✓	✓	✓	
		Cybersecurity Instructor	✓	✓	✓	✓	
Governance, Risk, Compliance and Laws	Governance, Risk and Compliance	Cybersecurity Risk Officer	✓	✓	✓	✓	
		Cybersecurity Compliance Officer	✓	✓	✓	✓	
		Cybersecurity Policy Officer	✓	✓	✓	✓	
		Security Controls Assessor	✓	✓	✓	✓	
		Cybersecurity Auditor		✓	✓	✓	
	Laws and Data Protection	Cybersecurity Legal Specialist	✓	✓	✓	✓	
		Data Protection Officer	✓	✓	✓	✓	

Document Classification: Public

TLP: Clear

Protection and Defense	**Defense**	Cybersecurity Defense Analyst	✓	✓	✓	✓	
		Cybersecurity Infrastructure Specialist		✓	✓	✓	
		Cybersecurity Specialist	✓	✓	✓		
	Protection	Cryptography Specialist		✓	✓	✓	
		Identity and Access Management Specialist		✓	✓	✓	
		Systems Security Analyst	✓	✓	✓	✓	
		Vulnerability Assessment Specialist	✓	✓	✓		
	Vulnerability Assessment	Penetration Tester / Red Team Specialist			✓	✓	
	Incident Response	Cybersecurity Incident Responder		✓	✓	✓	
		Digital Forensics Specialist		✓	✓	✓	
		Cyber Crime Investigator		✓	✓	✓	
		Malware Reverse Engineering Specialist			✓	✓	
	Threat Management	Threat Intelligence Analyst		✓	✓	✓	
		Threat Hunter			✓	✓	
Industrial Control Systems and Operational Technologies (ICS/OT)	**Industrial Control Systems and Operational Technologies (ICS/OT)**	ICS/OT Cybersecurity Architect			✓	✓	
		ICS/OT Cybersecurity Infrastructure Specialist		✓	✓	✓	
		ICS/OT Cybersecurity Defense Analyst		✓	✓	✓	
		ICS/OT Cybersecurity Risk Officer		✓	✓	✓	
		ICS/OT Cybersecurity Incident Responder			✓	✓	

TABLE 7: OVERVIEW OF ROLES AND LEVELS

Document Classification: Public

TLP: Clear

In the following sections, each job role and level are explained in detail, with diagrams and tables illustrating potential career movements (pathways). To keep these visuals simple, certain transitions are not explicitly shown but are possible:

- Lateral movements between job roles within the same job category (for levels L1 and L2)
- Entering any L1 job role as a QR1 Entry-Level Graduate[1]
- Entering any L2 job role as a QR2 Entry-Level Graduate[2]
- Progressions from any L3 job role to the L3 Cybersecurity Manager role
- Progressions from any L4 job role to the L4 Cybersecurity Manager or L4 Cybersecurity Advisor roles

[1] Refer to 'QR1 Entry Level Graduate' entry in table 3 for more details
[2] Refer to 'QR2 Entry Level Graduate' entry in table 3 for more details

TLP: Clear
Document Classification: Public

2. Cybersecurity Architecture, Research and Development

2.1 Cybersecurity Architect

The Cybersecurity Architect designs and oversees the development, implementation, and configuration of cybersecurity systems and networks. This role requires certifications or training in secure architecture design, risk management, secure configuration, cybersecurity risk assessment, disaster recovery, and integrating security into system design.

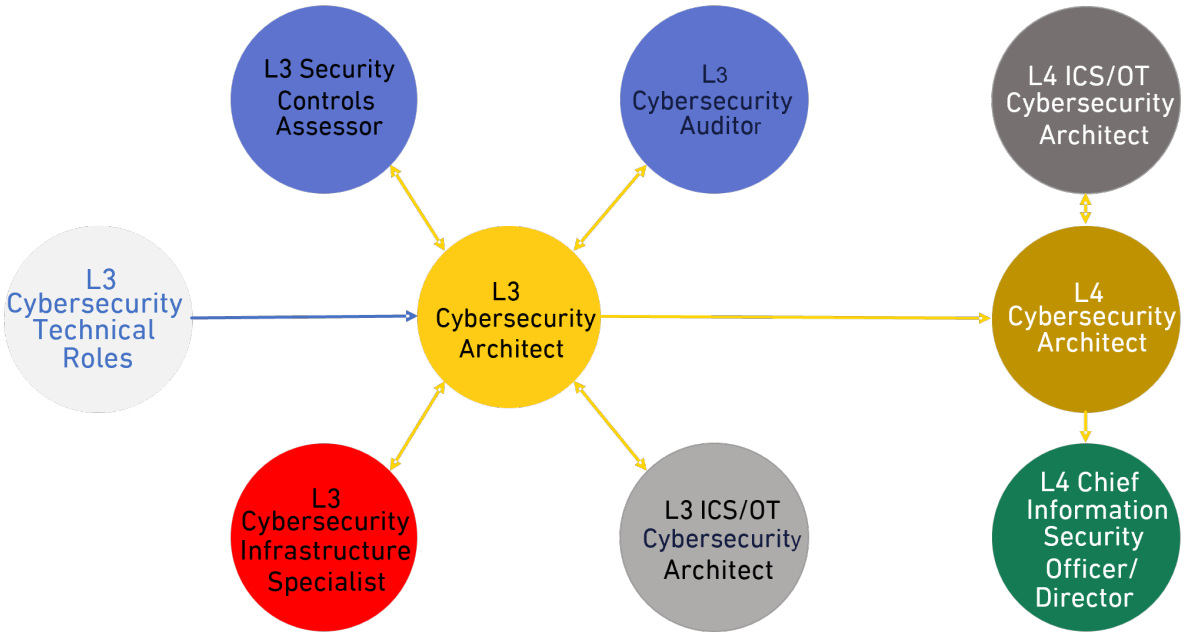

FIGURE 3: CYBERSECURITY ARCHITECT CAREER MAP

2.1.1 L3 Cybersecurity Architect

Job Role Name: Cybersecurity Architect (CARD-CA-001)	Job Level: Level 3
Role Description	Senior Practitioner managing a team or mentoring others to design and oversee the development, implementation and configuration of cybersecurity systems and networks. An individual in this role will be responsible for carrying out much of the Cybersecurity Architect's work at a lower level, carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Architect. Tasks will include performing cybersecurity reviews and identifying gaps in security architecture, and applying and incorporating information technologies into proposed solutions
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Technical Roles • L3 Cybersecurity Infrastructure Specialist • L3 ICS/OT Cybersecurity Architect • L3 Security Controls Assessor • L3 Cybersecurity Auditor	The next career step for someone in this role is one of the following: • L4 Cybersecurity Architect • L3 Cybersecurity Infrastructure Specialist • L3 ICS/OT Cybersecurity Architect • L3 Cybersecurity Auditor • L3 Security Controls Assessor

TABLE 8: L3 CYBERSECURITY ARCHITECT

2.1.2 L4 Cybersecurity Architect

Job Role Name: Cybersecurity Architect (CARD-CA-001)	Job Level: Level 4
Role Description	Expert managing a unit to design and oversee the development, implementation and configuration of cybersecurity systems and networks. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Architect's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include identifying and prioritizing critical business functions in collaboration with organizational stakeholders and providing advice on project costs, design concepts, or design changes.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Architect • L4 ICS/OT Cybersecurity Architect	The next career step for someone in this role is one of the following: • L4 Chief Information Security Officer / Director • L4 ICS/OT Cybersecurity Architect

TABLE 9: L4 CYBERSECURITY ARCHITECT

2.2 Secure Cloud Specialist

The Secure Cloud Specialist designs, implements, and operates secure cloud computing systems while developing and enforcing secure cloud policies. This role requires certifications or training in cloud computing, system security design, risk assessment, and secure testing methodologies.

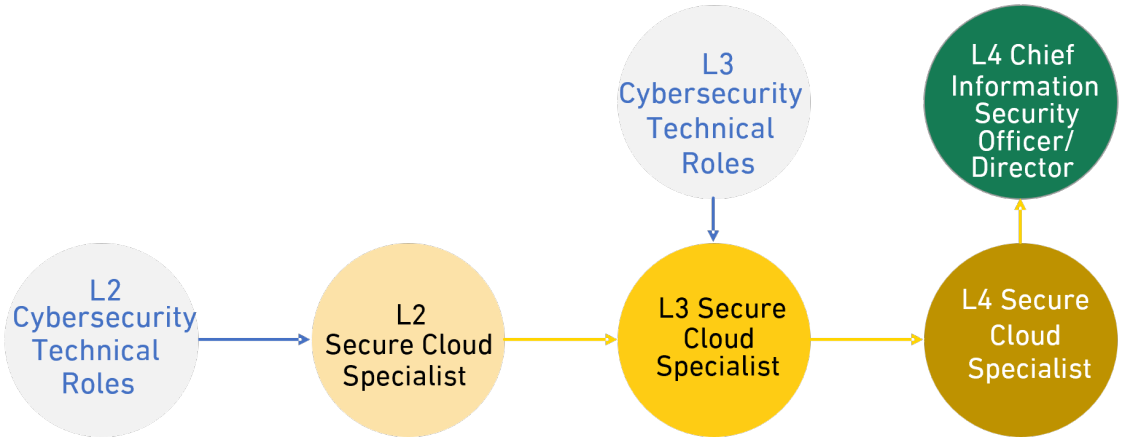

FIGURE 4: SECURE CLOUD SPECIALIST CAREER MAP

2.2.1 L2 Secure Cloud Specialist

Job Role Name: Secure Cloud Specialist (CARD-CA-002)	Job Level: Level 2
Role Description	Practitioner assisting in the design, implementation, and operation of secure cloud computing systems and contributing to the development of secure cloud policies. An individual in this role will carry out some of the basic tasks, under supervision, and will continue to develop their skills through practical application of their work. Tasks will include supporting the integration of cloud security elements into organizational systems and monitoring cloud environments for vulnerabilities
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Technical Roles • QR2 Entry Level Graduate	The next career step for someone in this role is one of the following: • L3 Secure Cloud Specialist

TABLE 10: L2 SECURE CLOUD SPECIALIST

2.2.2 L3 Secure Cloud Specialist

Job Role Name: Secure Cloud Specialist (CARD-CA-002)	Job Level: Level 3
Role Description	Senior Practitioner managing a team or mentoring others to design, implement and operate secure cloud computing systems and develop secure cloud policies. An individual in this role will be responsible for carrying out much of the Secure Cloud Specialist's work at a lower level, carrying out complex role related tasks for review by, and working under the direction of, the L4 Secure Cloud Specialist. Tasks will include developing security architecture elements to mitigate threats as they emerge and building the security controls to properly monitor and protect information held in cloud environments.

Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Secure Cloud Specialist • L3 Cybersecurity Technical Roles	The next career step for someone in this role is one of the following: • L4 Secure Cloud Specialist

TABLE 11: L3 SECURE CLOUD SPECIALIST

2.2.3 L4 Secure Cloud Specialist

Job Role Name: Secure Cloud Specialist (CARD-CA-002)	Job Level: Level 4
Role Description	Expert managing a unit to design, implement and operate secure cloud computing systems and develop secure cloud policies. An individual in this role will be responsible for providing oversight for much of the L3 Secure Cloud Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include providing subject matter expertise to develop and architect the next generation of organizational cybersecurity and working within and across multi-disciplinary teams as a domain expert in cloud security architecture standards and methodologies.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Secure Cloud Specialist	The next career step for someone in this role is one of the following: • L4 Chief Information Security Officer / Director

TABLE 12: L4 SECURE CLOUD SPECIALIST

2.3 Systems Security Development Specialist

The Systems Security Development Specialist designs, develops, tests, and evaluates the security of information systems throughout their development lifecycle. Certifications or training in secure software development, system security design, secure coding practices, vulnerability assessment, and security testing methodologies are essential for this role.

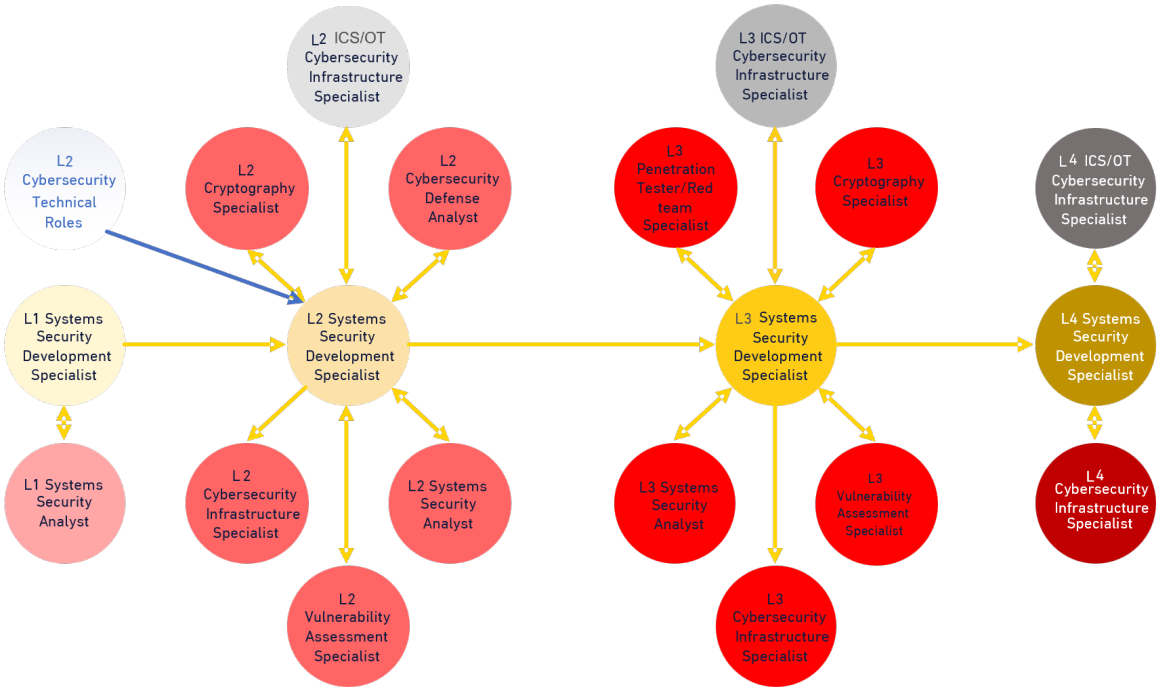

FIGURE 5: SYSTEMS SECURITY DEVELOPMENT SPECIALIST CAREER MAP

2.3.1 L1 Systems Security Development Specialist

Job Role Name: Systems Security Development Specialist (CARD-CRD-001)	Job Level: Level 1
Role Description	Assists the development team in designing, developing, testing, and evaluating security of information systems throughout the development lifecycle. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn the requirements of the role. Tasks will include supporting security certification test and evaluation activities and carrying out cybersecurity risk assessments.
Career Progression (Pathway)	
The individual will have come from the following roles: • L1 Systems Security Analyst • QR1 Entry Level Graduate	The next career step for someone in this role is one of the following: • L2 Systems Security Development Specialist • L1 Systems Security Analyst

TABLE 13: L1 SYSTEMS SECURITY DEVELOPMENT SPECIALIST

2.3.2 L2 Systems Security Development Specialist

Job Role Name: Systems Security Development Specialist (CARD-CRD-001)	Job Level: Level 2
Role Description	Practitioner designing, developing, testing, and evaluating security of information systems throughout the development lifecycle. An individual in this role will oversee the work done by the L1 Systems Security Development Specialist and will continue to develop their skills through practical application of their work. Tasks will include performing risk analysis whenever an application or system undergoes a major change and analyzing design constraints and trade-offs in detailed system cybersecurity design, including considering life cycle support.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Systems Security Development Specialist • L2 Cybersecurity Technical Roles • L2 ICS/OT Cybersecurity Infrastructure Specialist • L2 Cryptography Specialist • L2 Cybersecurity Defense Analyst • L2 Vulnerability Assessment Specialist • L2 System Security Analyst	The next career step for someone in this role is one of the following: • L3 Systems Security Development Specialist • L2 Cybersecurity Defense Analyst • L2 Systems Security Analyst • L2 ICS/OT Cybersecurity Infrastructure Specialist • L2 Vulnerability Assessment Specialist • L2 Cryptography Specialist • L2 Cybersecurity Infrastructure Specialist

TABLE 14: L2 SYSTEMS SECURITY DEVELOPMENT SPECIALIST

2.3.3 L3 Systems Security Development Specialist

Job Role Name: Systems Security Development Specialist (CARD-CRD-001)	Job Level: Level 3
Role Description	Senior Practitioner in designing, developing, testing, and evaluating security of information systems throughout the development lifecycle. An individual in this role will be responsible for carrying out much of the Systems Security Development Specialist's work at a lower level, carrying out complex role related tasks for review by, and working under the direction of, the L4 Systems Security Development Specialist. Tasks will include utilizing models and simulations to analyze or predict system performance under different operating conditions and developing detailed security design documentation for component and interface specifications to support system design and development.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Systems Security Development Specialist • L3 Cryptography Specialist • L3 Systems Security Analyst • L3 ICS/OT Cybersecurity Infrastructure Specialist • L3 Cybersecurity Infrastructure Specialist • L3 Vulnerability Assessment Specialist • L3 Penetration Tester/Red team Specialist	The next career step for someone in this role is one of the following: • L4 Systems Security Development Specialist • L3 Cryptography Specialist • L3 Cybersecurity Infrastructure Specialist • L3 Systems Security Analyst • L3 ICS/OT Cybersecurity Infrastructure Specialist • L3 Vulnerability Assessment Specialist • L3 Penetration Tester / Red Team Specialist

TABLE 15: L3 SYSTEMS SECURITY DEVELOPMENT SPECIALIST

2.3.4 L4 Systems Security Development Specialist

Job Role Name: Systems Security Development Specialist (CARD-CRD-001)	Job Level: Level 4
Role Description	Expert managing a unit to design, develop, test, and evaluate security of information systems throughout the development lifecycle. An individual in this role will be responsible for providing oversight for much of the L3 Systems Security Development Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include developing risk mitigation strategies to effectively manage risk in accordance with organizational risk appetite and ensuring these address cost, schedule, performance, and security risks.

Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Systems Security Development Specialist • L4 ICS/OT Cybersecurity Infrastructure Specialist • L4 Cybersecurity Infrastructure Specialist	The next career step for someone in this role is one of the following: • L4 ICS/OT Cybersecurity Infrastructure Specialist • L4 Cybersecurity Infrastructure Specialist

TABLE 16: L4 SYSTEMS SECURITY DEVELOPMENT SPECIALIST

2.4 Cybersecurity Developer

The Cybersecurity Developer develops cybersecurity software, applications, systems, and products. This role requires certifications or training in secure software development, application security, secure coding practices, and vulnerability mitigation techniques.

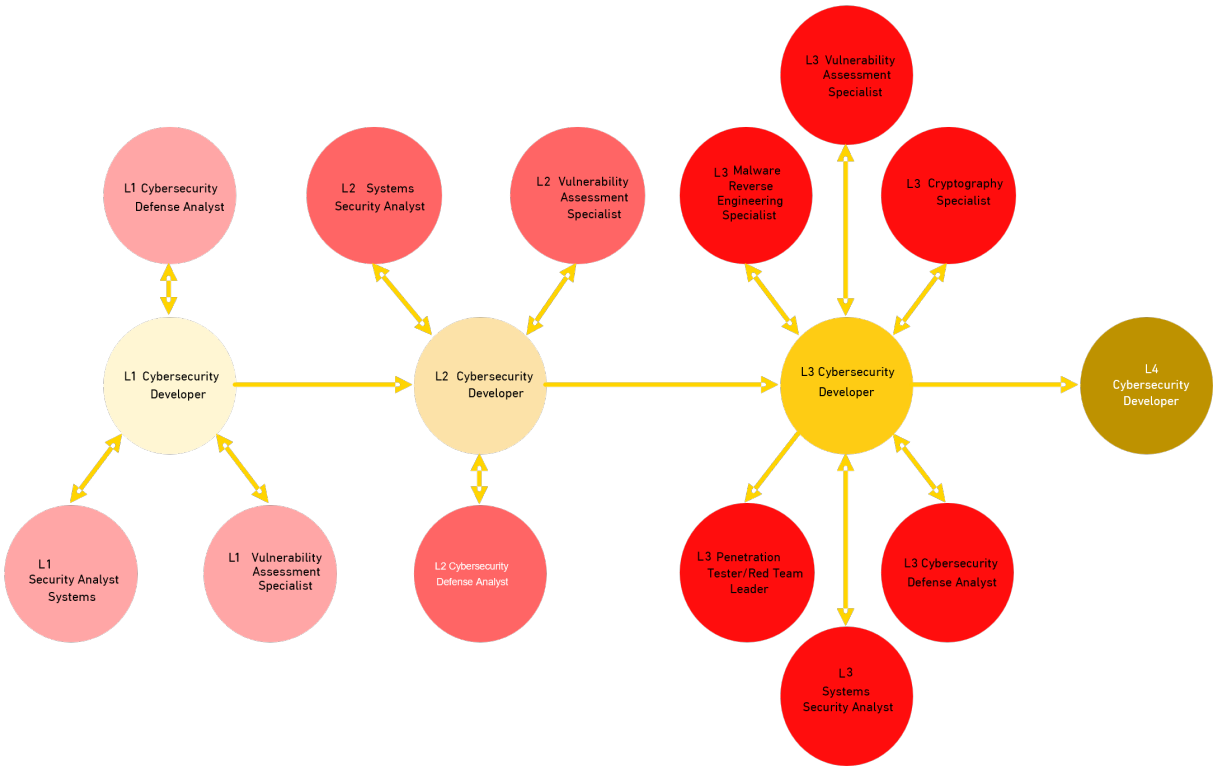

FIGURE 6: CYBERSECURITY DEVELOPER CAREER MAP

2.4.1 L1 Cybersecurity Developer

Job Role Name: Cybersecurity Developer (CARD-CRD-002)	Job Level: Level 1
Role Description	Supports the development of cybersecurity software, applications, systems, and products. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn the requirements of the role. Tasks will include applying coding and testing security standards and secure code documentation.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate • L1 Cybersecurity Defense Analyst • L1 Systems Security Analyst • L1 Vulnerability Assessment Specialist • Core Cybersecurity Role	The next career step for someone in this role is one of the following: • L2 Cybersecurity Developer • L1 Cybersecurity Defense Analyst • L1 Systems Security Analyst • L1 Vulnerability Assessment Specialist

TABLE 17: L1 CYBERSECURITY DEVELOPER

2.4.2 L2 Cybersecurity Developer

Job Role Name: Cybersecurity Developer (CARD-CRD-002)	Job Level: Level 2
Role Description	Practitioner that develops cybersecurity software, applications, systems, and products. An individual in this role will oversee the work done by the L1 Cybersecurity Developer and will continue to develop their skills through practical application of their work. Tasks will include integrating cybersecurity into the requirements process by defining and capturing security controls and ensuring program development and revisions are fully documented and can be understood by others by using comments in the coded instructions.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Cybersecurity Developer • L2 Cybersecurity Technical Roles • L2 Cybersecurity Defense Analyst • L2 Systems Security Analyst • L2 Vulnerability Assessment Specialist	The next career step for someone in this role is one of the following: • L3 Cybersecurity Developer • L2 Cybersecurity Defense Analyst • L2 Systems Security Analyst • L2 Vulnerability Assessment Specialist

TABLE 18: L2 CYBERSECURITY DEVELOPER

2.4.3 L3 Cybersecurity Developer

Job Role Name: Cybersecurity Developer (CARD-CRD-002)	Job Level: Level 3
Role Description	Senior Practitioner that develops cybersecurity software, applications, systems and products. An individual in this role will be responsible for carrying out much of the Cybersecurity Developer's work at a lower level, carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Developer. Tasks will include preparing detailed workflow charts and diagrams that describe input, output, and logical operation of security systems and translating security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Developer • L3 Cryptography Specialist • L3 Cybersecurity Defense Analyst • L3 Malware Reverse Engineering Specialist • L3 Systems Security Analyst • L3 Vulnerability Assessment Specialist	The next career step for someone in this role is one of the following: • L4 Cybersecurity Developer • L3 Cryptography Specialist • L3 Cybersecurity Defense Analyst • L3 Malware Reverse Engineering Specialist • L3 Systems Security Analyst • L3 Vulnerability Assessment Specialist • L3 Penetration Tester / Red Team Specialist

TABLE 19: L3 CYBERSECURITY DEVELOPER

2.4.4 L4 Cybersecurity Developer

Job Role Name: Cybersecurity Developer (CARD-CRD-002)	Job Level: Level 4
Role Description	Expert managing a unit to develop cybersecurity software, applications, systems and products. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Developer's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include assessing how user needs and software requirements can be met in line with cybersecurity policies and determining the feasibility of design within time and cost constraints.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Developer	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 20: L4 CYBERSECURITY DEVELOPER

2.5 Secure Software Assessor

The Secure Software Assessor evaluates the security of computer applications, software, code, or programs and delivers actionable results. This role requires certifications or training in secure software assessment, secure coding practices, vulnerability identification, and software security standards.

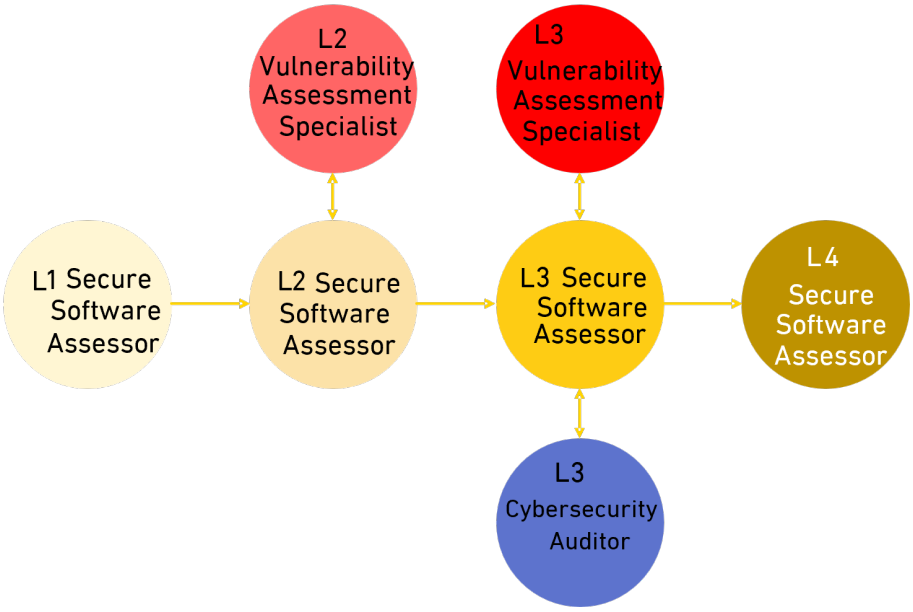

FIGURE 7: SECURE SOFTWARE ASSESSOR CAREER MAP

2.5.1 L1 Secure Software Assessor

Job Role Name: Secure Software Assessor (CARD-CRD-003)	Job Level: Level 1
Role Description	Supports the team to evaluate the security of computer applications, software, code, or programs and provides actionable results. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn the requirements of the role. Tasks will include addressing security implications in the software acceptance phase and conducting trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate • L1 Core Cybersecurity Role	The next career step for someone in this role is one of the following: • L2 Secure Software Assessor

TABLE 21: L1 SECURE SOFTWARE ASSESSOR

2.5.2 L2 Secure Software Assessor

Job Role Name: Secure Software Assessor (CARD-CRD-003)	Job Level: Level 2
Role Description	Practitioner assessing the security of computer applications, software, code, or programs and provides actionable results. An individual in this role will carry oversee the work done by the L1 Secure Software Assessor, and will continue to develop their skills through practical application of their work. Tasks will include performing secure program testing, review, and assessment to identify potential flaws in codes and mitigate vulnerabilities, and determining and documenting software patches or the extent of releases that would leave software vulnerable.

Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Secure Software Assessor • L2 Vulnerability Assessment Specialist	The next career step for someone in this role is one of the following: • L3 Secure Software Assessor • L2 Vulnerability Assessment Specialist

TABLE 22: L2 SECURE SOFTWARE ASSESSOR

2.5.3 L3 Secure Software Assessor

Job Role Name: Secure Software Assessor (CARD-CRD-003)	Job Level: Level 3
Role Description	Senior Practitioner assessing the security of computer applications, software, code, or programs and provides actionable results. An individual in this role will be responsible for carrying out much of the Secure Software Assessor's work at a lower level, carrying out complex role related tasks for review by, and working under the direction of, the L4 Secure Software Assessor. Tasks will include performing risk analysis whenever an application or system undergoes a major change and supervising and effectively assigning work to staff working on cybersecurity related tasks.

Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Secure Software Assessor • L3 Vulnerability Assessment Specialist • L3 Cybersecurity Auditor	The next career step for someone in this role is one of the following: • L4 Secure Software Assessor • L3 Vulnerability Assessment Specialist • L3 Cybersecurity Auditor

TABLE 23: L3 SECURE SOFTWARE ASSESSOR

2.5.4 L4 Secure Software Assessor

Job Role Name: Secure Software Assessor (CARD-CRD-003)		Job Level: Level 4
Role Description	Expert managing a unit to evaluate the security of computer applications, software, code, or programs and provide actionable results. An individual in this role will be responsible for providing oversight for much of the L3 Secure Software Assessor's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include developing threat models based on customer interviews and requirements, and translating security requirements into application design elements.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L3 Secure Software Assessor		The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 24: L4 SECURE SOFTWARE ASSESSOR

2.6 Cybersecurity Researcher

The Cybersecurity Researcher conducts scientific research in the field of cybersecurity. This role requires certifications or training in cybersecurity research methodologies, vulnerability analysis, and the development of cybersecurity tools and technologies, along with specialized training in the specific topics being researched.

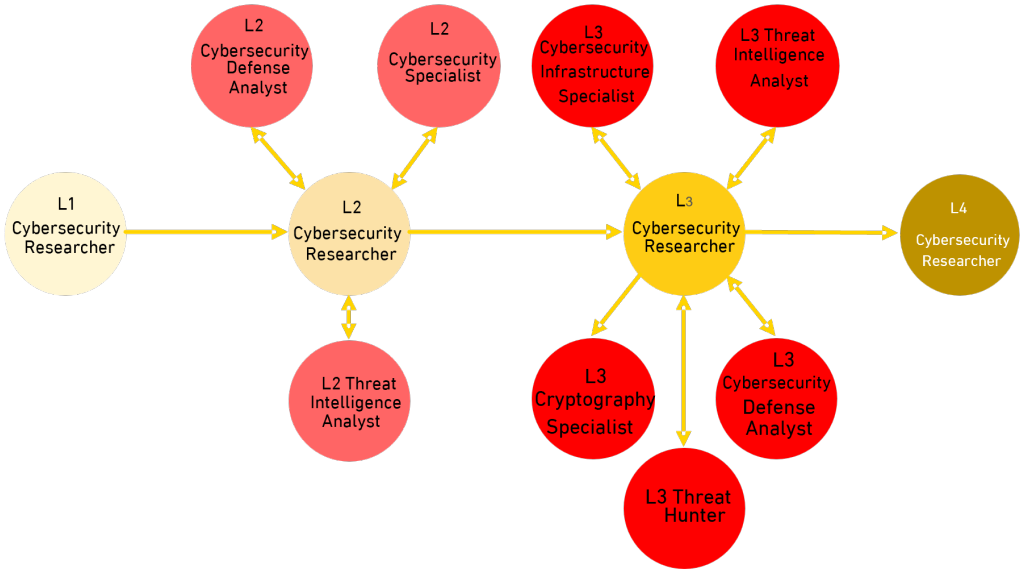

FIGURE 8: CYBERSECURITY RESEARCHER CAREER MAP

2.6.1 L1 Cybersecurity Researcher

Job Role Name: Cybersecurity Researcher (CARD-CRD-004)	Job Level: Level 1
Role Description	Supports the team to conduct scientific research in the cybersecurity field. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn the requirements of the role. Tasks will include evaluating network infrastructure vulnerabilities and following software and systems engineering lifecycle standards and processes when developing cybersecurity systems and solutions.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate	The next career step for someone in this role is one of the following: • L2 Cybersecurity Researcher

TABLE 25: L1 CYBERSECURITY RESEARCHER

2.6.2 L2 Cybersecurity Researcher

Job Role Name: Cybersecurity Researcher (CARD-CRD-004)	Job Level: Level 2
Role Description	Practitioner that conducts scientific research in the cybersecurity field. An individual in this role will carry oversee the work done by the L1 Cybersecurity Researcher and will continue to develop their skills through practical application of their work. Tasks will include researching current technology to understand cyber defense capability required by systems or networks and identifying and developing reverse engineering tools to enhance capabilities and detect vulnerabilities.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Cybersecurity Researcher • L2 Cybersecurity Defense Analyst • L2 Cybersecurity Specialist • L2 Threat Intelligence Analyst	The next career step for someone in this role is one of the following: • L3 Cybersecurity Researcher • L2 Cybersecurity Defense Analyst • L2 Threat Intelligence Analyst • L2 Cybersecurity Specialist

TABLE 26: L2 CYBERSECURITY RESEARCHER

2.6.3 L3 Cybersecurity Researcher

Job Role Name: Cybersecurity Researcher (CARD-CRD-004)	Job Level: Level 3
Role Description	Senior Practitioner that conducts scientific research in the cybersecurity field. An individual in this role will be responsible for carrying out much of the Cybersecurity Researcher's work at a lower level, carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Researcher. Tasks will include developing secure data management capabilities to support a mobile workforce and reviewing and validating data mining and data warehousing programs, processes, and requirements.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Researcher • L3 Cybersecurity Defense Analyst • L3 Cybersecurity Infrastructure Specialist • L3 Threat Intelligence Analyst • L3 Threat Hunter	The next career step for someone in this role is one of the following: • L4 Cybersecurity Researcher • L3 Cryptography Specialist • L3 Cybersecurity Defense Analyst • L3 Cybersecurity Infrastructure Specialist • L3 Threat Intelligence Analyst • L3 Threat Hunter

TABLE 27: L3 CYBERSECURITY RESEARCHER

2.6.4 L4 Cybersecurity Researcher

Job Role Name: Cybersecurity Researcher (CARD-CRD-004)	Job Level: Level 4
Role Description	Expert managing a unit to conduct scientific research in the cybersecurity field. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Researcher's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include identifying cybersecurity capability strategies for custom hardware and software development based on an organization's requirements and collaborating with stakeholders to identify appropriate cybersecurity solutions technology.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Researcher	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 28: L4 CYBERSECURITY RESEARCHER

2.7 Cybersecurity Data Science Specialist

The Cybersecurity Data Science Specialist applies mathematical models, scientific methods, and processes to design and implement algorithms and systems that derive cybersecurity insights from large-scale data sets. This role requires certifications or training in data science, statistical analysis, machine learning, and data mining techniques tailored to cybersecurity applications.

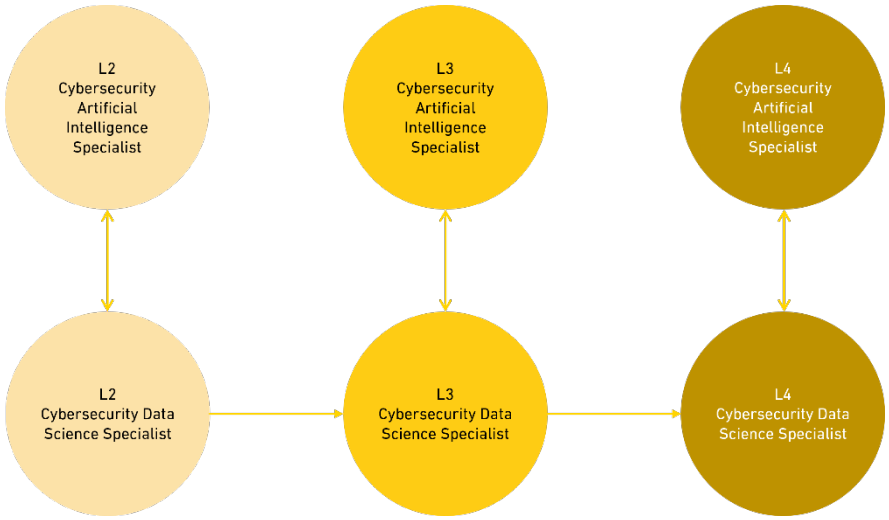

FIGURE 9: CYBERSECURITY DATA SCIENCE SPECIALIST CAREER MAP

2.7.1 L2 Cybersecurity Data Science Specialist

Job Role Name: Cybersecurity Data Science Specialist (CARD- CRD-005)	Job Level: Level 2
Role Description	Practitioner that 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. An individual in this role will carry out some of the basic tasks, under supervision, and will continue to develop their skills through practical application of their work. Tasks will include collecting metrics and trending data and analyzing data sources to provide actionable recommendations.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Artificial Intelligence Specialist	The next career step for someone in this role is one of the following: • L3 Cybersecurity Data Science Specialist • L2 Cybersecurity Artificial Intelligence Specialist

TABLE 29: L2 CYBERSECURITY DATA SCIENCE SPECIALIST

2.7.2 L3 Cybersecurity Data Science Specialist

Job Role Name: Cybersecurity Data Science Specialist (CARD- CRD-005)	Job Level: Level 3
Role Description	Senior Practitioner that 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. An individual in this role will be responsible for carrying out much of the Cybersecurity Data Science Specialist's work at a lower level, carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Data Science Specialist. Tasks will include conducting hypothesis testing using statistical processes and working with systems analysts, engineers, programmers, and others to design cybersecurity applications.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Data Science Specialist • L3 Cybersecurity Artificial Intelligence Specialist	The next career step for someone in this role is one of the following: • L4 Cybersecurity Data Science Specialist • L3 Cybersecurity Artificial Intelligence Specialist

TABLE 30: L3 CYBERSECURITY DATA SCIENCE SPECIALIST

2.7.3 L4 Cybersecurity Data Science Specialist

Job Role Name: Cybersecurity Data Science Specialist (CARD- CRD-005)	Job Level: Level 4
Role Description	Expert managing a unit to use 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. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Data Science Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include developing data standards, policies, and procedures and providing stakeholders with actionable recommendations derived from data analysis and findings.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Data Science Specialist • L4 Cybersecurity Artificial Intelligence Specialist	The next career step for someone in this role is one of the following: • L4 Cybersecurity Artificial Intelligence Specialist

TABLE 31: L4 CYBERSECURITY DATA SCIENCE SPECIALIST

2.8 Cybersecurity Artificial Intelligence Specialist

The Cybersecurity Artificial Intelligence Specialist leverages artificial intelligence models and techniques, including machine learning, to design and implement algorithms and systems that automate and enhance the efficiency and effectiveness of cybersecurity tasks. Certifications or training in artificial intelligence, machine learning, data analysis, and automation techniques for cybersecurity applications are essential for this role.

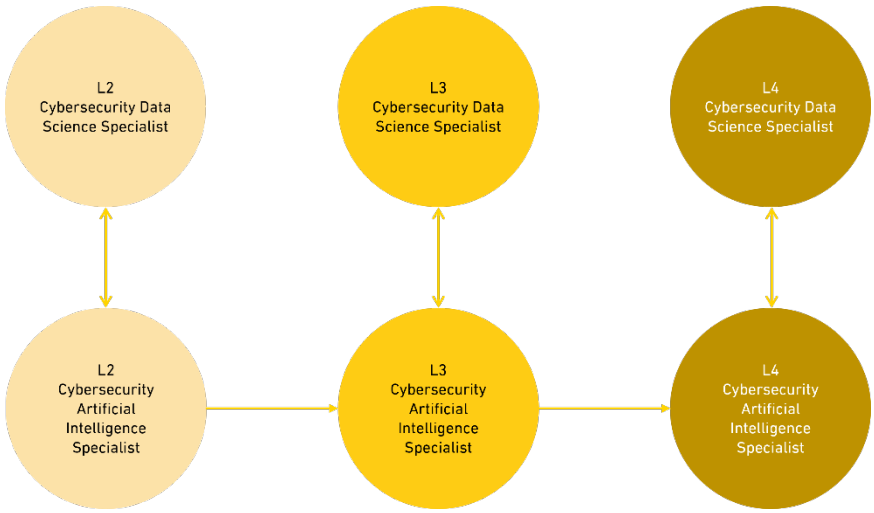

FIGURE 10: CYBERSECURITY ARTIFICIAL INTELLIGENCE SPECIALIST CAREER MAP

2.8.1 L2 Cybersecurity Artificial Intelligence Specialist

Job Role Name: Cybersecurity Artificial Intelligence Specialist (CARD-CRD-006)	Job Level: Level 2
Role Description	Practitioner that 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. An individual in this role will carry out some of the basic tasks, under supervision, and will continue to develop their skills through practical application of their work. Tasks will include utilizing different open source programming languages to write code, open, read, and process files, and write output to different files.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Data Science Specialist	The next career step for someone in this role is one of the following: • L3 Cybersecurity Artificial Intelligence Specialist • L2 Cybersecurity Data Science Specialist

TABLE 32: L2 CYBERSECURITY ARTIFICIAL INTELLIGENCE SPECIALIST

2.8.2 L3 Cybersecurity Artificial Intelligence Specialist

Job Role Name: Cybersecurity Artificial Intelligence Specialist (CARD-CRD-006)		Job Level: Level 3
Role Description	Senior Practitioner that 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. An individual in this role will be responsible for carrying out much of the Cybersecurity Artificial Intelligence Specialist's work at a lower level, carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Artificial Intelligence Specialist. Tasks will include using visualization tools to visualize data and create dashboards to communicate results, and performing data profiling, statistical and machine learning analysis.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L2 Cybersecurity Artificial Intelligence Specialist • L3 Cybersecurity Data Science Specialist		The next career step for someone in this role is one of the following: • L4 Cybersecurity Artificial Intelligence Specialist • L3 Cybersecurity Data Science Specialist

TABLE 33: L3 CYBERSECURITY ARTIFICIAL INTELLIGENCE SPECIALIST

2.8.3 L4 Cybersecurity Artificial Intelligence Specialist

Job Role Name: Cybersecurity Artificial Intelligence Specialist (CARD-CRD-006)	Job Level: Level 4
Role Description	Expert managing a unit to use 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. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Artificial Intelligence Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include applying 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, and keeping current with computer vision and machine learning research to replicate and baseline new techniques.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Artificial Intelligence Specialist • L4 Cybersecurity Data Science Specialist	The next career step for someone in this role is one of the following: • L4 Cybersecurity Data Science Specialist

TABLE 34: L4 CYBERSECURITY ARTIFICIAL INTELLIGENCE SPECIALIST

3. Leadership and Workforce Development

3.1 Chief Information Security Officer / Director

The Chief Information Security Officer (CISO) directs cybersecurity efforts within an organization, establishes the vision and strategy for cybersecurity initiatives, and advises leadership on managing cyber risks effectively. This role requires certifications or training in cybersecurity governance, risk management, cybersecurity strategy, defense, policy development, and leadership.

FIGURE 11: CHIEF INFORMATION SECURITY OFFICER / DIRECTOR CAREER MAP

3.1.1 L4 Chief Information Security Officer / Director

Job Role Name: Chief Information Security Officer / Director (LWD-L-001)	Job Level: Level 4
Role Description	Directs cybersecurity work within an organization, establishes vision and direction for its cybersecurity and related strategies, resources and activities and advises the Board on the effective management of the organization's cyber risks. An individual in this role oversees all aspects of cybersecurity across the organization to ensure that measures in place support the organization's business needs. Tasks will include effectively communicating financial aspects of cybersecurity related activities to senior management and aligning the organization's cybersecurity strategy with its business strategy.
Career Progression (Pathway)	
The individual will have come from the following roles: • L4 Cybersecurity Advisor • L4 Cybersecurity Architect • L4 Cybersecurity Auditor • L4 Cybersecurity Compliance Officer • L4 Cybersecurity Manager • L4 Cybersecurity Policy Officer • L4 Cybersecurity Risk Officer • L4 Secure Cloud Specialist • L4 ICS/OT Cybersecurity Architect • L4 ICS/OT Cybersecurity Risk Officer	The next career step for someone in this role is one of the following: • L5 Chief Information Security Officer/Director • L4 Cybersecurity Advisor • L4 Cybersecurity Manager

TABLE 35: L4 CHIEF INFORMATION SECURITY OFFICER / DIRECTOR

3.1.2 L5 Chief Information Security Officer / Director

Job Role Name: Chief Information Security Officer / Director (LWD-L-001)		Job Level: Level 5
Role Description	Directs cybersecurity work within an organization, establishes strategy and direction for its cybersecurity and related strategies, resources and activities and advises the Board on the effective management of the organization's cyber risks. An individual in this role liaises directly with the board and is accountable for all aspects of cybersecurity across the organization to ensure that measures in place support the organization's business needs. This role is more focused on technology and other controls applied to provide cybersecurity than the people who are employed to implement and maintain those controls. Tasks will include collaborating with stakeholders in the organization and with third parties when identifying future cybersecurity strategy requirements and attending and presenting at international cybersecurity events.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L4 Chief Information Security Officer/Director • L5 Cybersecurity Manager • L5 Cybersecurity Advisor		The next career step for someone in this role is one of the following: • L5 Cybersecurity Manager • L5 Cybersecurity Advisor

TABLE 36: L5 CHIEF INFORMATION SECURITY OFFICER / DIRECTOR

3.2 Cybersecurity Manager

The Cybersecurity Manager oversees the security of information systems and functions within an organization, leading cybersecurity teams, units, or enterprise-level functions. Certifications or training in cybersecurity governance, risk management, cybersecurity strategy, defense, policy development, and leadership are essential for this role.

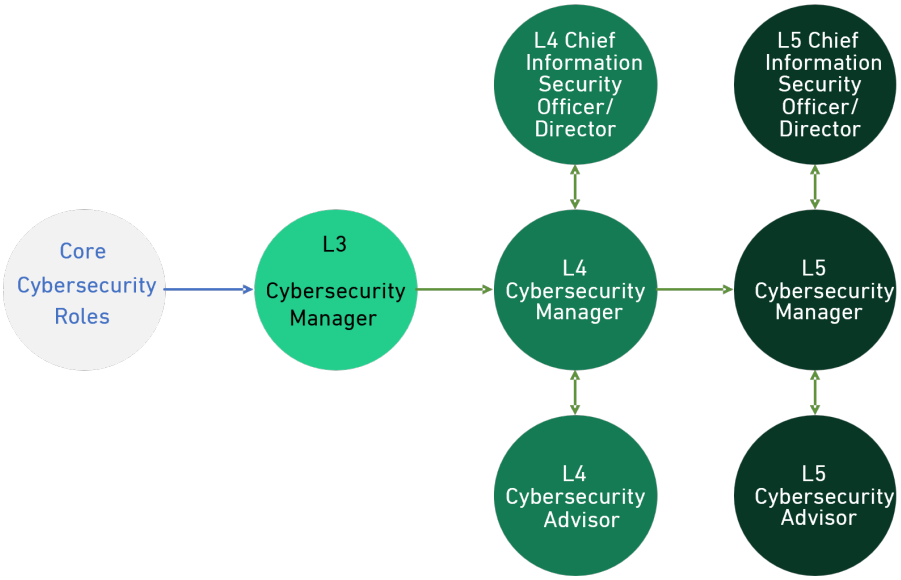

FIGURE 12: CYBERSECURITY MANAGER CAREER MAP

3.2.1 L3 Cybersecurity Manager

Job Role Name: Cybersecurity Manager (LWD-L-002)	Job Level: Level 3
Role Description	Senior Practitioner who manages the security of information systems and functions within an organization. Leads a cybersecurity team, unit and/or enterprise level function. An individual in this role will be responsible for carrying out general management duties relating to staff within each team, including annual appraisals and day-to-day support of team members. Tasks will include obtaining resources to develop and implement effective processes to meet strategic cybersecurity goals and identifying the implications of new technologies and upgrades on cybersecurity across the organization.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Core Cybersecurity Roles	The next career step for someone in this role is one of the following: • L4 Cybersecurity Manager

TABLE 37: L3 CYBERSECURITY MANAGER

3.2.2 L4 Cybersecurity Manager

Job Role Name: Cybersecurity Manager (LWD-L-002)	Job Level: Level 4
Role Description	Leads a cybersecurity team, unit and/or enterprise level function managing the security of information systems and functions within an organization. An individual in this role will be responsible for carrying out senior management duties relating to staff within several teams, including financial management and budgetary forecasting for the parts of the organization they are accountable for. Tasks will include ensuring that cybersecurity awareness training is provided to all members of staff, and promoting and demonstrating the value of cybersecurity to stakeholders within an organization.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Manager • L4 Chief Information Security Officer/Director • L4 Cybersecurity Advisor	The next career step for someone in this role is one of the following: • L5 Cybersecurity Manager • L4 Chief Information Security Officer/Director • L4 Cybersecurity Advisor

TABLE 38: L4 CYBERSECURITY MANAGER

3.2.3 L5 Cybersecurity Manager

Job Role Name: Cybersecurity Manager (LWD-L-002)	Job Level: Level 5
Role Description	Leads a cybersecurity team, unit and/or enterprise level function or Fellow providing expert advice on, managing the security of information systems and functions within an organization. An individual in this role liaises directly with the board and is accountable for all aspects of cybersecurity team management across the organization. This role is more focused on the people working in cybersecurity than the technology and other controls which are used. Tasks will include ensuring that cybersecurity requirements of all information technology systems are determined and participating in the acquisition process as necessary to ensure that appropriate supply chain risk management practices are adopted.
Career Progression (Pathway)	
The individual will have come from the following roles: • L4 Cybersecurity Manager • L5 Chief Information Security Officer/Director • L5 Cybersecurity Advisor	The next career step for someone in this role is one of the following: • L5 Chief Information Security Officer/Director • L5 Cybersecurity Advisor

TABLE 39: L5 CYBERSECURITY MANAGER

3.3 Cybersecurity Advisor

The Cybersecurity Advisor provides expert consultancy and advice on cybersecurity topics to an organization's leadership and cybersecurity teams. This role requires certifications or training in cybersecurity strategy, governance, risk communication, and policy advisory. Depending on the advisory scope, relevant training may also include secure software development, network security, incident management, cloud security, or data protection.

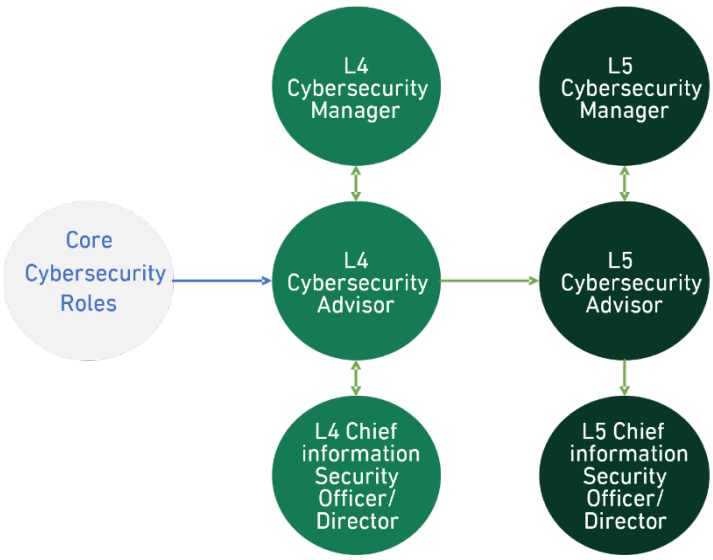

FIGURE 13: CYBERSECURITY ADVISOR CAREER MAP

3.3.1 L4 Cybersecurity Advisor

Job Role Name: Cybersecurity Advisor (LWD-L-003)	Job Level: Level 4
Role Description	Provides expert consultancy and advice on cybersecurity topics to an organization's leadership and to its cybersecurity leadership and teams. An individual in this role is the subject matter expert within the team, and will therefore have a high level of technical skill, knowledge and expertise. Provides advice and guidance to external teams / agencies / organizations as well as mentoring team members. Tasks will include effectively communicating cybersecurity risks and posture as well as financial aspects of cybersecurity related activities to senior management.
Career Progression (Pathway)	
The individual will have come from the following roles: • L4 Chief Information Security Officer / Director • L4 Cybersecurity Manager • L4 Core Cybersecurity Roles	The next career step for someone in this role is one of the following: • L5 Cybersecurity Advisor • L4 Chief Information Security Officer / Director • L4 Cybersecurity Manager

TABLE 40: L4 CYBERSECURITY ADVISOR

3.3.2 L5 Cybersecurity Advisor

Job Role Name: Cybersecurity Advisor (LWD-L-003)		Job Level: Level 5
Role Description	Provides expert consultancy and advice on cybersecurity topics to an organization's leadership and to its cybersecurity leadership and teams. An individual in this role represents the organization in high level discussions/negotiations relating to cybersecurity. Contributes to white papers and other academic research. Tasks will include understanding and communicating the organization's cybersecurity status during legal and regulatory scrutiny and promoting and demonstrating the value of cybersecurity to stakeholders within the organization.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L4 Cybersecurity Advisor • L5 Chief Information Security Officer / Director • L5 Cybersecurity Manager		The next career step for someone in this role is one of the following: • L5 Chief Information Security Officer /Director • L5 Cybersecurity Manager

TABLE 41: CYBERSECURITY ADVISOR

3.4 Cybersecurity Human Capital Manager

The Cybersecurity Human Capital Manager develops plans, strategies, and guidance to support the growth and management of an organization's cybersecurity workforce. Certifications or training in cybersecurity workforce planning, human capital management, training and development, and organizational strategy are essential for this role.

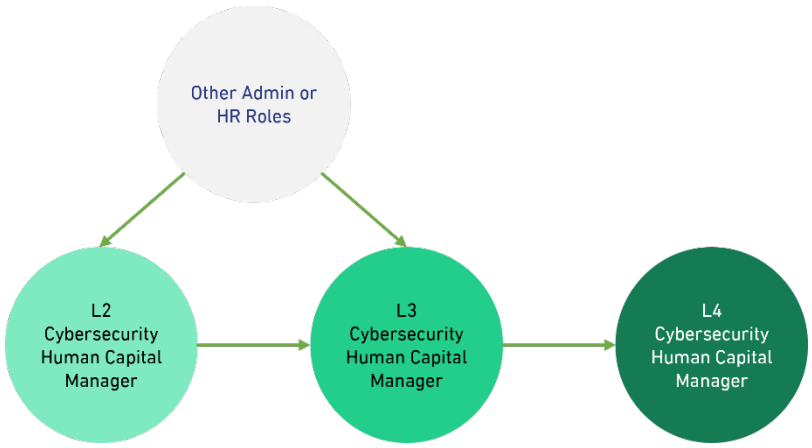

FIGURE 14: CYBERSECURITY HUMAN CAPITAL MANAGER CAREER MAP

3.4.1 L2 Cybersecurity Human Capital Manager

Job Role Name: Cybersecurity Human Capital Manager (LWD- WD-001)	Job Level: Level 2
Role Description	Practitioner developing plans, strategies and guidance within an organization to support the development and management of the cybersecurity workforce. An individual in this role will carry out some of the basic human capital management task such as recruitment and maintenance of personnel records, and will continue to develop their skills through practical application of their work. Tasks will include allocating resources to cybersecurity roles and assisting with the review and assessment cybersecurity staff effectiveness to identify skills gaps and training requirements.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • Other Admin or HR Roles	The next career step for someone in this role is one of the following: • L3 Cybersecurity Human Capital Manager

TABLE 42: L2 CYBERSECURITY HUMAN CAPITAL MANAGER

3.4.2 L3 Cybersecurity Human Capital Manager

Job Role Name: Cybersecurity Human Capital Manager (LWD- WD-001)		Job Level: Level 3
Role Description	Senior Practitioner developing plans, strategies and guidance within an organization to support the development and management of the cybersecurity workforce. An individual in this role will be responsible for carrying out mentoring of the L2 Cybersecurity Human Capital Manager, as well as carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Human Capital Manager. Tasks will include working with subject matter experts to ensure qualification standards reflect organizational functional requirements and industry standards and establishing and overseeing requirements, qualifications and processes for cyber career entry.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L2 Cybersecurity Human Capital Manager • Other HR or Admin Roles		The next career step for someone in this role is one of the following: • L4 Cybersecurity Human Capital Manager

TABLE 43: L3 CYBERSECURITY HUMAN CAPITAL MANAGER

3.4.3 L4 Cybersecurity Human Capital Manager

Job Role Name: Cybersecurity Human Capital Manager (LWD- WD-001)		Job Level: Level 4
Role Description	Expert managing unit to develop plans, strategies and guidance within an organization to support the development and management of the cybersecurity workforce. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Human Capital Manager's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include providing policy guidance (as it relates to Personnel security) to cybersecurity management and ensuring that cybersecurity careers are managed in accordance with organizational HR policies and directives.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L3 Cybersecurity Human Capital Manager		The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 44: L4 CYBERSECURITY HUMAN CAPITAL MANAGER

3.5 Cybersecurity Instructional Curriculum Developer

The Cybersecurity Instructional Curriculum Developer develops, plans, coordinates, and evaluates cybersecurity training, awareness, and education programs, courses, contents, methods, and techniques based to instructional needs. This role requires certifications or training in instructional design, curriculum development, cybersecurity education, and foundational cybersecurity topics, as well as topic-specific training, awareness, or certifications relevant to the areas of curriculum development.

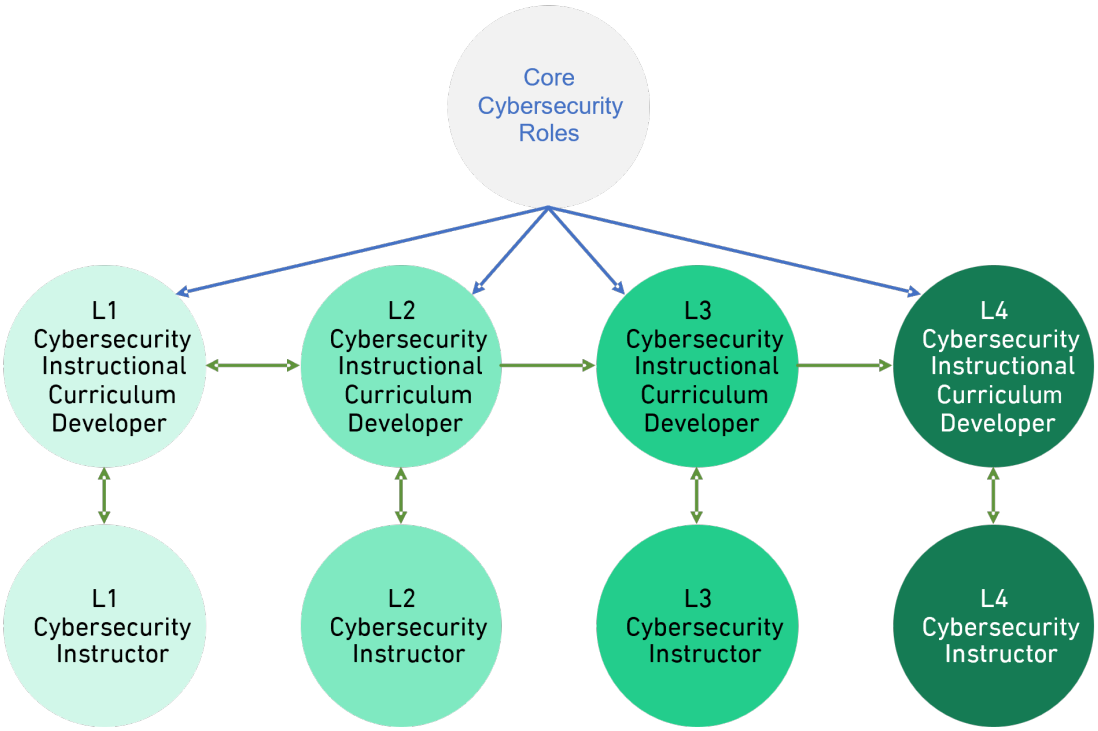

FIGURE 15: CYBERSECURITY INSTRUCTIONAL CURRICULUM DEVELOPER CAREER MAP

3.5.1 L1 Cybersecurity Instructional Curriculum Developer

Job Role Name: Cybersecurity Instructional Curriculum Developer (LWD-WD-002)	Job Level: Level 1
Role Description	Assists the team in developing, planning, coordinating and evaluating cybersecurity training, awareness, and education programs, courses, contents, methods and techniques based on instructional needs. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn the requirements of the role. Tasks will include supporting the design and execution of exercise scenarios and writing instructional materials to provide detailed guidance to the organization's staff or units.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate • L1 Core Cybersecurity Roles • L1 Cybersecurity Instructor	The next career step for someone in this role is one of the following: • L2 Cybersecurity Instructional Curriculum Developer • L1 Cybersecurity Instructor

TABLE 45: L1 CYBERSECURITY INSTRUCTIONAL CURRICULUM DEVELOPER

3.5.2 L2 Cybersecurity Instructional Curriculum Developer

Job Role Name: Cybersecurity Instructional Curriculum Developer (LWD-WD-002)	Job Level: Level 2
Role Description	Practitioner developing, planning, coordinating and evaluating cybersecurity training, awareness, and education programs, courses, contents, methods and techniques based on instructional needs. An individual in this role will carry oversee the work done by the L1 Cybersecurity Instructional Curriculum Developer, and will continue to develop their skills through practical application of their work. Tasks will include developing interactive learning exercises and an effective learning environment and developing or assisting in the development of training policies and protocols for cybersecurity training.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Core Cybersecurity Roles • L1 Cybersecurity Instructional Curriculum Developer • L2 Cybersecurity Instructor	The next career step for someone in this role is one of the following: • L3 Cybersecurity Instructional Curriculum Developer • L2 Cybersecurity Instructor

TABLE 46: L2 CYBERSECURITY INSTRUCTIONAL CURRICULUM DEVELOPER

3.5.3 L3 Cybersecurity Instructional Curriculum Developer

Job Role Name:	Job Level:
Cybersecurity Instructional Curriculum Developer (LWD-WD-002)	Level 3
Role Description	Senior Practitioner developing, planning, coordinating and evaluating cybersecurity training, awareness, and education programs, courses, contents, methods and techniques based on instructional needs. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Instructional Curriculum Developer. Tasks will include developing the goals and objectives for an organizational cybersecurity training curriculum and conducting periodic reviews and revisions of course content for accuracy, completeness, alignment, and currency.

Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Core Cybersecurity Roles • L2 Cybersecurity Instructional Curriculum Developer • L3 Cybersecurity Instructor	The next career step for someone in this role is one of the following: • L4 Cybersecurity Instructional Curriculum Developer • L3 Cybersecurity Instructor

TABLE 47: L3 CYBERSECURITY INSTRUCTIONAL CURRICULUM DEVELOPER

3.5.4 L4 Cybersecurity Instructional Curriculum Developer

Job Role Name:	Job Level:
Cybersecurity Instructional Curriculum Developer (LWD-WD-002)	Level 4
Role Description	Expert managing unit to develop, plan, coordinate and evaluate cybersecurity training, awareness, and education programs, courses, contents, methods and techniques based on instructional needs. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Instructional Curriculum Developer's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include developing the goals and objectives for an organizational cybersecurity training curriculum and evaluating instructional strategy and delivery options in conjunction with educators and trainers to develop the most effective organizational learning and development plan.

Career Progression (Pathway)	
The individual will have come from the following roles: • L4 Core Cybersecurity Roles • L3 Cybersecurity Instructional Curriculum Developer • L4 Cybersecurity Instructor	The next career step for someone in this role is one of the following: • L4 Cybersecurity Instructor

TABLE 48: L4 CYBERSECURITY INSTRUCTIONAL CURRICULUM DEVELOPER

3.6 Cybersecurity Instructor

The Cybersecurity Instructor teaches, trains, develops, and evaluates individuals in cybersecurity topics and awareness. This role requires certifications or training in cybersecurity education, instructional delivery methods, training evaluation, and foundational cybersecurity concepts, along with topic-specific expertise or certifications related to the subjects being taught.

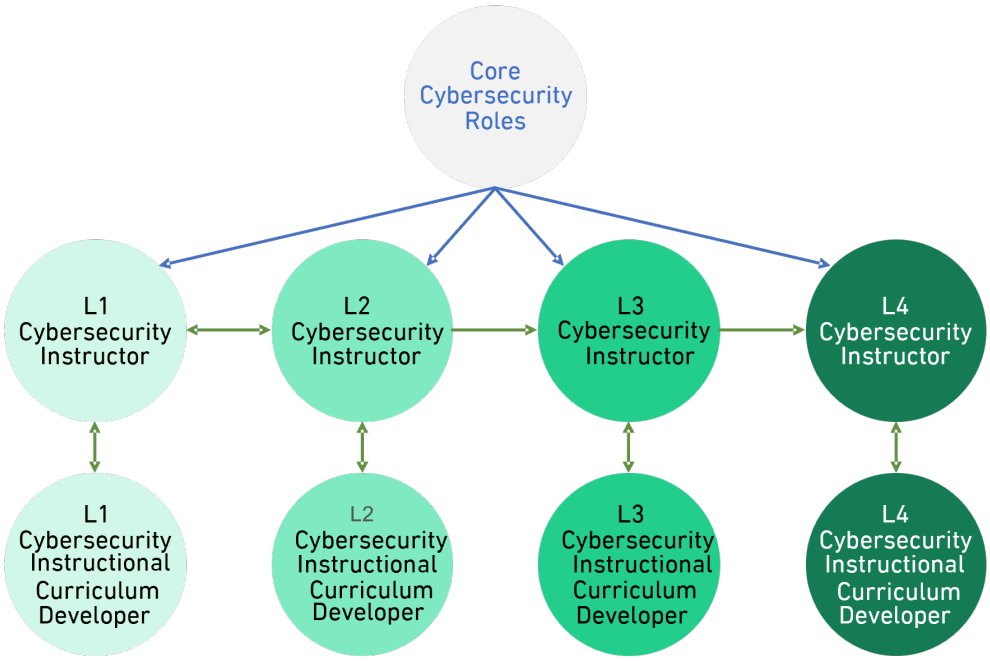

FIGURE 16: CYBERSECURITY INSTRUCTOR CAREER MAP

3.6.1 L1 Cybersecurity Instructor

Job Role Name: Cybersecurity Instructor (LWD-WD-002)	Job Level: Level 1
Role Description	Supports the team to provide assistance in teaching, training, developing and testing people in cybersecurity and awareness topics. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include supporting the design and execution of exercise scenarios and assisting the development of training curriculum and course content.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate • L1 Core Cybersecurity Roles • L1 Cybersecurity Instructional Curriculum Developer	The next career step for someone in this role is one of the following: • L2 Cybersecurity Instructor • L1 Cybersecurity Instructional Curriculum Developer

TABLE 49: L1 CYBERSECURITY INSTRUCTOR

3.6.2 L2 Cybersecurity Instructor

Job Role Name: Cybersecurity Instructor (LWD-WD-003)	Job Level: Level 2
Role Description	Practitioner who teaches, trains, develops and tests people in cybersecurity and awareness topics. An individual in this role will oversee the work done by the L1 Cybersecurity Instructor, and will continue to develop their skills through practical application of their work. Tasks will include writing instructional materials to provide detailed guidance to the organization's staff or units and developing or assisting in the development of course assignments..
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Core Cybersecurity Roles • L1 Cybersecurity Instructor • L2 Cybersecurity Instructional Curriculum Developer	The next career step for someone in this role is one of the following: • L3 Cybersecurity Instructor • L2 Cybersecurity Instructional Curriculum Developer

TABLE 50: L2 CYBERSECURITY INSTRUCTOR

3.6.3 L3 Cybersecurity Instructor

Job Role Name: Cybersecurity Instructor (LWD-WD-003)	Job Level: Level 3
Role Description	Senior Practitioner who teaches, trains, develops and tests people in cybersecurity and awareness topics. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Instructor. Tasks will include conducting learning needs assessments and identifying requirements and developing or assisting in the development of training policies and protocols for cybersecurity training.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Core Cybersecurity Roles • L2 Cybersecurity Instructor • L3 Cybersecurity Instructional Curriculum Developer	The next career step for someone in this role is one of the following: • L4 Cybersecurity Instructor • L3 Cybersecurity Instructional Curriculum Developer

TABLE 51: L3 CYBERSECURITY INSTRUCTOR

3.6.4 L4 Cybersecurity Instructor

Job Role Name: Cybersecurity Instructor (LWD-WD-003)	Job Level: Level 4
Role Description	Expert managing unit to teach, train, develop and test people in cybersecurity and awareness topics. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Instructor's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include designing training curriculum and course content based on the organization and workforce requirements and ensuring that training meets cybersecurity training, education, or awareness goals and objectives.
Career Progression (Pathway)	
The individual will have come from the following roles: • L4 Core Cybersecurity Roles • L3 Cybersecurity Instructor • L4 Cybersecurity Instructional Curriculum Developer	The next career step for someone in this role is one of the following: • L4 Cybersecurity Instructional Curriculum Developer

TABLE 52: L4 CYBERSECURITY INSTRUCTOR

4. Governance, Risk, Compliance and Laws

4.1 Cybersecurity Risk Officer

The Cybersecurity Risk Officer identifies, assesses, and manages an organization's cybersecurity risks to safeguard its information and technology assets in alignment with organizational policies, procedures, and applicable laws and regulations. This role requires certifications or training in risk management, cybersecurity governance, compliance, and threat assessment.

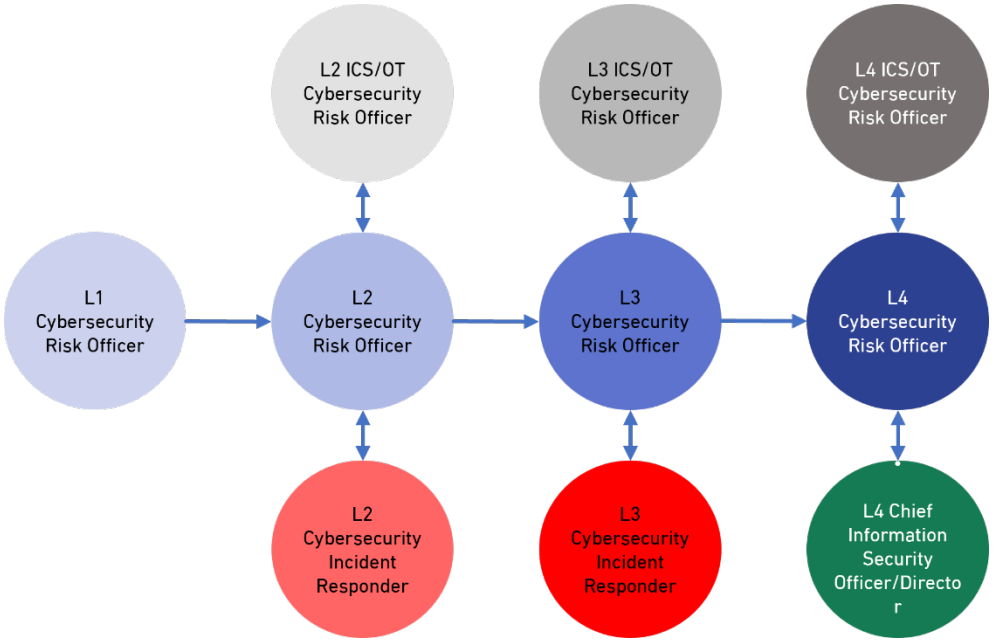

FIGURE 17: CYBERSECURITY RISK OFFICER CAREER MAP

4.1.1 L1 Cybersecurity Risk Officer

Job Role Name: Cybersecurity Risk Officer (GRCL-GRC-001)	Job Level: Level 1
Role Description	Supports a risk or compliance team in identifying, assessing and managing an organization's cybersecurity risks protecting its information and technology assets in line with organizational policies and procedures and related laws and regulations. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include carrying out cybersecurity risk assessments and working with others to implement and maintain a cybersecurity risk management program.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate	The next career step for someone in this role is one of the following: • L2 Cybersecurity Risk Officer

TABLE 53: L1 CYBERSECURITY RISK OFFICER

4.1.2 L2 Cybersecurity Risk Officer

Job Role Name: Cybersecurity Risk Officer (GRCL-GRC-001)	Job Level: Level 2
Role Description	Practitioner in identifying, assessing and managing an organization's cybersecurity risks protecting its information and technology assets in line with organizational policies and procedures and related laws and regulations. An individual in this role will oversee the work done by the L1 Cybersecurity Risk Officer, and will continue to develop their skills through practical application of their work. Tasks will include performing risk analysis whenever an application or system undergoes a major change and providing input to the risk management framework and related documentation.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Cybersecurity Risk Officer • L2 Cybersecurity Incident Responder • L2 ICS/OT Cybersecurity Risk Officer	The next career step for someone in this role is one of the following: • L3 Cybersecurity Risk Officer • L2 Cybersecurity Incident Responder • L2 ICS/OT Cybersecurity Risk Officer

TABLE 54: L2 CYBERSECURITY RISK OFFICER

4.1.3 L3 Cybersecurity Risk Officer

Job Role Name: Cybersecurity Risk Officer (GRCL-GRC-001)	Job Level: Level 3
Role Description	Senior Practitioner in identifying, assessing and managing an organization's cybersecurity risks protecting its information and technology assets in line with organizational policies and procedures and related laws and regulations. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Risk Officer. Tasks will include working with others to implement and maintain a cybersecurity risk management program and identifying and assigning individuals to specific roles associated with the execution of the Risk Management Framework.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Risk Officer • L3 Cybersecurity Incident Responder • L3 ICS/OT Cybersecurity Risk Officer	The next career step for someone in this role is one of the following: • L4 Cybersecurity Risk Officer • L3 Cybersecurity Incident Responder • L3 ICS/OT Cybersecurity Risk Officer

TABLE 55: L3 CYBERSECURITY RISK OFFICER

4.1.4 L4 Cybersecurity Risk Officer

Job Role Name: Cybersecurity Risk Officer (GRCL-GRC-001)	Job Level: Level 4
Role Description	Expert managing a unit to identify, assess and manage an organization's cybersecurity risks protecting its information and technology assets in line with organizational policies and procedures and related laws and regulations. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Risk Officer's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include effectively communicating cybersecurity risks and posture to senior management and ensuring cybersecurity risks are identified and managed appropriately through the organization's risk governance process.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Risk Officer • L4 ICS/OT Cybersecurity Risk Officer	The next career step for someone in this role is one of the following: • L4 Chief Information Security Officer/Director • L4 ICS/OT Cybersecurity Risk Officer

TABLE 56: L4 CYBERSECURITY RISK OFFICER

4.2 Cybersecurity Compliance Officer

The Cybersecurity Compliance Officer ensures that an organization's cybersecurity program adheres to applicable requirements, policies, and standards. This role requires certifications or training in compliance management, cybersecurity auditing, regulatory frameworks, and policy evaluation.

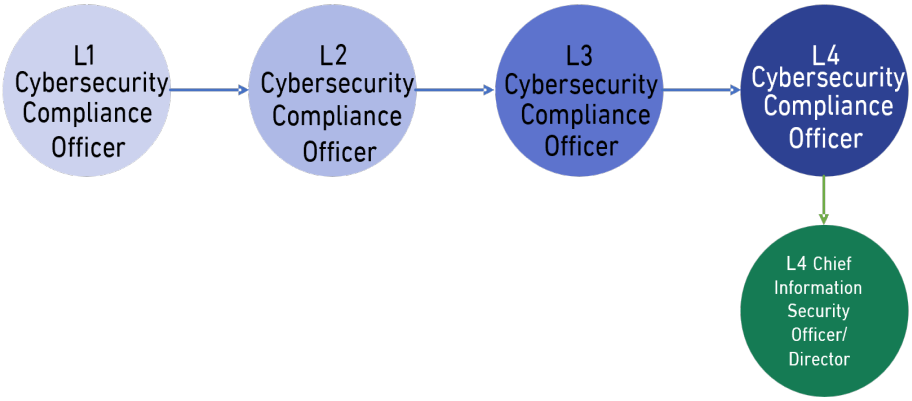

FIGURE 18: CYBERSECURITY COMPLIANCE OFFICER CAREER MAP

4.2.1 L1 Cybersecurity Compliance Officer

Job Role Name: Cybersecurity Compliance Officer (GRCL-GRC-003)	Job Level: Level 1
Role Description	Supports a risk or compliance team in ensuring an organization's cybersecurity program complies with applicable requirements, policies and standards. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include providing support to compliance activities as necessary.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate	The next career step for someone in this role is one of the following: • L2 Cybersecurity Compliance Officer

TABLE 57: L1 CYBERSECURITY COMPLIANCE OFFICER

4.2.2 L2 Cybersecurity Compliance Officer

Job Role Name: Cybersecurity Compliance Officer (GRCL-GRC-003)	Job Level: Level 2
Role Description	Practitioner in ensuring an organization's cybersecurity program complies with applicable requirements, policies and standards. An individual in this role will oversee the work done by the L1 Cybersecurity Compliance Officer, and will continue to develop their skills through practical application of their work. Tasks will include evaluating cybersecurity aspects of contracts to ensure compliance with financial, contractual, legal and regulatory requirements and ensuring that any products implemented to manage cybersecurity risks have been effectively evaluated and authorized for use.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Cybersecurity Compliance Officer	The next career step for someone in this role is one of the following: • L3 Cybersecurity Compliance Officer

TABLE 58: L2 CYBERSECURITY COMPLIANCE OFFICER

4.2.3 L3 Cybersecurity Compliance Officer

Job Role Name: Cybersecurity Compliance Officer (GRCL-GRC-003)	Job Level: Level 3
Role Description	Senior Practitioner in ensuring an organization's cybersecurity program complies with applicable requirements, policies and standards. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Compliance Officer. Tasks will include monitoring and evaluating a system's compliance with cybersecurity, resilience, and dependability requirements and providing an accurate technical evaluation of software applications, systems, or networks, and documenting their compliance with agreed cybersecurity requirements.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Compliance Officer	The next career step for someone in this role is one of the following: • L4 Cybersecurity Compliance Officer

TABLE 59: L3 CYBERSECURITY COMPLIANCE OFFICER

4.2.4 L4 Cybersecurity Compliance Officer

Job Role Name: Cybersecurity Policy Officer (GRCL-GRC-003)		Job Level: Level 4
Role Description	Expert managing a unit to ensure an organization's cybersecurity program complies with applicable requirements, policies and standards. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Compliance Officer's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include developing cybersecurity compliance processes and audits for services provided by third parties and cooperating with relevant regulatory agencies and other legal entities in any compliance reviews or investigations.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L3 Cybersecurity Compliance Officer		The next career step for someone in this role is one of the following: • L4 Chief Information Security Officer/Director

TABLE 60: L4 CYBERSECURITY COMPLIANCE OFFICER

4.3 Cybersecurity Policy Officer

The Cybersecurity Policy Officer develops, updates, and maintains cybersecurity policies to support and align with an organization's cybersecurity requirements. This role requires certifications or training in cybersecurity policy development, regulatory compliance, governance frameworks, and the strategic alignment of cybersecurity objectives.

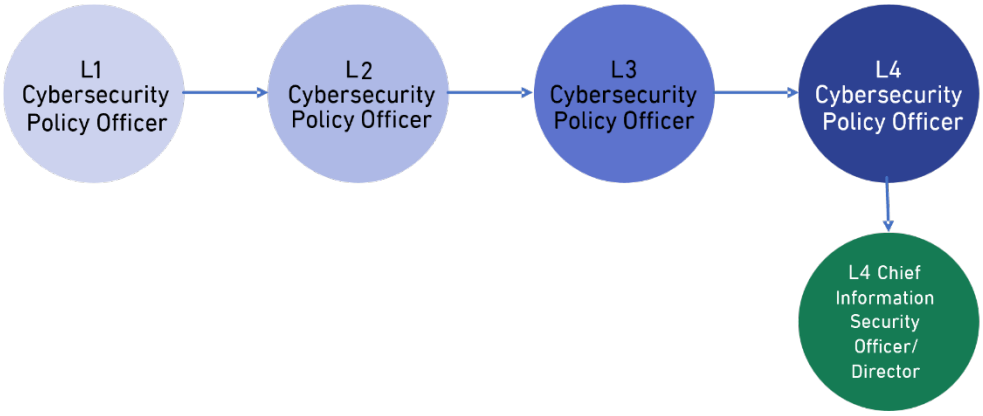

FIGURE 19: CYBERSECURITY POLICY OFFICER CAREER MAP

4.3.1 L1 Cybersecurity Policy Officer

Job Role Name: Cybersecurity Policy Officer (GRCL-GRC-003)	Job Level: Level 1
Role Description	Supports a risk or compliance team in developing, updating and maintaining cybersecurity policies to support and align with an organization's cybersecurity requirements. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include reviewing, conducting, or participating in audits of cyber programs and projects.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate	The next career step for someone in this role is one of the following: • L2 Cybersecurity Policy Officer

TABLE 61: L1 CYBERSECURITY POLICY OFFICER

4.3.2 L2 Cybersecurity Policy Officer

Job Role Name: Cybersecurity Policy Officer (GRCL-GRC-003)	Job Level: Level 2
Role Description	Practitioner in developing, updating and maintaining cybersecurity policies to support and align with an organization's cybersecurity requirements. An individual in this role will oversee the work done by the L1 Cybersecurity Policy Officer, and will continue to develop their skills through practical application of their work. Tasks will include developing cybersecurity policies and related documentation and assisting with the review of existing and proposed policies and related documentation with stakeholders.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Cybersecurity Policy Officer	The next career step for someone in this role is one of the following: • L3 Cybersecurity Policy Officer

TABLE 62: L2 CYBERSECURITY POLICY OFFICER

4.3.3 L3 Cybersecurity Policy Officer

Job Role Name: Cybersecurity Policy Officer (GRCL-GRC-003)	Job Level: Level 3
Role Description	Senior Practitioner in developing, updating and maintaining cybersecurity policies to support and align with an organization's cybersecurity requirements. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Policy Officer. Tasks will include creating and publishing the organization's cybersecurity policy and monitoring how effectively cybersecurity policies, principles, and practices are implemented in the delivery of planning and management services.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Policy Officer	The next career step for someone in this role is one of the following: • L4 Cybersecurity Policy Officer

TABLE 63: L3 CYBERSECURITY POLICY OFFICER

4.3.4 L4 Cybersecurity Policy Officer

Job Role Name: Cybersecurity Policy Officer (GRCL-GRC-003)	Job Level: Level 4
Role Description	Expert managing a unit to develop, update and maintain cybersecurity policies to support and align with an organization's cybersecurity requirements. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Policy Officer's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include ensuring that cybersecurity workforce management policies and processes comply with legal and organizational requirements and promoting awareness of cyber policy and strategy as appropriate among the organization's management.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Policy Officer	The next career step for someone in this role is one of the following: • L4 Chief Information Security Officer/Director

TABLE 64: L4 CYBERSECURITY POLICY OFFICER

4.4 Security Controls Assessor

The Security Controls Assessor analyzes and evaluates cybersecurity controls to determine their effectiveness. This role requires certifications or training in security control assessment, cybersecurity auditing, risk analysis, and evaluating cybersecurity measures.

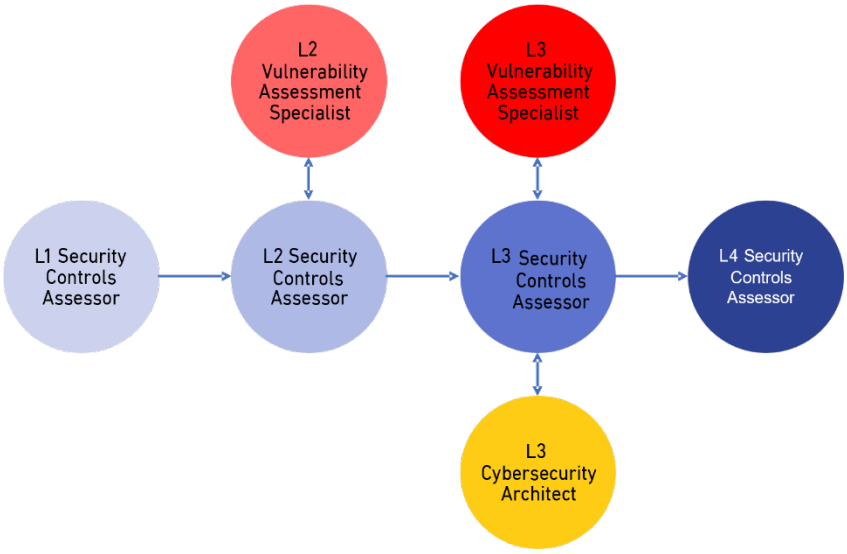

FIGURE 20: SECURITY CONTROL ASSESSOR CAREER MAP

4.4.1 L1 Security Controls Assessor

Job Role Name: Security Controls Assessor (GRCL-GRC-004)	Job Level: Level 1
Role Description	Assists the assessments team in analyzing cybersecurity controls and assessing their effectiveness. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include assessing the effectiveness of cybersecurity controls and assessing the configuration management process.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate	The next career step for someone in this role is one of the following: • L2 Security Controls Assessor

TABLE 65: L1 SECURITY CONTROLS ASSESSOR

4.4.2 L2 Security Controls Assessor

Job Role Name: Security Controls Assessor (GRCL-GRC-004)	Job Level: Level 2
Role Description	Practitioner in analyzing cybersecurity controls and assessing their effectiveness. An individual in this role will oversee the work done by the L1 Security Controls Assessor and will continue to develop their skills through practical application of their work. Tasks will include performing cybersecurity reviews and identifying security gaps in security architecture to inform risk mitigation strategies.

Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Security Controls Assessor • L2 Vulnerability Assessment Specialist	The next career step for someone in this role is one of the following: • L3 Security Controls Assessor • L2 Vulnerability Assessment Specialist

TABLE 66: L2 SECURITY CONTROLS ASSESSOR

4.4.3 L3 Security Controls Assessor

Job Role Name: Security Controls Assessor (GRCL-GRC-004)	Job Level: Level 3
Role Description	Senior Practitioner in analyzing cybersecurity controls and assessing their effectiveness. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Security Controls Assessor. Tasks will include planning and conducting cybersecurity authorization reviews and assurance case development for initial installation of systems and networks, and reviewing risk registers or other similar documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.

Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Security Controls Assessor • L3 Vulnerability Assessment Specialist • L3 Cybersecurity Architect	The next career step for someone in this role is one of the following: • L4 Security Controls Assessor • L3 Cybersecurity Architect • L3 Vulnerability Assessment Specialist

TABLE 67: L3 SECURITY CONTROLS ASSESSOR

4.4.4 L4 Security Controls Assessor

Job Role Name: Security Controls Assessor (GRCL-GRC-004)	Job Level: Level 4
Role Description	Expert managing a unit to analyze cybersecurity controls and assess their effectiveness. An individual in this role will be responsible for providing oversight for much of the L3 Security Controls Assessor's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include ensuring that cybersecurity risks are identified and managed appropriately through the organization's risk governance process and ensuring that the organization's cybersecurity requirements are considered in mergers, acquisitions, outsourcing and other operations involving third parties.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Security Controls Assessor	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 68: L4 SECURITY CONTROLS ASSESSOR

4.5 Cybersecurity Auditor

The Cybersecurity Auditor designs, conducts, and manages cybersecurity audits to assess an organization's compliance with applicable requirements, policies, standards, and controls. This role requires certifications or training in cybersecurity auditing, compliance frameworks, risk analysis, and evaluating security controls. Responsibilities include reviewing system configurations, ensuring compliance with regulatory standards and organizational policies, and preparing audit reports with actionable recommendations.

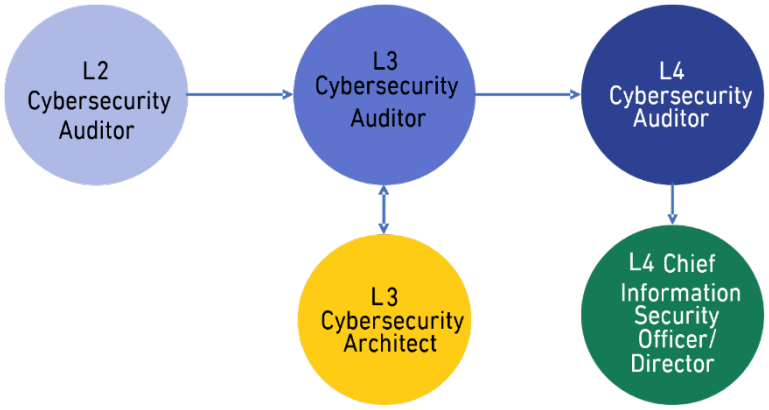

FIGURE 21: CYBERSECURITY AUDITOR CAREER MAP

4.5.1 L2 Cybersecurity Auditor

Job Role Name: Cybersecurity Auditor (GRCL-GRC-005)	Job Level: Level 2
Role Description	Practitioner in designing, performing and managing cybersecurity audits to assess an organization's compliance with applicable requirements, policies, standards and controls. Prepares audit reports and communicates them to authorized parties. An individual in this role will develop their skills through practical application of their work. Tasks will include performing risk analysis whenever an application or system undergoes a major change and tracking audit findings and recommendations to ensure that appropriate mitigation actions are taken.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate	The next career step for someone in this role is one of the following: • L3 Cybersecurity Auditor

TABLE 69: L2 CYBERSECURITY AUDITOR

4.5.2 L3 Cybersecurity Auditor

Job Role Name: Cybersecurity Auditor (GRCL-GRC-005)	Job Level: Level 3
Role Description	Senior Practitioner in designing, performing and managing cybersecurity audits to assess an organization's compliance with applicable requirements, policies, standards and controls. Prepares audit reports and communicates them to authorized parties. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Auditor. Tasks will include preparing cybersecurity audit reports that identify technical and procedural findings, and include recommended remediation strategies and solutions, and ensuring an audit log of evidence of security measures is maintained.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Auditor • L3 Cybersecurity Architect	The next career step for someone in this role is one of the following: • L4 Cybersecurity Auditor • L3 Cybersecurity Architect

TABLE 70: L3 CYBERSECURITY AUDITOR

4.5.3 L4 Cybersecurity Auditor

Job Role Name: Cybersecurity Auditor (GRCL-GRC-005)		Job Level: Level 4
Role Description	Expert managing a unit to design, perform and manage cybersecurity audits to assess an organization's compliance with applicable requirements, policies, standards and controls. Prepares audit reports and communicates them to authorized parties. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Auditor's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include maintaining knowledge of applicable cybersecurity defense policies, regulations, and compliance documents as they pertain to cybersecurity defense auditing and developing cybersecurity compliance processes and audits for services provided by third parties.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L3 Cybersecurity Auditor		The next career step for someone in this role is one of the following: • L4 Chief Information Security Officer / Director

TABLE 71: L4 CYBERSECURITY AUDITOR

4.6 Cybersecurity Legal Specialist

The Cybersecurity Legal Specialist provides legal services related to cyber laws and regulations. This role requires certifications or training in cybersecurity laws and regulations, cybersecurity auditing, compliance frameworks, and the legal aspects of cybersecurity policy development.

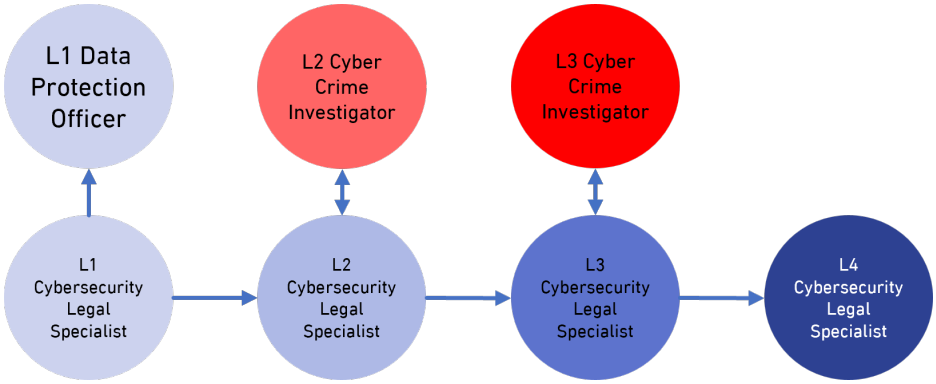

FIGURE 22: CYBERSECURITY LEGAL SPECIALIST CAREER MAP

4.6.1 L1 Cybersecurity Legal Specialist

Job Role Name: Cybersecurity Legal Specialist (GRCL-LDP- 001)	Job Level: Level 1
Role Description	Supports the organization by providing legal services on topics related to cyber laws and regulations. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include acquiring and maintaining a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures etc. and assisting with the implementation of new or revised laws, regulations, executive orders etc. as they relate to cybersecurity policies and other documentation.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate	The next career step for someone in this role is one of the following: • L2 Cybersecurity Legal Specialist • L1 Data Protection Officer

TABLE 72: L1 CYBERSECURITY LEGAL SPECIALIST

4.6.2 L2 Cybersecurity Legal Specialist

Job Role Name: Cybersecurity Legal Specialist (GRCL-LDP- 001)	Job Level: Level 2
Role Description	Practitioner in providing legal services on topics related to cyber laws and regulations. An individual in this role will oversee the work done by the L1 Cybersecurity Legal Specialist and will continue to develop their skills through practical application of their work. Tasks will include interpreting and applying laws, regulations, policies, standards, or procedures as necessary and maintaining awareness of applicable data protection laws, regulations and accreditation standards.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Cybersecurity Legal Specialist • L2 Cyber Crime Investigator	The next career step for someone in this role is one of the following: • L3 Cybersecurity Legal Specialist • L2 Cyber Crime Investigator

TABLE 73: L2 CYBERSECURITY LEGAL SPECIALIST

4.6.3 L3 Cybersecurity Legal Specialist

Job Role Name: Cybersecurity Legal Specialist (GRCL-LDP- 001)	Job Level: Level 3
Role Description	Senior Practitioner in providing legal services on topics related to cyber laws and regulations. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Legal Specialist. Tasks will include evaluating cybersecurity aspects of contracts to ensure compliance with financial, contractual, legal and regulatory requirements and understanding and communicating an organization's cybersecurity status during legal and regulatory scrutiny.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Legal Specialist • L3 Cyber Crime Investigator	The next career step for someone in this role is one of the following: • L4 Cybersecurity Legal Specialist • L3 Cyber Crime Investigator

TABLE 74: L3 CYBERSECURITY LEGAL SPECIALIST

4.6.4 L4 Cybersecurity Legal Specialist

Job Role Name: Cybersecurity Legal Specialist (GRCL-LDP- 001)	Job Level: Level 4
Role Description	Expert managing a unit to provide legal services on topics related to cyber laws and regulations. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Legal Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include providing cybersecurity expertise to the framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance and providing cybersecurity related guidance in the preparation of legal and other relevant documents.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Legal Specialist	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 75: L4 CYBERSECURITY LEGAL SPECIALIST

4.7 Data Protection Officer

The Data Protection Officer studies personal data schemes and applicable data protection laws and regulations, analyzes data protection risks, and develops and oversees the implementation of an organization's data protection compliance program and internal policies. This role requires certifications or training in data protection regulations, compliance frameworks, and personal data protection strategies. The officer also supports the organization's response to data protection incidents.

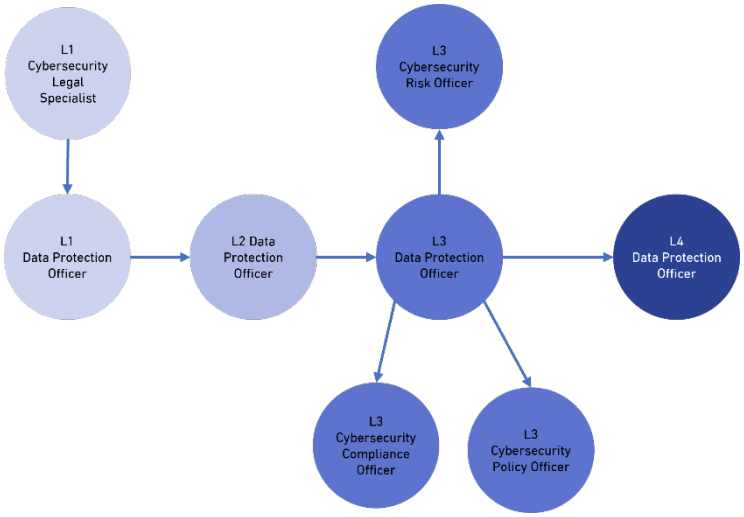

FIGURE 23: DATA PROTECTION OFFICER CAREER MAP

4.7.1 L1 Data Protection Officer

Job Role Name: Data Protection Officer (GRCL-LDP- 002)	Job Level: Level 1
Role Description	Assists the governance, risk, compliance and legal teams by studying personal data schemes and the applicable data protection laws and regulations and analyzing data protection risks. They develop and oversee the implementation of an organization's data protection compliance program and internal policies. They support organizational response to data protection incident. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include conducting data protection risk assessments, ensuring that Personally Identifiable Information (PII) is appropriately protected, and ensuring that training and awareness activities are delivered on a regular basis
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate • L1 Cybersecurity Legal Specialist	The next career step for someone in this role is one of the following: • L2 Data Protection Officer

TABLE 76: L1 DATA PROTECTION OFFICER

4.7.2 L2 Data Protection Officer

Job Role Name: Data Protection Officer (GRCL-LDP- 002)	Job Level: Level 2
Role Description	Practitioner in studying personal data schemes and the applicable data protection laws and regulations and analyzing data protection risks. They develop and oversee the implementation of an organization's data protection compliance program and internal policies. They support organizational response to data protection incident. An individual in this role will oversee the work done by the L1 Data Protection Officer, and will continue to develop their skills through practical application of their work. Tasks will include working with business teams and senior management to ensure awareness of best practices relating to data protection and developing and documenting procedures for reporting self-disclosures of any evidence of data protection violations.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Data Protection Officer	The next career step for someone in this role is one of the following: • L3 Data Protection Officer

TABLE 77: L2 DATA PROTECTION OFFICER

4.7.3 L3 Data Protection Officer

Job Role Name: Data Protection Officer (GRCL-LDP- 002)	Job Level: Level 3
Role Description	Senior Practitioner in studying personal data schemes and the applicable data protection laws and regulations and analyzing data protection risks. They develop and oversee the implementation of an organization's data protection compliance program and internal policies. They supports organizational response to data protection incidents. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Data Protection Officer. Tasks will include working with legal and HR teams to develop appropriate sanctions for failure to comply with the organization's data protection policies and procedures and establishing and maintaining a risk management and compliance framework for data protection.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Data Protection Officer	The next career step for someone in this role is one of the following: • L4 Data Protection Officer • L3 Cybersecurity Risk Officer • L3 Cybersecurity Compliance Officer • L3 Cybersecurity Policy Officer

TABLE 78: L3 DATA PROTECTION OFFICER

4.7.4 L4 Data Protection Officer

Job Role Name: Data Protection Officer (GRCL-LDP- 002)	Job Level: Level 4
Role Description	Expert managing a unit to study personal data schemes and the applicable data protection laws and regulations and analyzing data protection risks. They develop and oversee the implementation of an organization's data protection compliance program and internal policies. They support organizational response to data protection incidents. An individual in this role will be responsible for providing oversight for much of the L3 Data Protection Officer's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include providing leadership for the organization's data protection program and directing and overseeing data protection specialists and coordinate data protection programs with senior management to ensure consistency across the organization.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Data Protection Officer	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 79: L4 DATA PROTECTION OFFICER

5. Protection and Defense

5.1 Cybersecurity Defense Analyst

The Cybersecurity Defense Analyst uses data from cyber defense tools to analyze events within their organization, aiming to detect and mitigate cyber threats. This role requires certifications or training in network defense, threat detection, incident analysis, and cybersecurity monitoring tools.

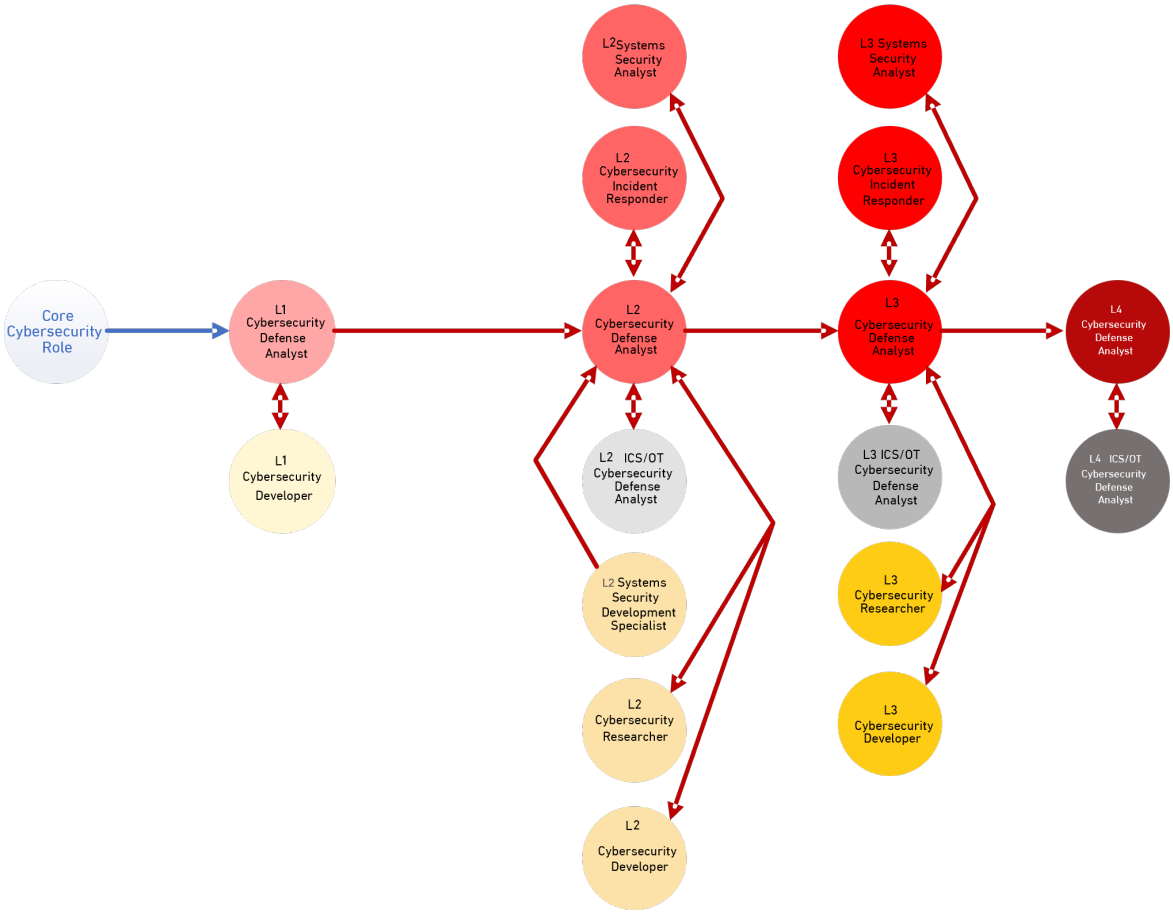

FIGURE 24: CYBERSECURITY DEFENSE ANALYST CAREER MAP

5.1.1 L1 Cybersecurity Defense Analyst

Job Role Name: Cybersecurity Defense Analyst (PD-D-001)	Job Level: Level 1
Role Description	Assists the team by using data collected from cyber defense tools to provide monitoring and first line triage of events that occur within their organization to detect and mitigate cyber threats. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include assisting in the construction of signatures for implementation on cybersecurity network tools to respond to new or observed threats within the environment and providing summary reports of network events and other cybersecurity-relevant activities in line with organizational policies and requirements.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate • Core Cybersecurity Role • L1 Cybersecurity Developer	The next career step for someone in this role is one of the following: • L1 Cybersecurity Developer • L2 Cybersecurity Defense Analyst

TABLE 80: L1 CYBERSECURITY DEFENSE ANALYST

5.1.2 L2 Cybersecurity Defense Analyst

Job Role Name: Cybersecurity Defense Analyst (PD-D-001)	Job Level: Level 2
Role Description	Assists the team by using data collected from cyber defense tools to provide monitoring and first line triage of events that occur within their organization to detect and mitigate cyber threats. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include assisting in the construction of signatures for implementation on cybersecurity network tools to respond to new or observed threats within the environment and providing summary reports of network events and other cybersecurity-relevant activities in line with organizational policies and requirements.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Cybersecurity Defense Analyst • L2 Cybersecurity Developer • L2 Cybersecurity Incident Responder • L2 Cybersecurity Researcher • L2 Systems Security Analyst • L2 Systems Security Development Specialist • L2 ICS/OT Cybersecurity Defense Analyst	The next career step for someone in this role is one of the following: • L3 Cybersecurity Defense Analyst • L2 Cybersecurity Developer • L2 Cybersecurity Incident Responder • L2 Cybersecurity Researcher • L2 Systems Security Analyst • L2 ICS/OT Cybersecurity Defense Analyst

TABLE 81: L2 CYBERSECURITY DEFENSE ANALYST

5.1.3 L3 Cybersecurity Defense Analyst

Job Role Name: Cybersecurity Defense Analyst (PD-D-001)	Job Level: Level 3
Role Description	Senior Practitioner using data collected from cyber defense tools to analyze events that occur within their organization to detect and mitigate cyber threats. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Defense Analyst. Tasks will include correlating information from multiple sources to understand situation and determine the effectiveness of an observed attack and performing cybersecurity reviews, and identify security gaps in security architecture to inform risk mitigation strategies.

Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Defense Analyst • L3 Cybersecurity Developer • L3 Cybersecurity Researcher • L3 Systems Security Analyst • L3 ICS/OT Cybersecurity Defense Analyst • L3 Cybersecurity Incident Responder	The next career step for someone in this role is one of the following: • L4 Cybersecurity Defense Analyst • L3 Cybersecurity Incident Responder • L3 Cybersecurity Researcher • L3 Systems Security Analyst • L3 ICS/OT Cybersecurity Defense Analyst • L3 Cybersecurity Developer

TABLE 82: L3 CYBERSECURITY DEFENSE ANALYST

5.1.4 L4 Cybersecurity Defense Analyst

Job Role Name: Cybersecurity Defense Analyst (PD-D-001)	Job Level: Level 4
Role Description	Expert managing a unit to use data collected from cyber defense tools to analyze events that occur within their organization to detect and mitigate cyber threats. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Defense Analyst's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include making cybersecurity recommendations to leadership based on significant threats and vulnerabilities and assessing the adequacy of access controls against organizational policies.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Defense Analyst • L4 ICS/OT Cybersecurity Defense Analyst	The next career step for someone in this role is one of the following: • L4 ICS/OT Cybersecurity Defense Analyst

TABLE 83: L4 CYBERSECURITY DEFENSE ANALYST

5.2 Cybersecurity Infrastructure Specialist

The Cybersecurity Infrastructure Specialist tests, implements, deploys, maintains, and administers hardware and software to protect and defend systems and networks against cybersecurity threats. This role requires certifications or training in system and network administration, cybersecurity infrastructure management, security controls implementation, and hardware/software deployment.

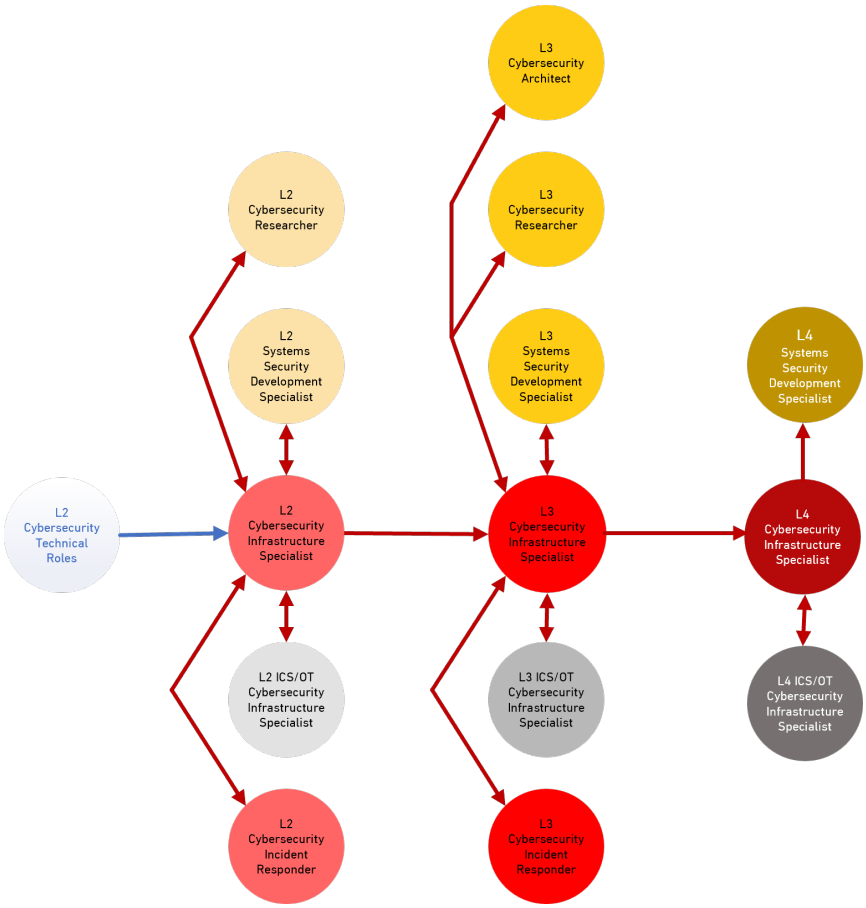

FIGURE 25: CYBERSECURITY INFRASTRUCTURE SPECIALIST CAREER MAP

5.2.1 L2 Cybersecurity Infrastructure Specialist

Job Role Name: Cybersecurity Infrastructure Specialist (PD- D-002)	Job Level: Level 2
Role Description	Practitioner assisting in testing, implementing, deploying, maintaining, and administering hardware and software that protect systems and networks against cybersecurity threats. An individual in this role will carry out some of the basic tasks under supervision and will continue to develop their skills through practical application of their work. Tasks will include supporting the configuration and management of cybersecurity infrastructure, performing system checks, and assisting with updating rules and signatures for cyber defense applications.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Technical Roles	The next career step for someone in this role is one of the following: • L3 Cybersecurity Infrastructure Specialist
• L2 Cybersecurity Incident Responder • L2 Cybersecurity Researcher • L2 Systems Security Development Specialist • L2 ICS/OT Cybersecurity Infrastructure Specialist	• L2 Cybersecurity Incident Responder • L2 Cybersecurity Researcher • L2 Systems Security Development Specialist • L2 ICS/OT Cybersecurity Infrastructure Specialist

TABLE 84: L2 CYBERSECURITY INFRASTRUCTURE SPECIALIST

5.2.2 L3 Cybersecurity Infrastructure Specialist

Job Role Name: Cybersecurity Infrastructure Specialist (PD- D-002)	Job Level: Level 3
Role Description	Senior Practitioner testing, implementing, deploying, maintaining and administering hardware and software that is protecting and defending systems and networks against cybersecurity threats. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Infrastructure Specialist. Tasks will include performing system administration on specialized cybersecurity applications and systems and managing and administering the updating of rules and signatures for cyber defense applications.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Infrastructure Specialist • L3 Cybersecurity Architect • L3 Cybersecurity Incident Responder • L3 Cybersecurity Researcher • L3 Systems Security Development Specialist • L3 ICS/OT Cybersecurity Infrastructure Specialist	The next career step for someone in this role is one of the following: • L4 Cybersecurity Infrastructure Specialist • L3 Cybersecurity Architect • L3 Cybersecurity Incident Responder • L3 Cybersecurity Researcher • L3 ICS/OT Cybersecurity Infrastructure Specialist • L3 Systems Security Development Specialist

TABLE 85: L3 CYBERSECURITY INFRASTRUCTURE SPECIALIST

5.2.3 L4 Cybersecurity Infrastructure Specialist

Job Role Name: Cybersecurity Infrastructure Specialist (PD- D-002)	Job Level: Level 4
Role Description	Expert managing a unit to test, implement, deploy, maintain and administer hardware and software that is defending systems and networks against cybersecurity threats. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Infrastructure Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and resources, and implementing risk management framework and security assessment and authorization requirements for dedicated cyber defense systems within the organization.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Infrastructure Specialist • L4 ICS/OT Cybersecurity Infrastructure Specialist • L4 Systems Security Development Specialist	The next career step for someone in this role is one of the following: • L4 ICS/OT Cybersecurity Infrastructure Specialist • L4 Systems Security Development Specialist

TABLE 86: L4 CYBERSECURITY INFRASTRUCTURE SPECIALIST

5.3 Cybersecurity Specialist

The Cybersecurity Specialist provides general cybersecurity support and assists with various cybersecurity tasks. This role requires certifications or training in cybersecurity fundamentals, threat analysis, vulnerability assessment, and cybersecurity operations support.

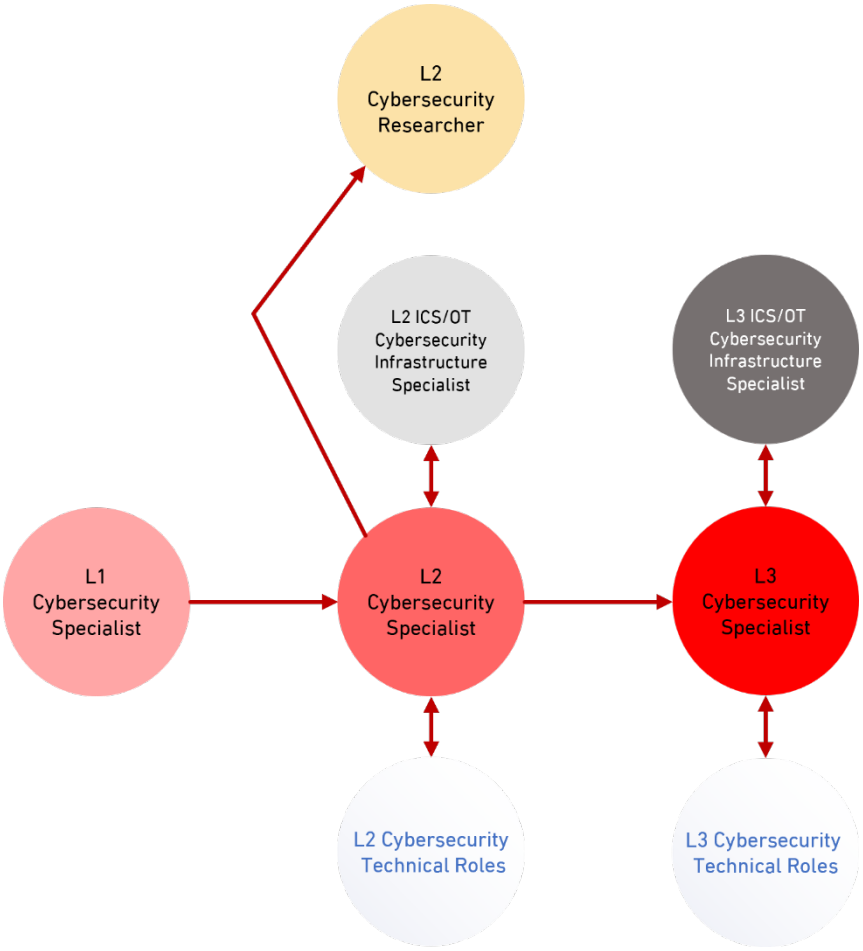

FIGURE 26: CYBERSECURITY SPECIALIST CAREER MAP

5.3.1 L1 Cybersecurity Specialist

Job Role Name: Cybersecurity Specialist (PD-D-003)	Job Level: Level 1
Role Description	Supports the team by providing general cybersecurity support. Assists in cybersecurity tasks. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include correlating incident data to identify vulnerabilities and providing summary reports of network events and other cybersecurity-relevant activities in line with organizational policies and requirements.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate	The next career step for someone in this role is one of the following: • L2 Cybersecurity Specialist

TABLE 87: L1 CYBERSECURITY SPECIALIST

5.3.2 L2 Cybersecurity Specialist

Job Role Name: Cybersecurity Specialist (PD-D-003)	Job Level: Level 2
Role Description	Practitioner providing general cybersecurity support. Assists in cybersecurity tasks. An individual in this role will oversee the work done by the L1 Cybersecurity Specialist, and will continue to develop their skills through practical application of their work. Tasks will include analyzing log files from multiple sources to identify possible threats to network security and analyzing and reporting cyber defense trends.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Cybersecurity Specialist • L2 Cybersecurity Technical Roles • L2 ICS/OT Cybersecurity Infrastructure Specialist	The next career step for someone in this role is one of the following: • L3 Cybersecurity Specialist • L2 Cybersecurity Technical Roles • L2 Cybersecurity Researcher • L2 ICS/OT Cybersecurity Infrastructure Specialist

TABLE 88: L2 CYBERSECURITY SPECIALIST

5.3.3 L3 Cybersecurity Specialist

Job Role Name: Cybersecurity Specialist (PD-D-003)	Job Level: Level 3
Role Description	Senior Practitioner managing a team or mentoring others providing general cybersecurity support. Leads in cybersecurity tasks. An individual in this role will be responsible for providing oversight for much of the L2 Cybersecurity Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include assessing and monitoring the cybersecurity of the organization's system implementation and testing practices and performing technical and nontechnical risk and vulnerability assessments of organizational technology environments.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Specialist • L3 Cybersecurity Technical Roles • L3 ICS/OT Cybersecurity Infrastructure Specialist	The next career step for someone in this role is one of the following: • L3 Cybersecurity Technical Roles • L3 ICS/OT Cybersecurity Infrastructure Specialist

TABLE 89: L3 CYBERSECURITY SPECIALIST

5.4 Cryptography Specialist

The Cryptography Specialist develops, evaluates, and analyzes cryptographic systems and algorithms, identifying weaknesses and recommending improvements. This role requires certifications or training in cryptographic systems design, encryption and decryption techniques, secure data management, and cryptographic algorithm analysis.

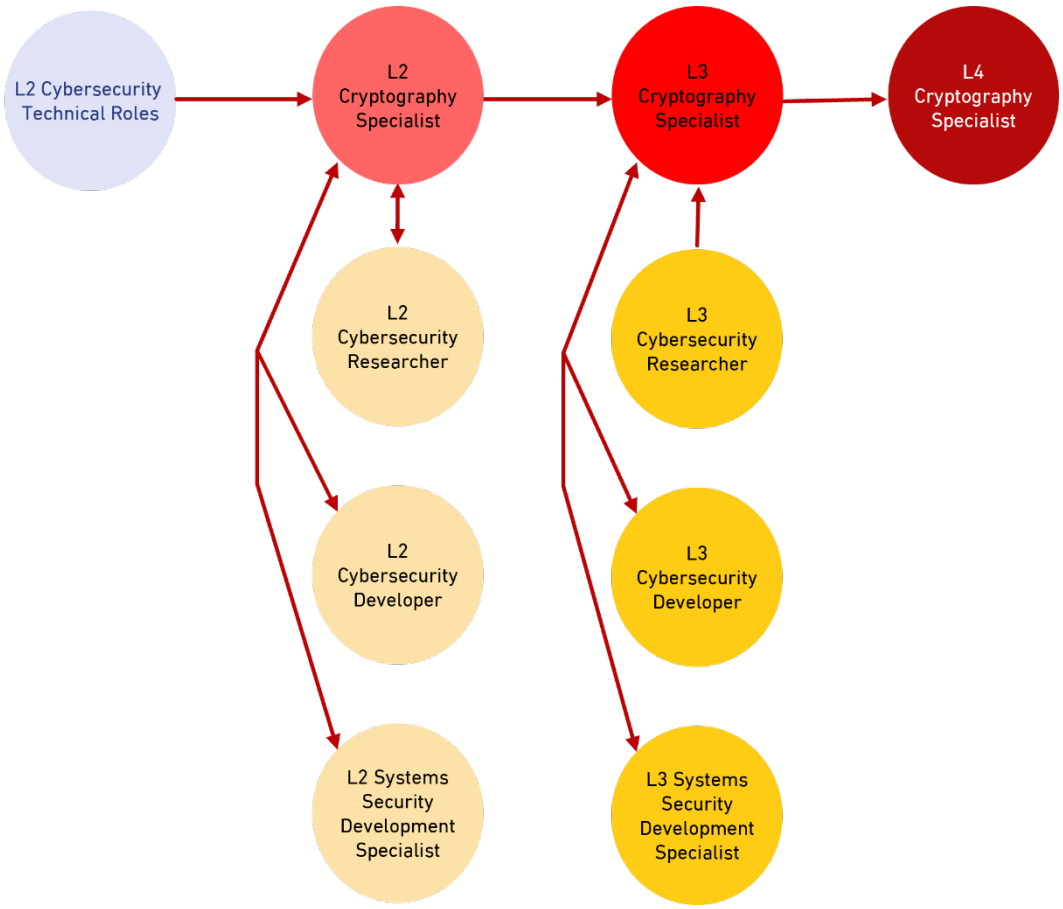

FIGURE 27: CRYPTOGRAPHY SPECIALIST CAREER MAP

5.4.1 L2 Cryptography Specialist

Job Role Name: Cryptography Specialist (PD-P-001)	Job Level: Level 2
Role Description	Practitioner assisting in the development, evaluation, and implementation of cryptographic systems and algorithms to protect organizational data and communications. An individual in this role will carry out some of the basic tasks, under supervision, and will continue to develop their skills through practical application of their work. Tasks will include performing encryption and decryption of data, supporting the implementation of cryptographic measures, and analyzing the effectiveness of existing cryptographic systems.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Technical Roles • L2 Cybersecurity Developer • L2 Cybersecurity Researcher • L2 Systems Security Development Specialist	The next career step for someone in this role is one of the following: • L3 Cryptography Specialist • L2 Cybersecurity Developer • L2 Cybersecurity Researcher • L2 Systems Security Development Specialist

TABLE 90: L2 CRYPTOGRAPHY SPECIALIST

5.4.2 L3 Cryptography Specialist

Job Role Name: Cryptography Specialist (PD-P-001)	Job Level: Level 3
Role Description	Senior Practitioner managing a team or mentoring others to develop, evaluate, analyze and identify weaknesses of, and improvements to, cryptography systems and algorithms. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cryptography Specialist. Tasks will include performing technical decryption of seized data and implementing system security measures in accordance with established procedures.

Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cryptography Specialist • L3 Cybersecurity Developer • L3 Cybersecurity Researcher • L3 Systems Security Development Specialist	The next career step for someone in this role is one of the following: • L4 Cryptography Specialist • L3 Cybersecurity Developer • L3 Cybersecurity Researcher • L3 Systems Security Development Specialist

TABLE 91: L3 CRYPTOGRAPHY SPECIALIST

5.4.3 L4 Cryptography Specialist

Job Role Name: Cryptography Specialist (PD-P-001)	Job Level: Level 4
Role Description	Senior Practitioner managing a team or mentoring others to develop, Expert managing a unit to collect and analyze digital evidence, or investigate cybersecurity incidents to derive useful information to mitigate system and network vulnerabilities. An individual in this role will be responsible for providing oversight for much of the L3 Cryptography Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include ensuring that protection and detection capabilities are aligned with the organization's cybersecurity strategy, policies and other related documentation, and developing secure data management capabilities to support a mobile workforce.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cryptography Specialist	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 92: L4 CRYPTOGRAPHY SPECIALIST

5.5 Identity and Access Management Specialist

The Identity and Access Management Specialist manages identities and access to resources by implementing identification, authentication, and authorization systems and processes. This role requires certifications or training in identity lifecycle management, access control policies, authentication protocols, and privileged access management.

FIGURE 28: IDENTITY AND ACCESS MANAGEMENT SPECIALIST CAREER MAP

5.5.1 L2 Identity and Access Management Specialist

Job Role Name: Identity and Access Management Specialist (PD-P-002)	Job Level: Level 2
Role Description	Practitioner assisting in managing individuals' and entities' identities and access to resources by applying identification, authentication, and authorization systems and processes. An individual in this role will carry out some of the basic tasks, under supervision, and will continue to develop their skills through practical application of their work. Tasks will include assisting with the implementation of identity access management solutions and supporting stakeholders to address gaps in the identity access management system.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate	The next career step for someone in this role is one of the following: • L3 Identity and Access Management Specialist

TABLE 93: L2 IDENTITY AND ACCESS MANAGEMENT SPECIALIST

5.5.2 L3 Identity and Access Management Specialist

Job Role Name: Identity and Access Management Specialist (PD-P-002)	Job Level: Level 3
Role Description	Senior Practitioner that manages individuals' and entities' identities and access to resources through applying identification, authentication and authorization systems and processes. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Identity and Access Management Specialist. Tasks will include working with other teams to design, develop and provide identity access management solutions and working with stakeholders to identify and address gaps in the identity access management implementation.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Identity and Access Management Specialist	The next career step for someone in this role is one of the following: • L4 Identity and Access Management Specialist

TABLE 94: L3 IDENTITY AND ACCESS MANAGEMENT SPECIALIST

5.5.3 L4 Identity and Access Management Specialist

Job Role Name: Identity and Access Management Specialist (PD-P-002)	Job Level: Level 4
Role Description	Expert managing a unit to manage individuals' and entities' identities and access to resources through applying identification, authentication and authorization systems and processes. An individual in this role will be responsible for providing oversight for much of the L3 Identity and Access Management Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include ensuring identity access management implementations follow organization's standards and policies and mentoring and advising team members on identity access management systems and processes
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Identity and Access Management Specialist	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 95: L4 IDENTITY AND ACCESS MANAGEMENT SPECIALIST

5.6 Systems Security Analyst

The Systems Security Analyst develops, tests, and maintains systems' security while analyzing the security of operations and integrated systems. This role requires certifications or training in systems security analysis, vulnerability management, secure systems operations, and the secure systems development lifecycle.

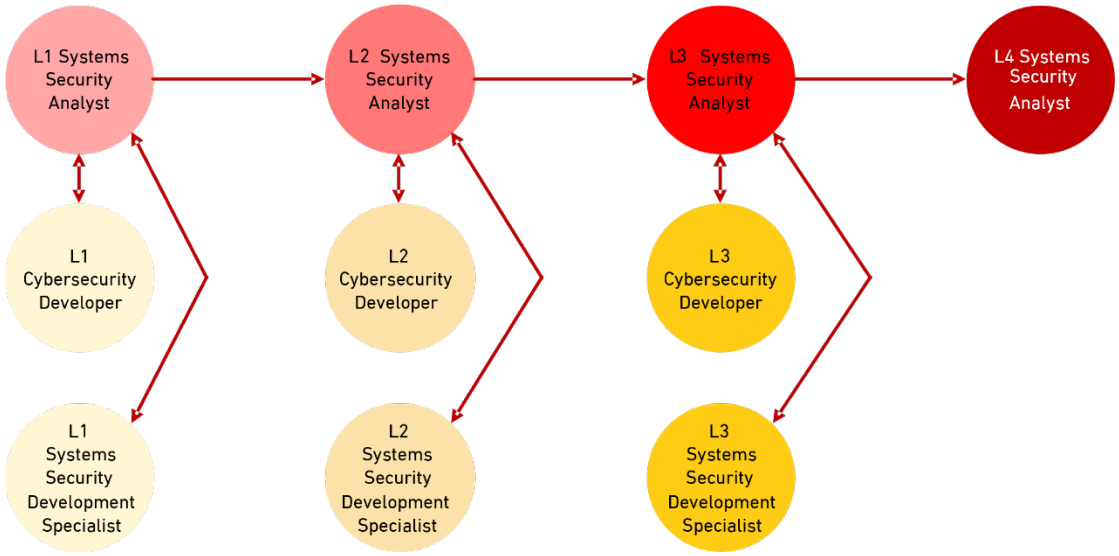

FIGURE 29: SYSTEMS SECURITY ANALYST CAREER MAP

5.6.1 L1 Systems Security Analyst

Job Role Name: Systems Security Analyst (PD-P-003)	Job Level: Level 1
Role Description	Assists the team with developing, testing and maintaining systems' security. Provides basic analysis of the security of operations and integrated systems. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include applying security patches to commercial products in accordance with the timelines dictated by the management authority for the intended operational environment and verifying minimum security requirements are in place for all applications
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate • L1 Cybersecurity Developer • L1 Systems Security Development Specialist	The next career step for someone in this role is one of the following: • L2 Systems Security Analyst • L1 Cybersecurity Developer • L1 Systems Security Development Specialist

TABLE 96: L1 SYSTEMS SECURITY ANALYST

5.6.2 L2 Systems Security Analyst

Job Role Name: Systems Security Analyst (PD-P-003)	Job Level: Level 2
Role Description	Practitioner that develops, tests and maintains systems' security. Analyzes security of operations and integrated systems. An individual in this role will oversee the work done by the L1 Systems Security Analyst, and will continue to develop their skills through practical application of their work. Tasks will include developing 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 and applying security policies to applications that interface with one another.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Systems Security Analyst • L2 Cybersecurity Developer • L2 Systems Security Development Specialist	The next career step for someone in this role is one of the following: • L3 Systems Security Analyst • L2 Cybersecurity Developer • L2 Systems Security Development Specialist

TABLE 97: L2 SYSTEMS SECURITY ANALYST

5.6.3 L3 Systems Security Analyst

Job Role Name: Systems Security Analyst (PD-P-003)	Job Level: Level 3
Role Description	Senior Practitioner that develops, tests and maintains systems' security. Analyzes security of operations and integrated systems. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Systems Security Analyst. Tasks will include working with stakeholders to resolve cybersecurity incidents and vulnerability compliance issues and applying service-oriented security architecture principles to meet the organization's confidentiality, integrity, and availability requirements.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Systems Security Analyst • L3 Cybersecurity Developer • L3 Systems Security Development Specialist	The next career step for someone in this role is one of the following: • L4 Systems Security Analyst • L3 Cybersecurity Developer • L3 Systems Security Development Specialist

TABLE 98: L3 SYSTEMS SECURITY ANALYST

5.6.4 L4 Systems Security Analyst

Job Role Name: Systems Security Analyst (PD-P-003)	Job Level: Level 4
Role Description	Expert managing unit to develop, test and maintain systems' security. Analyzes security of operations and integrated systems. An individual in this role will be responsible for providing oversight for much of the L3 Systems Security Analyst's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include making cybersecurity recommendations to leadership based on significant threats and vulnerabilities and ensuring the integration and implementation of cross-domain solutions in a secure environment.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Systems Security Analyst	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 99: L4 SYSTEMS SECURITY ANALYST

5.7 Vulnerability Assessment Specialist

The Vulnerability Assessment Specialist performs assessments of systems and networks to identify deviations from acceptable configurations or policies and evaluates the effectiveness of defense-in-depth architectures against known vulnerabilities. This role requires certifications or training in vulnerability assessment, penetration testing methodologies, risk analysis, and the use of tools for scanning and testing systems for security weaknesses.

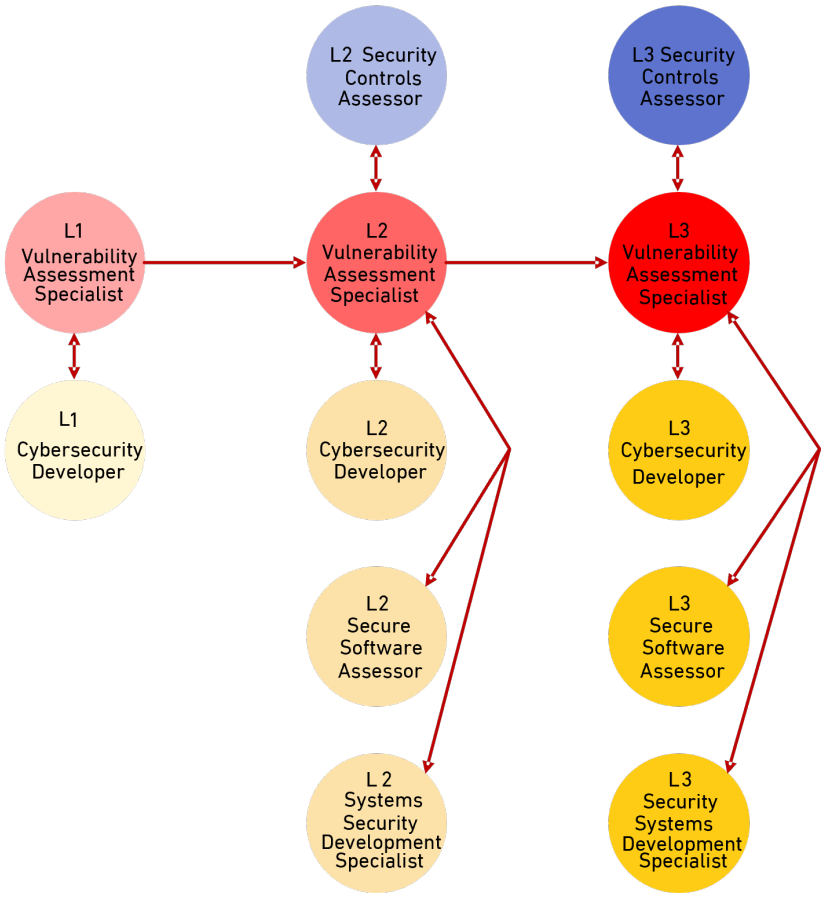

FIGURE 30: VULNERABILITY ASSESSMENT SPECIALIST CAREER MAP

5.7.1 L1 Vulnerability Assessment Specialist

Job Role Name: Vulnerability Assessment Specialist (PD-VA- 001)	Job Level: Level 1
Role Description	Assists with performing 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. An individual in this role will carry out some of the basic tasks, under supervision, while continuing to learn about the requirements of the role. Tasks will include using security testing and code scanning tools to conduct code reviews and performing technical and nontechnical risk and vulnerability assessments of organizational technology environments.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR1 Entry Level Graduate • Core Cybersecurity Role • L1 Cybersecurity Developer	The next career step for someone in this role is one of the following: • L2 Vulnerability Assessment Specialist • L1 Cybersecurity Developer

TABLE 100: L1 VULNERABILITY ASSESSMENT SPECIALIST

5.7.2 L2 Vulnerability Assessment Specialist

Job Role Name: Vulnerability Assessment Specialist (PD-VA- 001)	Job Level: Level 2
Role Description	Practitioner that 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. An individual in this role will oversee the work done by the Vulnerability Assessment Specialist, and will continue to develop their skills through practical application of their work. Tasks will include analyzing organization's cybersecurity defense policies and configurations to evaluate compliance with regulations and organizational directives and maintaining a deployable cyber defense audit toolkit based on industry best practice to support cyber defense audits.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L1 Vulnerability Assessment Specialist • L2 Cybersecurity Developer • L2 Systems Security Development Specialist • L2 Secure Software Assessor • L2 Security Controls Assessor	The next career step for someone in this role is one of the following: • L3 Vulnerability Assessment Specialist • L2 Cybersecurity Developer • L2 Systems Security Development Specialist • L2 Secure Software Assessor • L2 Security Controls Assessor

TABLE 101: L2 VULNERABILITY ASSESSMENT SPECIALIST

5.7.3 L3 Vulnerability Assessment Specialist

Job Role Name: Vulnerability Assessment Specialist (PD-VA- 001)	Job Level: Level 3
Role Description	Senior Practitioner that 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. An individual in this role will be responsible for providing oversight for much of the L2 Vulnerability Assessment Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include maintaining knowledge of applicable cybersecurity defense policies, regulations, and compliance documents as they pertain to cybersecurity defense auditing and recommending cost-effective security controls to mitigate risks identified through testing and review. The L3 Vulnerability Assessment Specialist will typically be managed by the L4 Penetration Tester / Red Team Specialist, who will, as well as providing normal staff management, ensure that: • vulnerabilities are appropriately identified, classified and scored • closure plans are implemented effectively
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Vulnerability Assessment Specialist • L3 Cybersecurity Developer • L3 Systems Security Development Specialist • L3 Secure Software Assessor • L3 Security Controls Assessor	The next career step for someone in this role is one of the following: • L3 Cybersecurity Developer • L3 Systems Security Development Specialist • L3 Secure Software Assessor • L3 Security Controls Assessor

TABLE 102: L3 VULNERABILITY ASSESSMENT SPECIALIST

5.8 Penetration Tester/Red Team Specialist

The Penetration Tester/Red Team Specialist conducts authorized penetration tests on computer systems, networks, and physical premises, using realistic threat techniques to evaluate security and identify vulnerabilities. This role requires certifications or training in penetration testing methodologies, ethical hacking techniques, vulnerability exploitation, and red team operations to assess security gaps.

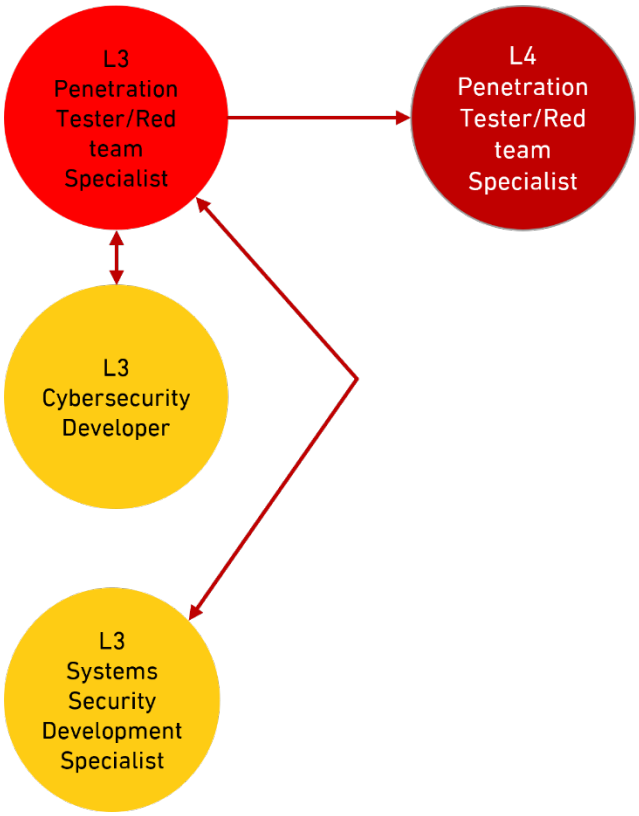

FIGURE 31: PENETRATION TESTER / RED TEAM SPECIALIST CAREER MAP

5.8.1 L3 Penetration Tester/Red Team Specialist

Job Role Name: Penetration Tester/Red Team Specialist (PD-VA-002)	Job Level: Level 3
Role Description	Senior Practitioner that conducts authorized attempts to penetrate computer systems or networks and physical premises, using realistic threat techniques, to evaluate their security and detect potential vulnerabilities. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Penetration Tester / Red Team Specialist. Tasks will include gathering information about network topography and usage through technical analysis and open source research and document findings and mimicking malicious social engineering techniques that an attacker would use to attempt a system breach to uncover security gaps and vulnerabilities
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Developer • L3 Systems Security Development Specialist	The next career step for someone in this role is one of the following: • L4 Penetration Tester / Red Team Specialist • L3 Cybersecurity Developer • L3 Systems Security Development Specialist

TABLE 103: L3 PENETRATION TESTER / RED TEAM SPECIALIST

5.8.2 L4 Penetration Tester/Red Team Specialist

Job Role Name: Penetration Tester/Red Team Specialist (PD-VA-002)		Job Level: Level 4
Role Description	Expert managing a unit to conduct authorized attempts to penetrate computer systems or networks and physical premises, using realistic threat techniques, to evaluate their security and detect potential vulnerabilities. An individual in this role will be responsible for providing oversight for much of the L3 Penetration Tester / Red Team Specialist's work, as well as that of the L3 Vulnerability Assessment Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. This role provides vulnerability management oversight, ensuring that the Penetration Tester/Red Team Specialist and Vulnerability Assessment Specialist roles address vulnerabilities in the most appropriate manner and timeframes. Tasks will include reporting penetration testing and vulnerability assessment findings including risk level, proposed mitigation and details necessary to reproduce the test results and including business considerations in security strategies and recommendations.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L3 Penetration Tester/Red Team Specialist		The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 104: L4 PENETRATION TESTER / RED TEAM SPECIALIST

5.9 Cybersecurity Incident Responder

The Cybersecurity Incident Responder investigates, analyzes, and responds to cybersecurity incidents. This role requires certifications or training in incident handling and response, digital forensics, malware analysis, network security monitoring, and Security Operations Center (SOC) processes to effectively detect, analyze, and mitigate cybersecurity incidents.

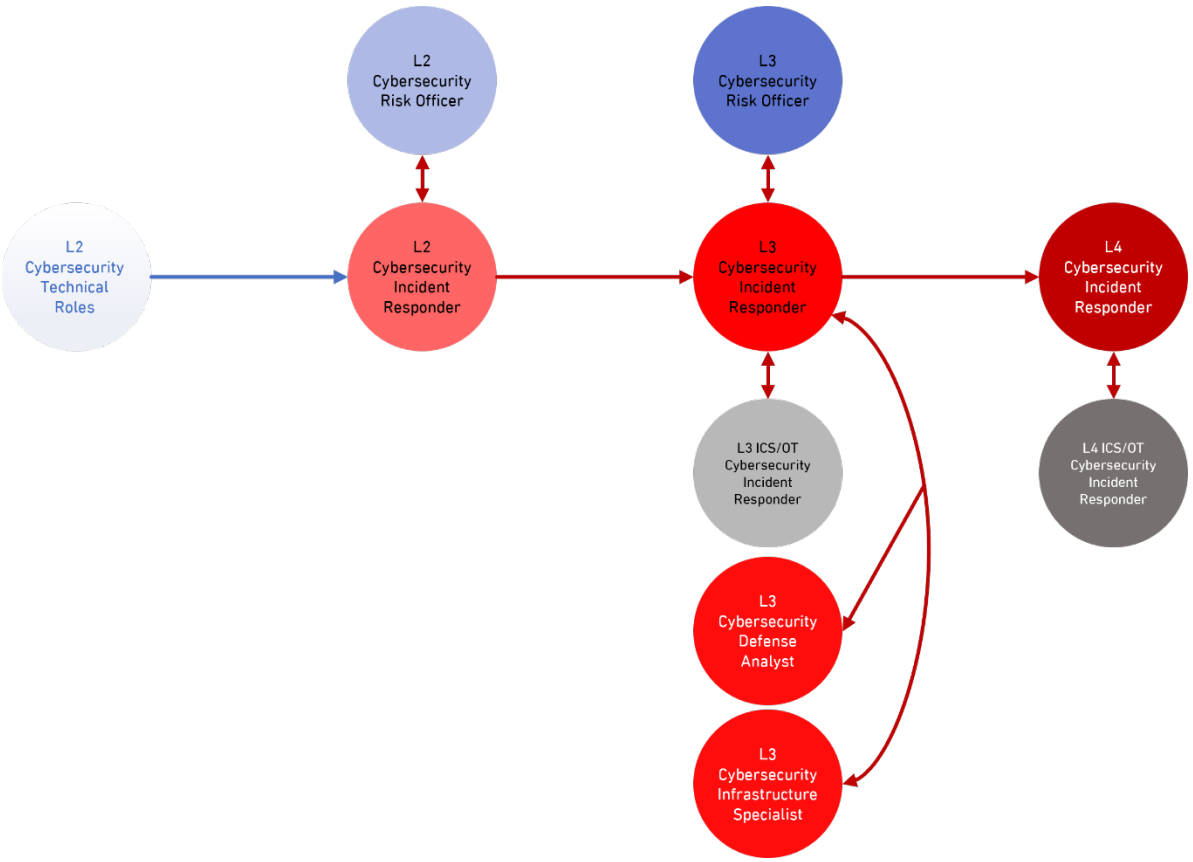

FIGURE 32: CYBERSECURITY INCIDENT RESPONDER CAREER MAP

5.9.1 L2 Cybersecurity Incident Responder

Job Role Name: Cybersecurity Incident Responder (PD-IR- 001)	Job Level: Level 2
Role Description	Practitioner investigating, analyzing and responding to cybersecurity incidents. An individual in this role will carry out some of the basic tasks of the role, under supervision, and will continue to develop their skills through practical application of their work. Tasks will include collection of incident data, triaging security alerts to identify incident breaches correlating incident data to identify vulnerabilities and handling and performing procedures as set out in the incident response plan.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Technical Roles • L2 Cybersecurity Risk Officer	The next career step for someone in this role is one of the following: • L3 Cybersecurity Incident Responder • L2 Cybersecurity Risk Officer

TABLE 105: L2 CYBERSECURITY INCIDENT RESPONDER

5.9.2 L3 Cybersecurity Incident Responder

Job Role Name: Cybersecurity Incident Responder (PD-IR- 001)	Job Level: Level 3
Role Description	Senior Practitioner investigating, analyzing and responding to cybersecurity incidents. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cybersecurity Incident Responder. include correlating evidence artifacts. Tasks will include assessing incident severity, declaring incidents and identifying possible impact, determining incident scope and urgent containment and eradication actions that needs to be performed during the incident, and may also involve performing deep analysis on collected host and network artifacts.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cybersecurity Incident Responder • L3 Cybersecurity Risk Officer • L3 ICS/OT Cybersecurity Incident Responder • L3 Cybersecurity Defense analyst • L3 Cybersecurity Infrastructure Specialist	The next career step for someone in this role is one of the following: • L4 Cybersecurity Incident Responder • L3 ICS/OT Cybersecurity Incident Responder • L3 Cybersecurity Risk Officer • L3 Cybersecurity Defense analyst • L3 Cybersecurity Infrastructure Specialist

TABLE 106: L3 CYBERSECURITY INCIDENT RESPONDER

5.9.3 L4 Cybersecurity Incident Responder

Job Role Name: Cybersecurity Incident Responder (PD-IR- 001)	Job Level: Level 4
Role Description	Expert managing a unit to investigate, analyze and respond to cybersecurity incidents. An individual in this role will be responsible for providing oversight for much of the L3 Cybersecurity Incident Responder's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include formulating and assigning the incident response team, leading and coordinating all incident response activities, providing guidance and consultancy during incidents, providing remediation plans, managing the implementation of remediation plans and identifying the remediation triggers and timing.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Incident Responder • L4 ICS/OT Cybersecurity Incident Responder	The next career step for someone in this role is one of the following: • L4 ICS/OT Cybersecurity Incident Responder

TABLE 107: L4 CYBERSECURITY INCIDENT RESPONDER

5.10 Digital Forensics Specialist

The Digital Forensics Specialist collects and analyzes digital evidence to investigate cybersecurity incidents and derive actionable information for mitigating system and network vulnerabilities. This role requires certifications or training in digital evidence handling, forensic analysis, malware analysis, and network traffic analysis.

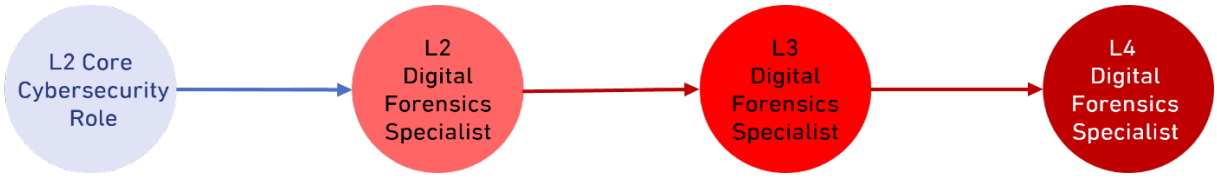

FIGURE 33: DIGITAL FORENSICS SPECIALIST CAREER MAP

5.10.1 L2 Digital Forensics Specialist

Job Role Name: Digital Forensics Specialist (PD-IR-002)	Job Level: Level 2
Role Description	Practitioner collecting and analyzing digital evidence, and investigating cybersecurity incidents to derive useful information to mitigate system and network vulnerabilities. An individual in this role will oversee the work done by the L1 Digital Forensics Specialist, and will continue to develop their skills through practical application of their work. Tasks will include ensuring that processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody are followed and conducting initial forensic analysis in multiple operating system environments.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Core Cybersecurity Role	The next career step for someone in this role is one of the following: • L3 Digital Forensics Specialist

TABLE 108: L2 DIGITAL FORENSICS SPECIALIST

5.10.2 L3 Digital Forensics Specialist

Job Role Name: Digital Forensics Specialist (PD-IR-002)	Job Level: Level 3
Role Description	Senior Practitioner managing a team or mentoring others to collect and analyze digital evidence and investigate cybersecurity incidents to derive useful information to mitigate system and network vulnerabilities. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Digital Forensics Specialist. Tasks will include performing incident response tasks to support deployable incident response teams including forensic collection, intrusion correlation, tracking, threat analysis, and system remediation and providing a technical summary of findings in accordance with established reporting procedures.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Digital Forensics Specialist Role	The next career step for someone in this role is one of the following: • L4 Digital Forensics Specialist

TABLE 109: L3 DIGITAL FORENSICS SPECIALIST

5.10.3 L4 Digital Forensics Specialist

Job Role Name: Digital Forensics Specialist (PD-IR-002)	Job Level: Level 4
Role Description	Expert managing a unit to collect and analyze digital evidence, or investigate cybersecurity incidents to derive useful information to mitigate system and network vulnerabilities. An individual in this role will be responsible for providing oversight for much of the L3 Digital Forensics Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include ensuring that chain of custody is followed for all acquired digital media in accordance with national law or organizational policies as applicable and working as a technical expert in support of law enforcement, explaining incident details and forensic analysis as required
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Digital Forensics Specialist Role	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 110: L4 DIGITAL FORENSICS SPECIALIST

5.11 Cyber Crime Investigator

The Cyber Crime Investigator identifies, collects, examines, and preserves digital evidence using controlled and documented analytical and investigative techniques. This role requires certifications or training in digital forensics, cybercrime investigation methodologies, evidence handling, and the legal aspects of cybercrime.

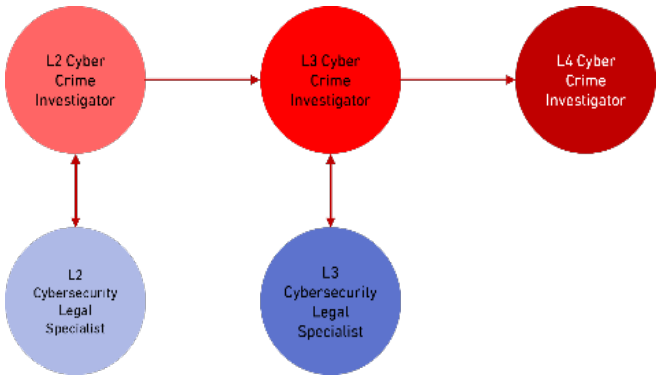

FIGURE 34: CYBER CRIME INVESTIGATOR CAREER MAP

5.11.1 L2 Cyber Crime Investigator

Job Role Name: Cyber Crime Investigator (PD-IR-003)	Job Level: Level 2
Role Description	Practitioner who specializes in identifying, collecting, examining and preserving evidence using controlled and documented analytical and investigative techniques. An individual in this role will carry out some of the basic tasks for the role and will continue to develop their skills through practical application of their work. Tasks will include interviewing victims of a possible cybercrime and witnesses and gathering and preserving evidence that could be used to prosecute perpetrators of the cybercrime.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Legal Specialist	The next career step for someone in this role is one of the following: • L3 Cyber Crime Investigator • L2 Cybersecurity Legal Specialist

TABLE 111: L2 CYBER CRIME INVESTIGATOR

5.11.2 L3 Cyber Crime Investigator

Job Role Name: Cyber Crime Investigator (PD-IR-003)	Job Level: Level 3
Role Description	Senior Practitioner managing a team or mentoring others to identify, collect, examine and preserve evidence using controlled and documented analytical and investigative techniques. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Cyber Crime Investigator. Tasks will include determining whether a cybersecurity incident may be a violation of law requiring specific legal action and determining the extent of threats and risks arising from them and recommend courses of action or countermeasures to mitigate them
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Cyber Crime Investigator • L3 Cybersecurity Legal Specialist	The next career step for someone in this role is one of the following: • L4 Cyber Crime Investigator • L3 Cybersecurity Legal Specialist

TABLE 112: L3 CYBER CRIME INVESTIGATOR

5.11.3 L4 Cyber Crime Investigator

Job Role Name: Cyber Crime Investigator (PD-IR-003)	Job Level: Level 4
Role Description	Expert managing a unit to identify, collect, examine and preserve evidence using controlled and documented analytical and investigative techniques. An individual in this role will be responsible for providing oversight for much of the L3 Cyber Crime Investigator's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include providing criminal investigative support to legal authorities during the judicial process and documenting the investigation in line with legal standards and requirements.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cyber Crime Investigator	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 113: L4 CYBER CRIME INVESTIGATOR

5.12 Malware Reverse Engineering Specialist

The Malware Reverse Engineering Specialist analyzes malicious software by disassembling and decompiling it to understand its functionality, impact, and intent. The specialist also recommends mitigation techniques and incident response actions. This role requires certifications or training in malware analysis, reverse engineering, and threat intelligence.

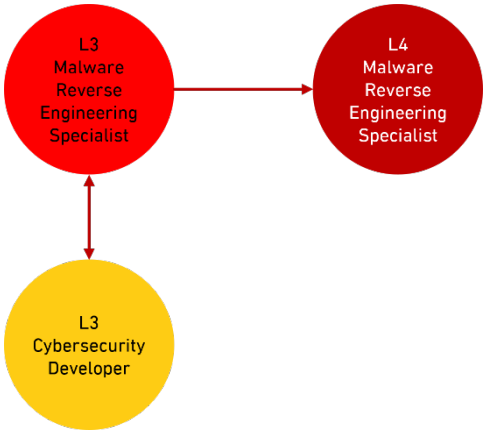

FIGURE 35: MALWARE REVERSE ENGINEERING SPECIALIST CAREER MAP

5.12.1 L3 Malware Reverse Engineering Specialist

Job Role Name: Malware Reverse Engineering Specialist (PD- IR-004)	Job Level: Level 3
Role Description	Senior Practitioner that analyzes (by disassembling and/or decompiling) malicious software, understands how it works, its impact and intent and recommends mitigation techniques and incident response actions. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Malware Reverse Engineering Specialist. Tasks will include identifying and developing reverse engineering tools to enhance capabilities and detect vulnerabilities and reviewing and analyzing cybersecurity threats to provide stakeholders with information needed to respond to threats
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Developer	The next career step for someone in this role is one of the following: • L4 Malware Reverse Engineering Specialist • L3 Cybersecurity Developer

TABLE 114: L3 MALWARE REVERSE ENGINEERING SPECIALIST

5.12.2 L4 Malware Reverse Engineering Specialist

Job Role Name: Malware Reverse Engineering Specialist (PD- IR-004)	Job Level: Level 4
Role Description	Expert managing a unit to analyze (by disassembling and/or decompiling) malicious software, understand how it works, its impact and intent and recommend mitigation techniques and incident response actions. An individual in this role will be responsible for providing oversight for much of the L3 Malware Reverse Engineering Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include providing current intelligence support to critical internal / external stakeholders as appropriate and providing timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Malware Reverse Engineering Specialist	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 115: L4 MALWARE REVERSE ENGINEERING SPECIALIST

5.13 Threat Intelligence Analyst

The Threat Intelligence Analyst collects and analyzes multi-source information to develop a deep understanding of cybersecurity threats and the tactics, techniques, and procedures (TTPs) of threat actors. This role involves deriving and reporting indicators of compromise (IOCs) to help organizations detect and predict cyber incidents and safeguard systems and networks. Certifications or training in cyber threat intelligence, TTP analysis, and IOC development are essential for this role.

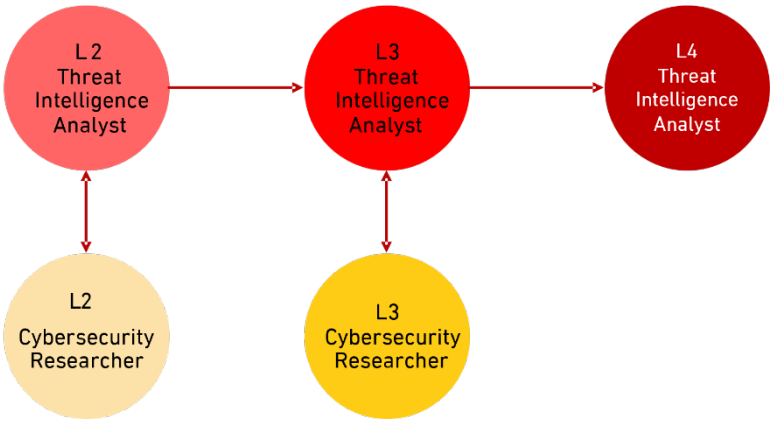

FIGURE 36: THREAT INTELLIGENCE ANALYST CAREER MAP

5.13.1 L2 Threat Intelligence Analyst

Job Role Name: Threat Intelligence Analyst (PD-TM-001)	Job Level: Level 2
Role Description	Practitioner collecting and analyzing multi-source information about cybersecurity threats to develop deep understanding and awareness of cyber threats and actors' Tactics, Techniques and Procedures (TTPs), deriving and reporting indicators that help organizations detect and predict cyber incidents and protect systems and networks from cyber threats. An individual in this role will carry out some of the basic tasks for the role and will continue to develop their skills through practical application of their work. Tasks will include monitoring open source websites for hostile content directed towards organizational or partner interests and monitoring and reporting on threat actor activities to fulfil the organization's threat intelligence and reporting requirements
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Researcher	The next career step for someone in this role is one of the following: • L3 Threat Intelligence Analyst • L2 Cybersecurity Researcher

TABLE 116: L2 THREAT INTELLIGENCE ANALYST

5.13.2 L3 Threat Intelligence Analyst

Job Role Name: Threat Intelligence Analyst (PD-TM-001)	Job Level: Level 3
Role Description	Senior Practitioner managing a team or mentoring others to collect and analyze 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. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Threat Intelligence Analyst. Tasks will include coordinating, validating, and managing the organization's cyber threat intelligence sources and feeds and identifying information gaps in threat intelligence and assess their implications for the organization
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 Threat Intelligence Analyst • L3 Cybersecurity Researcher	The next career step for someone in this role is one of the following: • L4 Threat Intelligence Analyst • L3 Cybersecurity Researcher

TABLE 117: L3 THREAT INTELLIGENCE ANALYST

5.13.3 L4 Threat Intelligence Analyst

Job Role Name: Threat Intelligence Analyst (PD-TM-001)	Job Level: Level 4
Role Description	Expert managing unit to collect and analyze multi-source information about cybersecurity threats to develop deep understanding and awareness of cyber threats and actors' Tactics, Techniques and Procedures (TTPs), derive and report indicators that help organizations detect and predict cyber incidents and protect systems and networks from cyber threats. An individual in this role will be responsible for providing oversight for much of the L3 Threat Intelligence Analyst's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include providing current intelligence support to critical internal/external stakeholders as appropriate and preparing and delivering briefs on specific threats to the organization.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Threat Intelligence Analyst	The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 118: L4 THREAT INTELLIGENCE ANALYST

5.14 Threat Hunter

The Threat Hunter proactively searches for undetected threats within networks and systems, identifies Indicators of Compromise (IOCs), and recommends effective mitigation strategies. This role requires certifications or training in cyber threat hunting, advanced incident response, and digital forensics.

5.14.1 L3 Threat Hunter

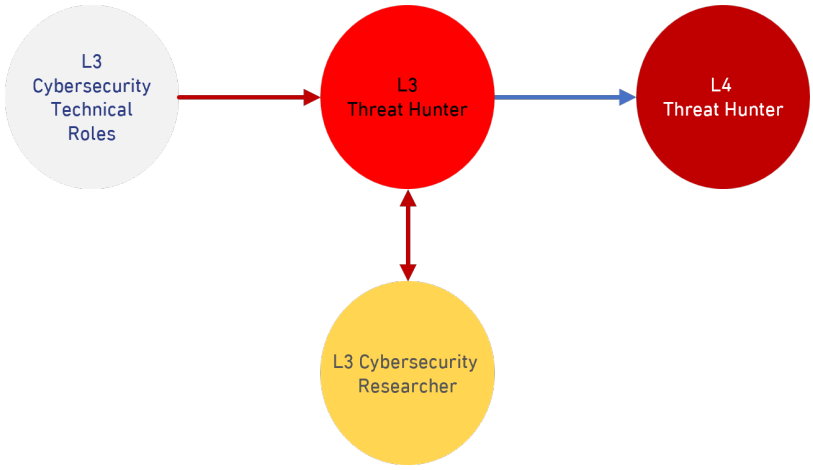

FIGURE 37: THREAT HUNTER CAREER MAP

Job Role Name: Threat Hunter (PD-TM-002)	Job Level: Level 3
Role Description	Senior Practitioner that proactively searches for undetected threats in networks and systems, identifies their Indicators of Compromise (IOCs) and recommends mitigation plans. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 Threat Hunter. Tasks will include analyzing log files from multiple sources to identify possible threats to network security and analyzing malicious activity to determine what was exploited, exploitation methods, and effects on system and information.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Researcher • L3 Cybersecurity Technical Roles	The next career step for someone in this role is one of the following: • L4 Threat Hunter • L3 Cybersecurity Researcher

TABLE 119: L3 THREAT HUNTER

5.14.2 L4 Threat Hunter

Job Role Name: Threat Hunter (PD-TM-002)		Job Level: Level 4
Role Description	Expert managing a unit to proactively search for undetected threats in networks and systems, identify their Indicators of Compromise (IOCs) and recommend mitigation plans. An individual in this role will be responsible for providing oversight for much of the L3 Threat Hunter's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include advocating cybersecurity related topics with senior management, to ensure the organization's strategic goals include cybersecurity and establishing and maintaining appropriate communication channels with stakeholders.	
Career Progression (Pathway)		
The individual will have come from the following roles: • L3 Threat Hunter		The next career step for someone in this role is one of the L4 leadership specialty area roles.

TABLE 120: L4 THREAT HUNTER

6. Industrial Control Systems and Operational Technology (ICS/OT)

6.1 ICS/OT Cybersecurity Architect

The ICS/OT Cybersecurity Architect designs and oversees the development, implementation, and configuration of cybersecurity systems and networks in industrial control systems (ICS) and operational technology (OT) environments. This role requires certifications or training in ICS/OT cybersecurity, secure architecture design, risk management, secure configuration, cybersecurity risk assessment, disaster recovery, and the integration of security into system design for ICS/OT environments.

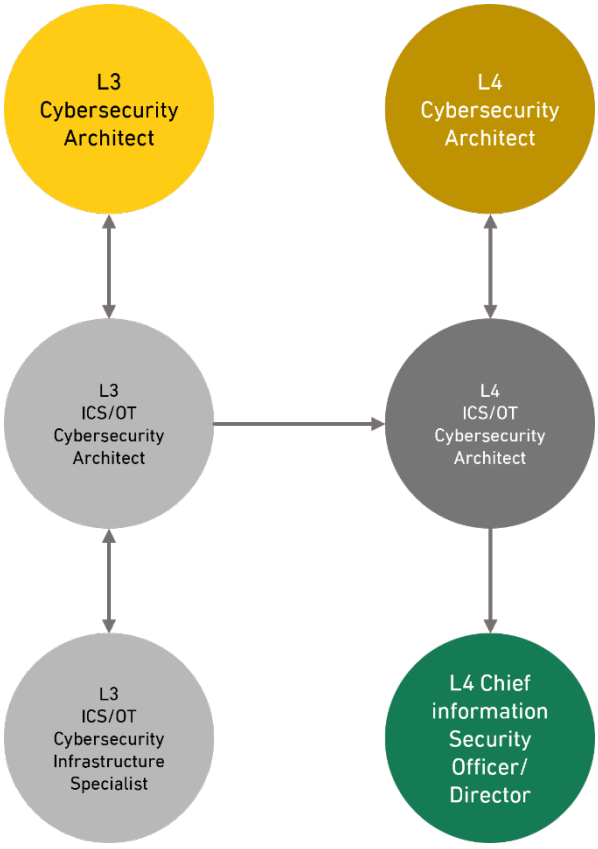

FIGURE 38: ICS/OT CYBERSECURITY ARCHITECT CAREER MAP

6.1.1 L3 ICS/OT Cybersecurity Architect

Job Role Name: ICS/OT Cybersecurity Architect (ICSOT- ICSOT-001)	Job Level: Level 3
Role Description	Senior Practitioner designs and oversees the development, implementation and configuration of cybersecurity systems and networks in ICS/OT environments. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 ICS/OT Cybersecurity Architect. Tasks will include translating proposed ICS/OT capabilities into technical requirements and working with agile team members to conduct fast prototyping, feasibility studies, and evaluation of new technologies.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Architect • L3 ICS/OT Cybersecurity Infrastructure Specialist	The next career step for someone in this role is one of the following: • L4 ICS/OT Cybersecurity Architect • L3 Cybersecurity Architect • L3 ICS/OT Cybersecurity Infrastructure Specialist

TABLE 121: L3 ICS/OT CYBERSECURITY ARCHITECT

6.1.2 L4 ICS/OT Cybersecurity Architect

Job Role Name: ICS/OT Cybersecurity Architect (ICSOT- ICSOT-001)	Job Level: Level 4
Role Description	Expert managing a unit to designs and oversees the development, implementation and configuration of cybersecurity systems and networks in ICS/OT environments. An individual in this role will be responsible for providing oversight for much of the L3 ICS/OT Cybersecurity Architect's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include defining and prioritizing essential ICS/OT system capabilities or business functions required for partial or full system restoration after a catastrophic failure event and ensuring that acquired or developed ICS/OT systems and architectures are consistent with organization's cybersecurity architecture guidelines.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 ICS/OT Cybersecurity Architect • L4 Cybersecurity Architect	The next career step for someone in this role is one of the following: • L4 Chief Information Security Officer/Director • L4 Cybersecurity Architect

TABLE 122: L4 ICS/OT CYBERSECURITY ARCHITECT

6.2 ICS/OT Cybersecurity Infrastructure Specialist

The ICS/OT Cybersecurity Infrastructure Specialist tests, implements, deploys, maintains, and administers hardware and software to protect and defend systems and networks against cybersecurity threats in industrial control systems (ICS) and operational technology (OT) environments. This role requires certifications or training in ICS/OT cybersecurity, system and network administration, ICS/OT cybersecurity infrastructure management, security controls implementation, and hardware/software deployment.

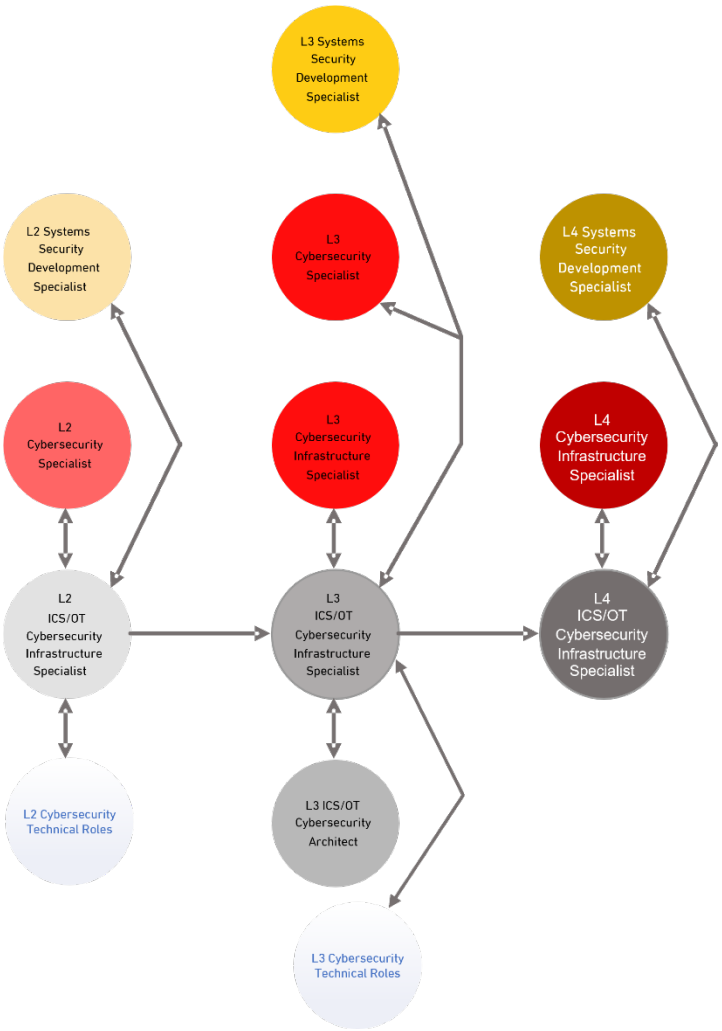

FIGURE 39: ICS/OT CYBERSECURITY INFRASTRUCTURE SPECIALIST CAREER MAP

6.2.1 L2 ICS/OT Cybersecurity Infrastructure Specialist

Job Role Name: ICS/OT Cybersecurity Infrastructure Specialist (ICSOT-ICSOT-002)	Job Level: Level 2
Role Description	Practitioner testing, implementing, deploying, maintaining and administering hardware and software that defend and protect and defend systems and networks against cybersecurity threats in ICS/OT environments. An individual in this role will carry out some of the basic tasks of the role and will continue to develop their skills through practical application of their work. Tasks will include performing incident response tasks to support deployable incident response teams including forensic collection, intrusion correlation, tracking, threat analysis, and system remediation and assessing the effectiveness of cybersecurity controls.
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Technical Roles • L2 Cybersecurity Specialist • L2 Systems Security Development Specialist	The next career step for someone in this role is one of the following: • L3 ICS/OT Cybersecurity Infrastructure Specialist • Cybersecurity Technical Roles • L2 Cybersecurity Specialist • L2 Systems Security Development Specialist

TABLE 123: L2 ICS/OT CYBERSECURITY INFRASTRUCTURE SPECIALIST

6.2.2 L3 ICS/OT Cybersecurity Infrastructure Specialist

Job Role Name: ICS/OT Cybersecurity Infrastructure Specialist (ICSOT-ICSOT-002)	Job Level: Level 3
Role Description	Senior Practitioner managing a team or mentoring others testing, implementing, deploying, maintaining and administering hardware and software that defend and protect and defend systems and networks against cybersecurity threats in ICS/OT environments. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 ICS/OT Cybersecurity Infrastructure Specialist. Tasks will include selecting the security controls for ICS/OT systems and document the functional description of the implementation in a security plan and implementing the ICS/OT security controls specified in a security plan or other system documentation.
Career Progression (Pathway)	
The individual will have come from the following roles:	The next career step for someone in this role is one of the following:
• L2 ICS/OT Cybersecurity Infrastructure Specialist • Cybersecurity Technical Roles • L3 Cybersecurity Infrastructure Specialist • L3 Cybersecurity Specialist • L3 ICS/OT Cybersecurity Architect • L3 Systems Security Development Specialist	• L4 ICS/OT Cybersecurity Infrastructure Specialist • Cybersecurity Technical Roles • L3 Cybersecurity Infrastructure Specialist • L3 Cybersecurity Specialist • L3 ICS/OT Cybersecurity Architect • L3 Systems Security Development Specialist

TABLE 124: L3 ICS/OT CYBERSECURITY INFRASTRUCTURE SPECIALIST

6.2.3 L4 ICS/OT Cybersecurity Infrastructure Specialist

Job Role Name: ICS/OT Cybersecurity Infrastructure Specialist (ICSOT-ICSOT-002)	Job Level: Level 4
Role Description	Expert managing a unit testing, implementing, deploying, maintaining and administering hardware and software that defend and protect and defend systems and networks against cybersecurity threats in ICS/OT environments. An individual in this role will be responsible for providing oversight for much of the L3 ICS/OT Cybersecurity Infrastructure Specialist's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include collaborating with stakeholders to ensure business continuity and disaster recovery programs meet organizational requirements and promoting and demonstrating the value of cybersecurity to stakeholders within an organization.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 ICS/OT Cybersecurity Infrastructure Specialist • L4 Cybersecurity Infrastructure Specialist • L4 Systems Security Development Specialist	The next career step for someone in this role is one of the following: • L4 Cybersecurity Infrastructure Specialist • L4 Systems Security Development Specialist

TABLE 125: L4 ICS/OT CYBERSECURITY INFRASTRUCTURE SPECIALIST

6.3 ICS/OT Cybersecurity Defense Analyst

The ICS/OT Cybersecurity Defense Analyst uses data collected from various cybersecurity tools to analyze events within industrial control systems (ICS) and operational technology (OT) environments, aiming to detect and mitigate cybersecurity threats. This role requires certifications or training in ICS/OT cybersecurity, network defense, threat detection, incident analysis, and cybersecurity monitoring tools tailored for ICS/OT environments.

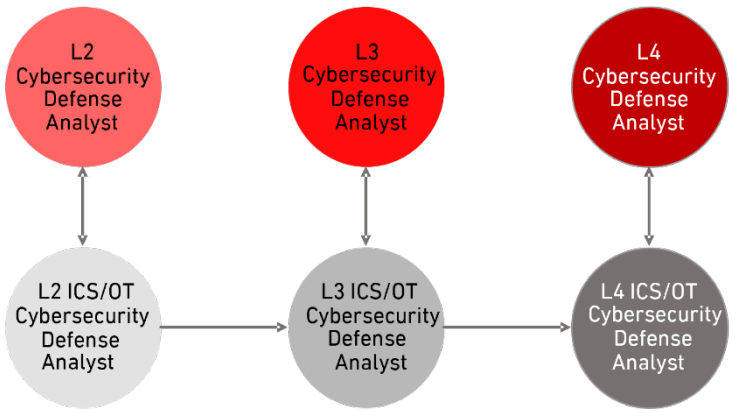

FIGURE 40: ICS/OT CYBERSECURITY DEFENSE ANALYST CAREER MAP

6.3.1 L2 ICS/OT Cybersecurity Defense Analyst

Job Role Name: ICS/OT Cybersecurity Defense Analyst (ICSOT-ICSOT-003)	Job Level: Level 2
Role Description	Practitioner using data collected from a variety of cybersecurity tools to analyze events that occur within ICS/OT environments to detect and mitigate cybersecurity threats. An individual in this role will carry out some of the basic tasks of the role and will continue to develop their skills through practical application of their work. Tasks will include correlating information from multiple sources to understand situation and determine the effectiveness of an observed attack and providing timely detection, identification, and alerting of possible attacks, anomalous activities, and misuse activities and distinguishing them from benign activities
Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Defense Analyst	The next career step for someone in this role is one of the following: • L3 ICS/OT Cybersecurity Defense Analyst • L2 Cybersecurity Defense Analyst

TABLE 126: L2 ICS/OT CYBERSECURITY DEFENSE ANALYST

6.3.2 L3 ICS/OT Cybersecurity Defense Analyst

Job Role Name: ICS/OT Cybersecurity Defense Analyst (ICSOT-ICSOT-003)	Job Level: Level 3
Role Description	Senior Practitioner using data collected from a variety of cybersecurity tools to analyze events that occur within ICS/OT environments to detect and mitigate cybersecurity threats. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 ICS/OT Cybersecurity Defense Analyst. Tasks will include performing cybersecurity reviews and identify security gaps in security architecture to inform risk mitigation strategies and identifying indications and warnings through research, analysis, and correlation across multiple data sets.
Career Progression (Pathway)	
The individual will have come from the following roles: • L2 ICS/OT Cybersecurity Defense Analyst • L3 Cybersecurity Defense Analyst	The next career step for someone in this role is one of the following: • L4 ICS/OT Cybersecurity Defense Analyst • L3 Cybersecurity Defense Analyst

TABLE 127: L3 ICS/OT CYBERSECURITY DEFENSE ANALYST

6.3.3 L4 ICS/OT Cybersecurity Defense Analyst

Job Role Name: ICS/OT Cybersecurity Defense Analyst (ICSOT-ICSOT-003)	Job Level: Level 4
Role Description	Expert managing a unit to use data collected from a variety of cybersecurity tools to analyze events that occur within ICS/OT environments to detect and mitigate cybersecurity threats. An individual in this role will be responsible for providing oversight for much of the L3 ICS/OT Cybersecurity Defense Analyst's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include making cybersecurity recommendations to leadership based on significant threats and vulnerabilities and working with stakeholders to resolve cybersecurity incidents and vulnerability compliance issues.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 ICS/OT Cybersecurity Defense Analyst • L4 Cybersecurity Defense Analyst	The next career step for someone in this role is one of the following: • L4 Cybersecurity Defense Analyst

TABLE 128: L4 ICS/OT CYBERSECURITY DEFENSE ANALYST

6.4 ICS/OT Cybersecurity Risk Officer

The ICS/OT Cybersecurity Risk Officer identifies, assesses, and manages cybersecurity risks within industrial control systems (ICS) and operational technology (OT) environments. The role involves evaluating the effectiveness of existing cybersecurity controls and providing actionable feedback and recommendations. Certifications or training in ICS/OT cybersecurity, risk management, cybersecurity governance, compliance, and threat assessment specific to ICS/OT environments are essential for this position.

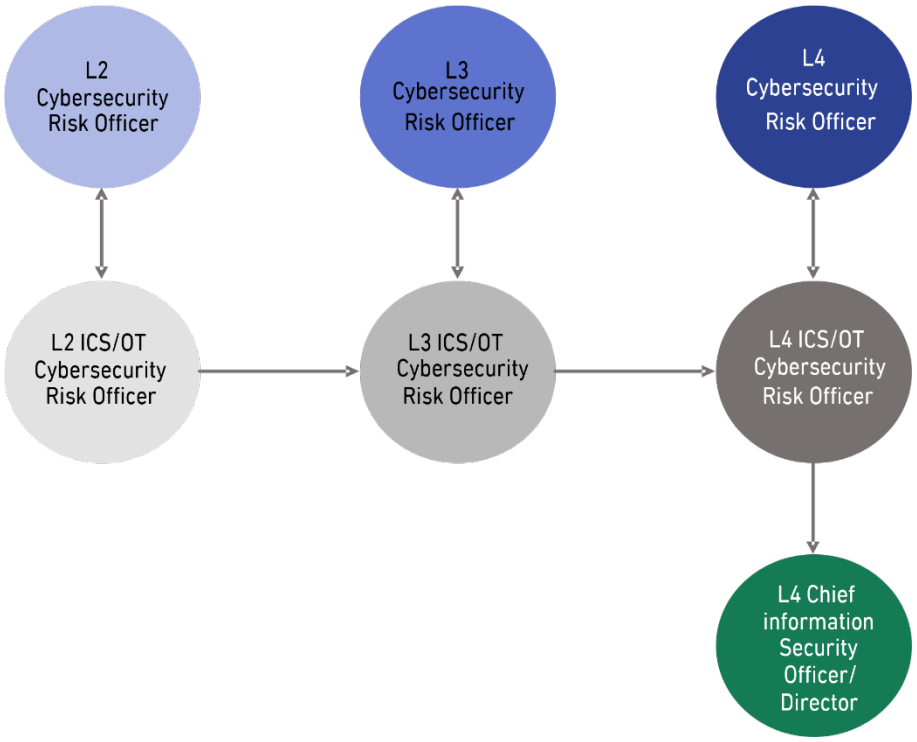

FIGURE 41: ICS/OT CYBERSECURITY RISK OFFICER CAREER MAP

6.4.1 L2 ICS/OT Cybersecurity Risk Officer

Job Role Name: ICS/OT Cybersecurity Risk Officer (ICSOT- ICSOT-004)	Job Level: Level 2
Role Description	Practitioner who 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 An individual in this role will carry out some of the basic tasks of the role and will continue to develop their skills through practical application of their work. Tasks will include providing input to the risk management framework and related documentation and carrying out cybersecurity risk assessments.

Career Progression (Pathway)	
The individual will have come from the following roles: • QR2 Entry Level Graduate • L2 Cybersecurity Risk Officer	The next career step for someone in this role is one of the following: • L3 ICS/OT Cybersecurity Risk Officer • L2 Cybersecurity Risk Officer

TABLE 129: L2 ICS/OT CYBERSECURITY RISK OFFICER

6.4.2 L3 ICS/OT Cybersecurity Risk Officer

Job Role Name: ICS/OT Cybersecurity Risk Officer (ICSOT- ICSOT-004)	Job Level: Level 3
Role Description	Senior Practitioner who 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. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 ICS/OT Cybersecurity Risk Officer. Tasks will include ensuring cybersecurity risks are identified and managed appropriately through the organization's risk governance process and working with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels.

Career Progression (Pathway)	
The individual will have come from the following roles: • L2 ICS/OT Cybersecurity Risk Officer • L3 Cybersecurity Risk Officer	The next career step for someone in this role is one of the following: • L4 ICS/OT Cybersecurity Risk Officer • L3 Cybersecurity Risk Officer

TABLE 130: L3 ICS/OT CYBERSECURITY RISK OFFICER

6.4.3 L4 ICS/OT Cybersecurity Risk Officer

Job Role Name: ICS/OT Cybersecurity Risk Officer (ICSOT- ICSOT-004)	Job Level: Level 4
Role Description	Expert managing a unit to identify, assess and manage cybersecurity risks within ICS/OT environments. Evaluates and analyzes the effectiveness of existing cybersecurity controls and provides feedback and recommendations based on assessments. An individual in this role will be responsible for providing oversight for much of the L3 ICS/OT Cybersecurity Risk Officer's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include ensuring that decisions relating to cybersecurity are based on sound risk management principles and establishing a risk management strategy for the organization that includes a determination of risk tolerance.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 ICS/OT Cybersecurity Risk Officer • L4 Cybersecurity Risk Officer	The next career step for someone in this role is one of the following: • L4 Cybersecurity Risk Officer • L4 Chief Information Security Officer / Director

TABLE 131: L4 ICS/OT CYBERSECURITY RISK OFFICER

6.5 ICS/OT Cybersecurity Incident Responder

The ICS/OT Cybersecurity Incident Responder investigates, analyzes, and responds to cybersecurity incidents within industrial control systems (ICS) and operational technology (OT) environments. This role requires certifications or training in ICS/OT cybersecurity, incident handling and response, digital forensics, malware analysis, network security monitoring, and Security Operations Center (SOC) processes.

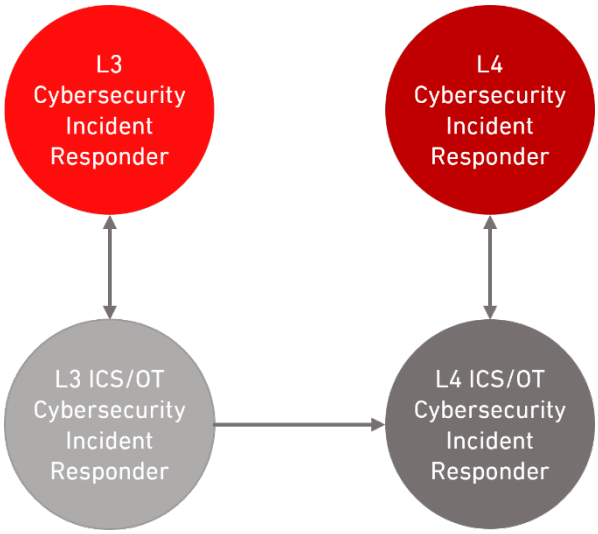

FIGURE 42: ICS/OT CYBERSECURITY INCIDENT RESPONDER CAREER MAP

6.5.1 L3 ICS/OT Cybersecurity Incident Responder

Job Role Name: ICS/OT Cybersecurity Incident Responder (ICSOT-ICSOT-005)	Job Level: Level 3
Role Description	Senior Practitioner investigating, analyzing and responding to cybersecurity incidents. An individual in this role will be responsible for carrying out complex role related tasks for review by, and working under the direction of, the L4 ICS/OT Cybersecurity Incident Responder. Tasks will include employing defense-in-depth principles and practices in line with organizational policies and collecting intrusion artefacts and using discovered data to mitigate potential cybersecurity incidents within the organization.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 Cybersecurity Incident Responder	The next career step for someone in this role is one of the following: • L4 ICS/OT Cybersecurity Incident Responder • L3 Cybersecurity Incident Responder

TABLE 132: L3 ICS/OT CYBERSECURITY INCIDENT RESPONDER

6.5.2 L4 ICS/OT Cybersecurity Incident Responder

Job Role Name: ICS/OT Cybersecurity Incident Responder (ICSOT-ICSOT-005)	Job Level: Level 4
Role Description	Expert managing a unit to investigate, analyze and respond to cybersecurity incidents. An individual in this role will be responsible for providing oversight for much of the L3 ICS/OT Cybersecurity Incident Responder's work, ensuring that it is completed to appropriate standards and within relevant timeframes. Tasks will include writing and publishing cyber defense techniques, guidance, and post incident reports to appropriate constituencies and working as a technical expert in support of law enforcement, explaining incident details and forensic analysis as required.
Career Progression (Pathway)	
The individual will have come from the following roles: • L3 ICS/OT Cybersecurity Incident Responder • L4 Cybersecurity Incident Responder	The next career step for someone in this role is one of the following: • L4 Cybersecurity Incident Responder

TABLE 133: L4 ICS/OT CYBERSECURITY INCIDENT RESPONDER


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority