CYBERPATH

Occupations Framework Discussion Paper

V 0.2 Draft discussion paper released for public consultation

Consultation opens May 2026 and closes 30 June 2026 at 5:00 PM AEST

Submit your response via the Web Form or visit cyberpath.acs.org.au/insights.html

Contents

1.0 Introduction

Australia's cyber security workforce is evolving rapidly, shaped by increasing threat complexity, accelerating technological change, and persistent skills shortages. As highlighted in the 2023-2030 Australian Cyber Security Strategy, *"Australia faces a growing shortage of cyber workers, while threats are increasing faster than the country can respond."* These pressures underscore the need for a coherent, nationally consistent way to describe cyber roles and the capabilities required to perform them.

The CyberPath Cyber Workforce Professionalisation Pilot is addressing this challenge by developing a scalable, industry-led framework that strengthens workforce capability and supports national resilience. A foundational component of this work is the Occupations Framework, which establishes a structured and coherent view of the roles that make up the cyber workforce.

The Occupations Framework provides the role architecture upon which the broader CyberPath ontology including competencies, pathways, assessment, and recognition will be built. It aims to reduce ambiguity, improve mobility, and support consistent workforce planning across industry, government, and education. The scope of the Occupations Framework encapsulates the purple boxes in the diagram below:

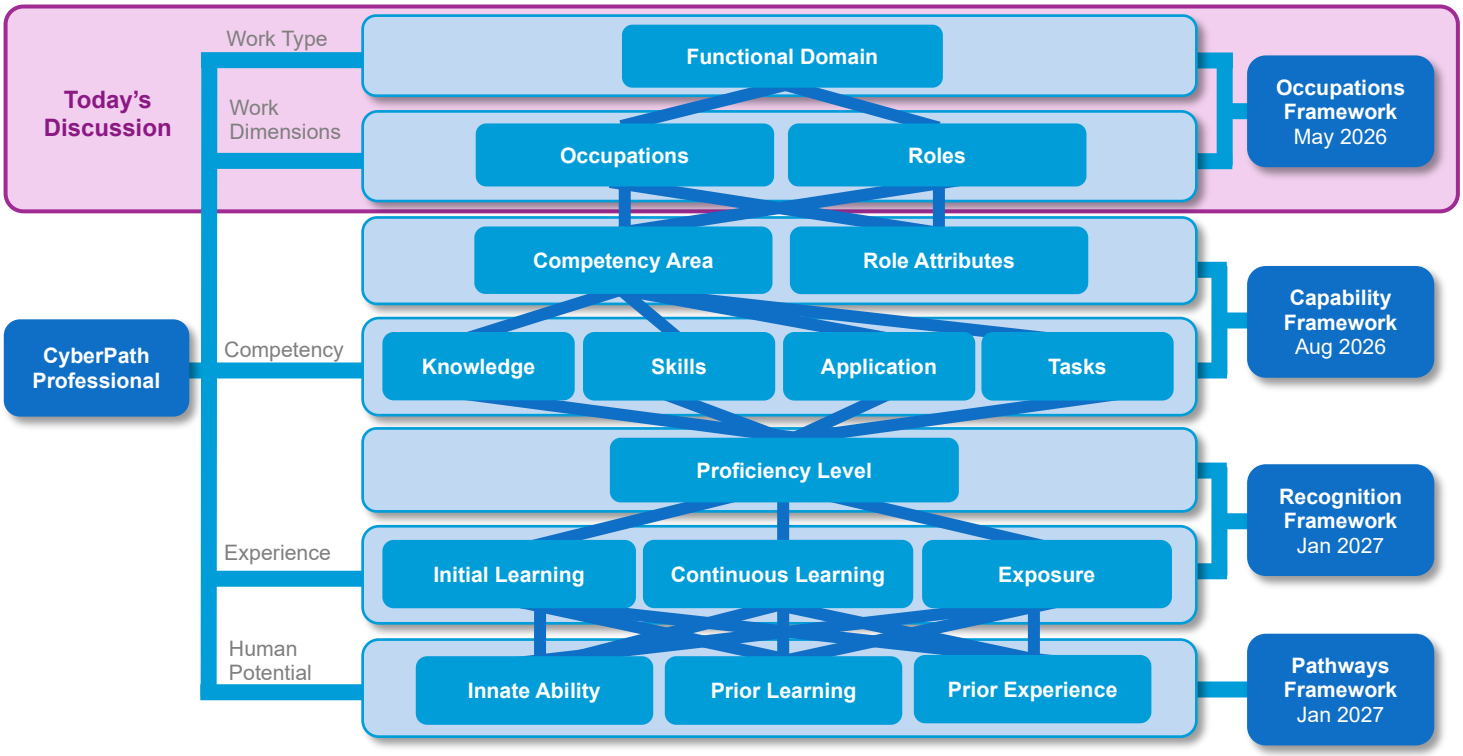


Figure 1 CyberPath Ontology

2.0 Overview of Methodology

The methodology undertaken for the CyberPath Occupations Framework design follows a structured, iterative process that consists of the following steps:

Step 1: Occupational Landscape Review

A comprehensive analysis of existing occupational classifications, job advertisements, organisational structures, and cyber workforce studies was conducted to identify common patterns, gaps, and emerging specialisations.

Step 2: Validation Through Consultation (Doing NOW)

Draft occupational groupings are tested with industry stakeholders to ensure accuracy, clarity, and usability. Feedback was incorporated through iterative refinement cycles.

Step 3: Alignment with Competency and Pathways Frameworks

Occupations will be mapped to competencies, proficiency levels, and learning pathways to ensure coherence across the broader CyberPath ecosystem.

Step 4: Role and Task Decomposition

Cyber work will be broken down into tasks, responsibilities, and functional domains. This aligns with the CyberPath ontology which includes *"functional domains, occupations/roles, competency areas, knowledge, skills, abilities, and attitudes."*

Step 5: Occupational Grouping and Taxonomy Design

Tasks and responsibilities will be clustered into coherent occupational groupings based on similarity, labour market patterns, and industry practice. This step ensures that occupations reflect real-world work rather than organisational idiosyncrasies.

Step 6: Future-Proofing and Update Mechanisms

A governance model will be designed to ensure the taxonomy remains current as technologies, threats, and workforce needs evolve. This respects the principle of *living competency frameworks* that adapt over time.

Figure 2 CyberPath Occupations Framework Methodology

2.1 Evidence Base and Inputs

The methodology behind the CyberPath Occupations Framework draws on three primary data sources to inform its design being OSCA - Occupation Standard Classification for Australia, established global workforce models, and industry consultation.

OSCA (previously ANZSCO) provides the foundational occupational structure used across government, labour market analysis, and education systems. While these standards offer essential alignment, they do not yet capture the full breadth of cyber specialisations. *Complexity of modern environments raises the bar for required* expertise is a theme that was consistently highlighted throughout the CyberPath industry consultation process.

This is particularly relevant across areas such as AI, OT, and cloud security, areas where adoption of technology outpaces occupational definitions, regulation, and in some cases development of appropriate strategies and secure by design principles.

CyberPath then reviewed global professionalisation and workforce models, including those from the UK, Singapore, Canada, the US NICE Framework, and European ECSF. With 37 programs examined across emerging, developing, and mature schemes, even across more mature jurisdictions examined, professionalisation globally is still an evolving area. Lessons learned from these models inform CyberPath's design principles, particularly around flexibility, inclusivity, and industry co-ownership.

Noting the emphasis and importance of co-design, CyberPath then undertook a process of engagement with employers, practitioners, educators, regulators, and DEI groups through workshops, interviews, surveys, and targeted consultations. The industry consultation was carried out independently by Evolved Group to capture a broad data set. This was then further augmented with deeper consultation carried out by the CyberPath program team to provide the finer details. This approach aligns with the grant objective of CyberPath being industry led for industry by industry and with a focus on capturing diverse stakeholder inputs.

One thing that was noted throughout the engagement process is that cyber capability varies significantly by organisation size, maturity, and sector. Smaller organisations often rely on hybrid roles, while large enterprises employ highly specialised practitioners. This diversity is reflected in the framework's layered design, ensuring it is usable across SMBs, government agencies, critical infrastructure, and large corporates.

Overall, through the extensive stakeholder engagement and consultation process, the framework has been shaped by the lived experience of the Australian cyber workforce.

See Appendices for further details.

3.0 Grouping Occupations into Domains

In developing an ontology for CyberPath, beginning at the occupation or job title level is too granular and quickly becomes unworkable. Job titles are notoriously inconsistent across organisations, jurisdictions, and industries. For example, what one organisation calls a *Cyber Security Analyst*, another may label a *Security Operations Specialist, Threat Monitoring Officer*, or *Information Security Technician*. Because job titles reflect organisational structure, legacy HR practices, or even branding preferences, they are a poor foundation for a national professionalisation framework.

Before beginning a conversation around occupations, we must first add a preceding categorising layer. This is common across various cyber and technical frameworks used globally; however the title of this categorising layer varies. Common titles include functional domains, job families, career families, capability clusters, role archetypes, or professional streams. These constructs group related types of work based on shared purpose, functional alignment, and underlying capability requirements, creating a stable arrangement that sits above the variability of job titles.

This top layer provides the conceptual scaffolding that allows a professionalisation program to be coherent, scalable, and future-proof as occupation dimensions evolve, particularly with emerging technologies. It captures the essence of what work is being done or cyber capabilities delivered, rather than how organisations choose to label it. For example, domains such as “Cyber Defence,” “Governance, Risk and Assurance,” “Secure Architecture,” or “Digital Forensics and Incident Response” remain relatively stable even as individual job titles evolve. By anchoring the ontology in these higher-order groupings, CyberPath can define competency standards, assessment pathways, and career progression models that reflect the real structure of the profession rather than the idiosyncrasies of organisational HR systems.

For HR teams, this layer is indispensable. It provides a consistent, cross-industry language for understanding the workforce, enabling more accurate workforce planning, capability mapping, and talent mobility. Instead of managing hundreds of unique job titles, HR can plan around a smaller number of coherent job families or functional domains that reflect how work is organised. This supports clearer succession planning, identification of capability gaps, and alignment of learning and development programs. It also helps organisations benchmark themselves against industry norms and anticipate emerging skill needs. In short, this top layer is the backbone of a professionalisation ontology, bringing structure, clarity, and strategic value to both the scheme and the organisations that rely on it.

3.1 Definition of an Occupation

In Australia, an occupation is formally defined as a *grouping of jobs that require similar skills, knowledge, and tasks, classified according to skill level and skill specialisation*. The classification of occupations in Australia is maintained by the Australian Bureau of Statistics (ABS) through the Occupation Standard Classification for Australia (OSCA) which is a skills-based classification of jobs and occupations (ABS, 2024).

Scope of OSCA

Jobs are a set of tasks designed to be performed by one person for an employer in return for pay or profit. This includes jobs undertaken via self-employment and jobs undertaken for payment in kind.

Occupations are a group of jobs requiring the performance of highly similar sets of tasks. Task similarity is defined in terms of 'skill level' and 'skill specialisation'.

Skill level refers to the requirements for competent performance of a set of tasks and determined by the range and complexity of the set of tasks performed. The broader and more complex the set of tasks, the greater the skill level of the occupation. It is measured operationally by considering the dimensions:

- the level or amount of formal education and training
- the amount of previous experience in a related occupation
- the amount of on-the-job training, and
- personal attributes.

Formal education and training refers to the level and amount of education and training required for competent performance of an occupation's tasks. It is measured according to qualifications in the Australian Qualifications Framework (AQF).

Previous experience is time spent gaining relevant work experience measured in months or years.

On-the-job training is the amount of training needed after starting work in a job. It is measured in months or years and may be undertaken at the same time as formal education and training.

Personal attributes are an alternative way to assess skill level and used where the other three elements fail to accurately describe the skill level.

Skill level is an attribute of jobs, not individuals and based on the requirements for competent performance of the occupation's set of tasks.

Skill specialisation relates to the tasks required of an occupation and defined in terms of field of knowledge required, tools and equipment used, materials worked on, and goods or services produced or provided.

Source: Australian Bureau of Statistics.

OSCA replaced the Australian and New Zealand Standard Classification of Occupations (ANZSCO) in 2024. On the other hand, the International Standard Classification of Occupations (ISCO) developed and maintained by the International Labour Organisation is a global framework to classify and organisation occupations. It is somewhat interoperable with OSCA because ANZSCO which formed the base line for

OSCA was originally designed using ISCO's structure, concepts, and hierarchy, allowing Australian occupation data to be compared and mapped internationally. This means that if CyberPath is aligned to OSCA, it also broadly creates a common language to describe Australian professionals to international stakeholders.

For the purposes of CyberPath, an occupation is defined as:

> *A recognised category of cyber security work defined by a coherent set of tasks, skills, and responsibilities that can be assessed, credentialed, and supported through professional standards.*

CyberPath explicitly aims to shape the professionalisation of the cyber workforce by clarifying roles, skills, and pathways, which inherently relies on a consistent definition of occupation. This aligns with the government's objective to:

- Define roles, skills, and career pathways for the cyber sector
- Standardise professional expectations across the workforce
- Support capability uplift through structured development and assessment

A clear definition of an occupation is essential to a cyber professionalisation program because it provides the stable foundation needed to build standards, assessments, and career pathways that are consistent across the workforce. It ensures the program is durable and scalable by anchoring cyber roles in a nationally recognised classification system, while also supporting inclusivity by giving individuals, regardless of background, a transparent understanding of how to enter and progress within the profession. It enables the development of credible, assessable competencies and helps employers, educators, and practitioners align expectations, ultimately strengthening the coherence and capability of Australia's cyber workforce.

Using OSCA as the foundation for defining cyber occupations matters because it connects the professionalisation program to the wider machinery of government. OSCA is the national standard for how occupations are classified, and many major government systems such as taxation, skilled migration, workforce planning, education funding, and labour market analytics are built around it.

If CyberPath aligns its occupational definitions with OSCA, it becomes interoperable with these systems rather than sitting outside them. That alignment allows cyber roles to be recognised consistently across policy domains, supports accurate workforce forecasting, and ensures that training pathways, visa settings, and taxation categories reflect the real structure of the cyber workforce. It also reduces duplication and confusion by giving employers, educators, and government agencies a shared language for describing cyber work.

See Appendix A for further details.

3.2 Occupations, Roles and Scalability

In workforce planning, an occupation is a broad labour-market category defined by a shared set of skills, knowledge, and tasks, while a role is the specific job an individual performs within an organisation. This distinction becomes particularly visible in cyber security. OSCA defines occupations at a high level such as Cyber Security Analyst or ICT Security Specialist based on national labour-market standards. But smaller organisations rarely have the scale or resources to employ the full suite of discrete cyber occupations to meet the full spectrum of cyber security capability requirements.

Instead, they often rely on one or two individuals who perform a blend of tasks spanning multiple occupational categories. As you go down in organisation size and maturity, there's often overlaps between IT professionals and cyber security whereby an individual in a role that is defined as sitting within an IT occupation takes on cyber security responsibilities. For example, it's common for a single employee might manage network administration, incident response, governance tasks, and user support, even though these activities span several OSCA-defined occupations. This creates a practical conundrum: the labour market classifies cyber work into distinct occupations, yet the operational reality, especially in SMBs, regional organisations, and start-ups, is that cyber responsibilities are distributed across hybrid or generalist roles.

This distinction matters deeply for CyberPath. A professionalisation program must define standards, competencies, and assessment pathways that align with recognised occupations, but it must also reflect how cyber work is actually performed across different organisational contexts. If the program is too rigidly tied to occupational categories, it risks excluding the many practitioners who operate in blended or multi-disciplinary roles. Conversely, if it focuses only on roles, it loses the ability to integrate with national workforce systems, education pathways, and government policy settings that rely on occupational classifications. CyberPath therefore requires a layered approach: occupations provide the structural backbone for national consistency, while roles capture the lived reality of cyber work. This duality ensures that individuals can be recognised for the competencies they practically use, even if their job title or organisational context does not map neatly to a single OSCA occupation.

The Canadian Cyber Security Skills Framework offers a useful case study in how to reconcile this tension (Communications Security Establishment, 2023). Canada explicitly designed its framework to be scalable across organisation size, maturity, and operating environment, recognising that cyber capability looks very different in a federal department, a large enterprise, and a small business. Rather than forcing organisations to adopt rigid occupational structures, the Canadian model defines a set of competency-based work roles that can be combined, expanded, or collapsed depending on organisational need. A small organisation might assign several work roles to one generalist practitioner, while a large organisation might distribute those same

roles across multiple specialists. This flexibility allows professionalisation to be inclusive and realistic: individuals can be assessed and recognised for the competencies they perform, regardless of whether they work in a highly specialised environment or a resource-constrained one. The Canadian approach demonstrates that a national professionalisation scheme can maintain alignment with occupational standards while still accommodating the diverse ways cyber work is organised in practice, a principle that is highly relevant to the Australian context noting the dominance of SMBs across the economy.

3.3 An ontology for CyberPath Roles

A core requirement for a professionalisation program is standardising the definition of how we describe roles. This removes ambiguity, making it easier for employers as well as practitioners to understand the requirements and realities of a role. In standardising an ontology, there is a fine line between being too generic and being too prescriptive which leads to a loss of utility given the diversity across organisational contexts. Similar approaches have been leveraged in other frameworks such as SFIA which have enough detail to describe the nature of the work, without going to the fine detail around technologies, vendors, etc. As well as offering flexibility, taking this approach enables CyberPath to remain durable and require fewer updates which would otherwise also introduce additional administrative and operational overhead.

A flexible ontology means there is tailoring that will need to be carried out by an organisation to cater for their unique context and operational requirements:

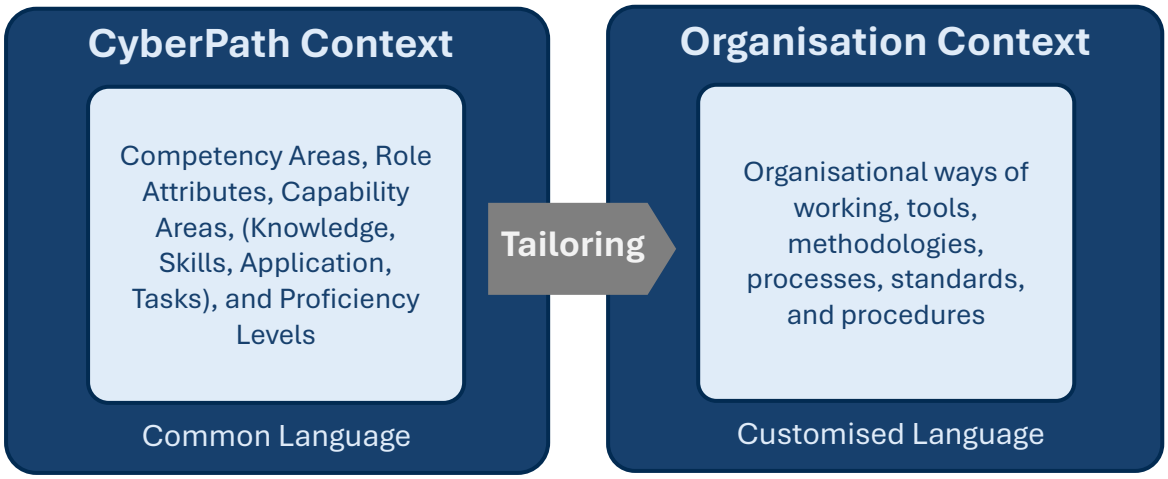


Figure 3 Tailoring in Context

With this concept in mind, to develop a standardised approach to describe CyberPath professionalised roles, organisations and individuals must consider what information should be common and established under a professional standard, and what makes sense to customise without imposing constraints on utility and durability.

There also needs to be an agreed upon working definition for each ontology element to assist with understanding what information should be included. The following role definition fields are proposed to define the various elements that would form part of a standardised role definition. This could then be leveraged as a template for consistent job descriptions across the sector. The table below presents a proposed glossary and draws a distinction between the common (CP) and customised (ORG) elements:

	Role Fields	Working Definition
CP	**Role Title**	The accepted title for a CyberPath professionalised role.
ORG	**Alternative job titles**	Other common job titles used across industry.
CP	**OSCA mapping**	Where applicable, a mapping to the Occupation Standard Classification for Australia (OSCA) system for occupations (previously ANZCO codes).
CP	**Domain**	A grouping of jobs having similar characteristics such as skills, responsibilities and career paths but requiring different levels of skill, responsibility, or working conditions. A career family may also be referred to as a specialty area. Career families are used to benchmark jobs to create fair remuneration and incentives.
CP	**Common entry points (technical adjacent)**	Typical entry pathways for people into the role from existing cyber adjacent backgrounds. I.e. technical (IT), consulting or risk management roles. Because talent in these roles will often have some underpinning knowledge that is required for cyber roles, building capabilities from this labour pool has a faster ramp up to required proficiency levels.
CP	**Common entry points (non-technical)**	Scaling the Australian sovereign cyber workforce requires bringing new talent into the industry through reskilling from other occupations to increase the pool of talent in the cyber workforce. This represents typical roles that have similar skills or 'ways of thinking' which increase the likelihood of success in transitioning into cyber technical roles.
CP	**Common exit points**	Modern careers in cyber don't necessarily follow the traditional linear career progression of other professions where someone "progresses through the ranks". It is more typical for people to move laterally in their careers through the portability and applicability of skills across multiple role areas. This area focuses on typical non-linear career options for people transitioning through these roles.
CP	**Inputs**	The upstream inputs exploited to achieve the role's effects such as data, information, intelligence and processes.
ORG	**Organisational alignment**	Where the role sits in supporting a broader organisation strategy and/or forms a part of a holistic cyber risk management strategy.
CP	**Outputs**	The typical deliverables or artefacts produced by the role as well as the consumer/beneficiary of those outputs.
ORG	**Relationships**	Key people, teams and organisations that this role interacts with.
CP	**Skills**	Capabilities required to perform specific practical/hands-on tasks effectively and accurately. This includes technical skills, such as using tools and equipment, analysing data, and following procedures, as well as learned interpersonal skills for effective communication, collaboration, and problem-solving.
CP	**Knowledge**	The theoretical and practical understanding of a particular subject or field required to undertake the role. This includes familiarity with relevant principles, concepts, terminology, procedures and best practices.
CP	**Application**	The real-world use of knowledge and skill in authentic or simulated contexts.
ORG	**Tasks**	Tasks are the concrete activities, responsibilities, and outputs that make up a real-life role. It represents actual work performed by practitioners in a specific workplace and provides context of how ability, skill, and application are observed.
ORG	**Tooling and technologies**	The tooling and technologies used in this role to achieve effects.
CP	**Learning Pathways**	This has been omitted as using prescriptive qualifications and certifications can act as a barrier to accessibility and inclusion by diminishing attractiveness to underrepresented groups.

	Role Fields	Working Definition
CP	Qualifications and certifications	This has been omitted as using prescriptive qualifications and certifications can act as a barrier to accessibility and inclusion by diminishing attractiveness to underrepresented groups.

4.0 Proposed CyberPath Occupations Framework

The CyberPath Occupations Framework provides a structured, nationally consistent way to describe cyber security occupations. It is designed to be:

- **Aligned** with OSCA and national workforce systems
- **Flexible** enough to reflect hybrid and generalist roles
- **Scalable** across organisation size and maturity
- **Future-ready**, accommodating emerging specialisations
- **Inclusive**, supporting diverse entry pathways

The CyberPath lexicon uses the terms occupation and roles interchangeably to enable consistency for larger organisations that hire dedicated cyber specialists, as well as smaller organisations that leverage cyber generalists, often in traditional IT roles.

However, for clarity, to delineate between an occupation and a role:

- **Occupations** - Within each functional domain, occupations represent OSCA recognised definitions of cyber work. This enables national alignment, workforce planning, education design, and professional standards. Under CyberPath pathways, these are designed to be assessable and credential-ready.
- **Roles** - Roles describe how cyber work is performed within organisations. They reflect real-world job structures and may combine tasks from multiple occupations, particularly in SMBs, and early-stage companies.

This layered approach mirrors the Canadian model, which allows roles to be combined, expanded, or collapsed depending on organisational need. It ensures that CyberPath can recognise practitioners working in blended or multidisciplinary roles while maintaining alignment with national occupational standards. This structure ensures:

- Practitioners in hybrid roles are not excluded
- Employers can map their workforce regardless of size or maturity
- Educators can align curricula to recognised occupations
- Government can use consistent occupational data for policy and planning
- The framework remains adaptable as new specialisations emerge

For the purposes of CyberPath professional titles, and going forward, the word “Roles” will be used and is defined as:

"A recognised category of cyber security work defined by a coherent set of tasks, skills, and responsibilities that can be assessed, credentialed, and supported through professional standards."

This layered approach mirrors the Canadian cyber workforce model, which allows roles to be combined, expanded, or collapsed depending on organisational need. It ensures that CyberPath can recognise practitioners working in blended or multidisciplinary roles while maintaining alignment with national occupational standards.

This structure ensures:

- Practitioners in hybrid roles are not excluded
- Employers can map their workforce regardless of size or maturity
- Educators can align curricula to recognised occupations
- Government can use consistent occupational data for policy and planning
- The framework remains adaptable as new specialisations emerge

4.1 CyberPath Functional Domains

A CyberPath domain is the categorising layer that groups together related types of work based on shared purpose, functional alignment, or the organisation's underlying capability requirements. Often functional domains are reflected in the hierarchical structure of larger organisations as the names representing a business unit, team, or division. In other frameworks and in HR language, functional domains are also commonly referred to as job families, career families, capability clusters, role archetypes, or professional streams.

Using functional domains as an organising structure creates the stable ontology for CyberPath that mitigates the variability of job titles used across organisations as well as providing scalability of the solution that's reflective of the Australian organisation context which is fragmented in terms of sizes and dominated by SMBs.

The functional domains defined under CyberPath are:

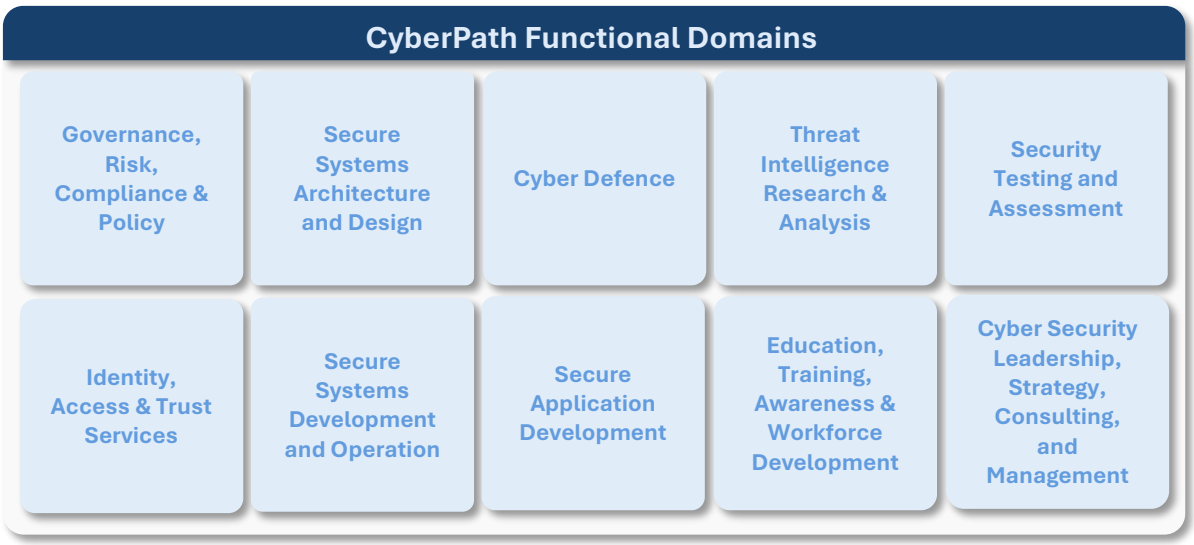


Figure 4 CyberPath Functional Domains

Domains	Description	Example Job Titles
Governance, Risk, Compliance & Policy	• Cyber security governance • Risk management of cyber security risk as part of a broader enterprise risk management • Develops and maintains policies that align organisational cyber security objectives and regulatory requirements • Internal audit and overall cyber security program assurance • Monitoring protective security and insider threat risk • Monitors regulatory environment and provides legal advice and recommendations • Oversees privacy, information, and data compliance • Assures information management • Measures, baselines, and monitors organisational cyber security maturity • Inventories and manages assets from acquisition to sustainment, to disposal	• GRC analyst • IRAP assessor • Cyber policy officer • Privacy advisor • Protective Security officer • Legal advisor
Secure Systems Architecture and Design	• Translating organisation needs into 'secure by design' systems blueprints • Identifying requirements for security controls applied to cloud, on-premises, and hybrid environments • Designs network topologies and defines the security integration requirements • Develops reference architecture standards in line with best practices, budget, and organisational goals • Authorises systems into service based on acceptable organisation risk level • Assesses cyber security supply chain risk policies, processes, and procedures • Consults with internal and external stakeholders to gather and translate functional requirements into appropriate technical solutions, security control requirements, and security policies	• Security architect • Cloud security architect • Presales engineer • OT Architect • Solutions architect • Enterprise architect • Business analyst • COMSEC Manager

Domains	Description	Example Job Titles
	• Develops and implementing plans, policies and practices that control, protect and govern data assets. • Specifies and designs hardware systems and components to meet agreed security design principles and standards.	
Cyber Defence	• Analyses data from various log sources to identify, triage, and respond to potential threats • Investigates cyber security incidents • Assess cyber security incident impacts, identifies mitigations and supports eradication and recovery from threats • Monitors advisories and scans the enterprise IT environment to identify risks • Performs threat hunting and purple teaming activities • Identifies, collects, and examines digital evidence using controlled methods and preservation techniques • Enabling data-driven decision making by extracting, analysing and communicating insights from structured and unstructured data.	• SOC analyst • Incident responder • Digital Forensics specialist
Threat Intelligence Research & Analysis	• Collects, processes, and analyses all source threat intelligence sources to provide actionable insights • Identifies capabilities of threats and conducts contextualised threat modelling for the organisation • Conducts applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses • Analyses malware • Develops cyber security indicators to support detection of threats as part of security operations • Researches new and emerging technologies to evaluate potential vulnerabilities • Testing networks and applications to identify security control gaps and weaknesses before adversaries find them	• Threat analyst • Vulnerability researcher • Malware researcher
Security Testing and Assessment	• Plans and executes tests of networks, systems, and applications to identify effectiveness of applied security controls • Assesses deviations from best practice and security configuration baselines, providing advice to enhance risk posture • Measures effectiveness of defence in depth architecture • Executes automated scanning of environment to identify vulnerabilities • Plans, executes and manages offensive cyber security operations, including target selection, simulated attack, and post-operation analysis • Collaborates with intelligence and security teams to integrate offensive cyber security operations with broader objectives	• Vulnerability analyst • Penetration Tester
Identity, Access & Trust Services	• Develops processes and policies for Identity governance, PAM, authentication • Supports the engineering capabilities required for digital identity integration (e.g., TDIF, myGovID) • Manages identity verification and access permissions within organisational systems and environments.	• IAM policy specialist • PAM engineer • Digital identity architect
Secure Systems Development and Operation	• Installs, configures, tests, and maintains secure configuration of, and administers cyber security infrastructure • Plans, implements, and operates network services and systems • Manages backup and recovery of systems	• Network security engineer • Secure endpoint engineer

Domains	Description	Example Job Titles
	• Configures and manages endpoint security • Configures, and maintains the safety, reliability, and security of industrial (OT/ICS) systems	• Systems administrator • Infrastructure support • OT security specialist
Secure Application Development	• Secure application development, modification, and maintenance • Tests and evaluates application security throughout the development lifecycle • Managing the release and transition of new and updated applications into production environments • Integrates application components across the internal and external IT environment • Designs, builds, operationalises, secures, and monitoring data pipelines, stores and real-time processing systems for scalable and reliable data management to provide security operations teams with visibility into the environment • Secure software integration and configuration	• AppSec engineer • Software developer • Systems integration engineer • DevSecOps engineer • Detection engineer • Secure software developer
Education, Training, Awareness & Workforce Development	• Develops and/or delivers cyber security awareness programs • Develops cyber security curriculum and training packages • Delivers training in academic/VET education environments • Anticipates cyber security workforce needs, conducts gap analysis and develops workforce plans • Facilitates cultural and behavioural change by enabling individuals to embed new ways of working and adapt to changes as part of cyber security cultural uplift • Plans, designs and implements the transition of organisations and people through cyber security change	• Cyber security trainer • Cyber security awareness lead • Cyber security trainer and/or lecturer • Organisational change manager • Cyber security workforce manager
Cyber Security Leadership, Strategy, Consulting, and Management	• Establishes vision and direction for cyber security program strategy in line with organisation objectives • Supports costing, budgeting and develops security program plans • Advocates for, and ensures cyber security is considered in all critical infrastructure and assets • Overall accountability for developing and running a cyber security program • Develops board/executive level reporting with actionable intelligence on cyber security risk posture • Manages and governs delivery of cyber security programs, projects and maturity uplift initiatives • Provides people leadership and management for cyber security teams or business functions • Oversees development, implementation, and management of cyber security operational capability • Manages knowledge and intellectual capital of the organisation • Provides specialist cyber security advice and recommendations, based on expertise and experience, to address client and/or internal stakeholder needs. • Sources and manages suppliers to establish secure supply chains • Systematically analyses, manages and influences internal and external stakeholder relationships through structured engagement	• CISO • Cyber security program/project managers • Cyber security consultants • Sales and account executives • Solutions consultant • Information security manager • Cyber security team leader • Cyber strategy lead • Delivery manager • Crisis management

Note that these domains reflect cyber specialist domain areas and do not reflect cyber integrators or the broader workforce base that may handle some level of cyber responsibilities or interact with the cyber team. These areas may be pathways into professionalisation, but in terms of defining professional standards or roles for them, this is out of scope for the CyberPath professionalisation pilot program. To understand these other areas, they can be grouped as:

- **Cyber Generalist** roles are IT and adjacent technical expert roles that integrate cyber considerations into broader work, systems, and processes. That is, they handle some level of cyber tasks responsibilities as part of a broader role. This is common in smaller organisations and creates a neat pathway for IT workers looking to transition into dedicated cyber security roles.
- **Cyber Enabler** roles are non-technical business functions such as procurement teams, vendor managers, as well as broader enterprise risk roles. These roles work closely with cyber security specialists to ensure cyber security risk is managed appropriately across broader business operations.

4.2 CyberPath Roles

As part of the CyberPath pilot, a selection of roles has been chosen to test the framework and allow adjustments based on industry consultation and testing. This ensures utility for the Australian context and is referenced herein as the pilot MVP. This follows a similar approach to that used in other professionalisation schemes implemented globally whereby professionalised roles have been progressively rolled out as their overarching frameworks have matured and iterated.

The proposed MVP roles for CyberPath are:

1. Cyber Security Architect
2. GRC Analyst
3. Chief Information Security Officer (CISO)
4. SOC Analyst

The CyberPath MVP requires a focused set of occupations that can demonstrate the value of a national professionalisation framework while providing early impact for employers, practitioners, educators, and government. These four roles have been selected based on their ability to represent:

- High-demand and high-risk areas
- Clear workforce gaps or inconsistencies
- Strong alignment with national priorities
- Opportunities to uplift diversity and inclusion
- Roles where professional standards can meaningfully reduce risk
- Roles that span both entry-level and advanced career pathways

A summary rationale behind the selection of each of these is outlined below:

Role	Why It Is Critical	Challenges	Opportunities	Expected Impact
Cyber Security Architect	• Strategically essential for secure-by-design, AI adoption, OT/IT convergence, and quantum readiness. • High influence on organisational resilience and long-term technical direction.	• Lack of clear pathways into architecture roles. • Heavy reliance on expensive contractors, especially in government. • Underrepresentation of diverse groups. • Inconsistent expectations and no national competency model.	• Establish a nationally consistent model for architectural practice. • Structured pathways to reduce reliance on contractors and retain organisational knowledge. • Encourage diversity by clarifying entry and progression routes.	• Reduced technical debt and improved secure-by-design adoption. • Stronger internal capability and reduced contractor dependency. • Increased diversity in senior technical roles. • Better preparedness for AI, cloud, OT, and quantum disruption.
GRC Analyst	• High-volume entry pathway into cyber. • Critical for regulatory compliance, risk management, and board-level reporting. • Strong alignment with national governance expectations.	• Entry-level friendly but limited progression without technical uplift. • Imposter syndrome and confidence barriers for under-represented groups. • Global definitions exist but lack Australian sector-specific nuance (APRA, SOCI, Privacy Act).	• Define an Australian-context GRC competency model. • Strengthen technical depth and progression pathways. • Improve accessibility and confidence for diverse entrants.	• More job-ready GRC practitioners. • Stronger compliance and risk management across sectors. • Increased diversity in governance-focused cyber roles. • Better alignment between regulation and workforce capability.
Chief Information Security Officer	• Holds organisational accountability for cyber outcomes. • Central to governance, risk, incident response, and workforce leadership. • Key to national resilience and surge capability.	• Highly inconsistent expectations across organisations. • Heavy reliance on certifications (CISSP, CISM) that create barriers for diverse practitioners. • No standardised ethical or professional requirements.	• Establish a professional standard with ethics, accountability, and competency-based assessment. • Reduce reliance on certification-only pathways. • Support leadership development and inclusive progression.	• More consistent and accountable cyber leadership. • Improved organisational maturity and resilience. • Reduced barriers for women and career changers. • Stronger national surge capability.
SOC Analyst	• One of the most common technical entry points. • Essential for threat detection, monitoring, and incident response. • Directly supports national threat readiness.	• Many graduates are not job-ready; training often lacks real-world context. • Over-reliance on tools and playbooks. • Limited understanding of enterprise infrastructure and attacker behaviour. • High burnout and limited progression pathways.	• Develop a practical, scenario-based competency model. • Build foundational IT, infrastructure, and threat-hunting skills. • Clarify progression into advanced technical roles.	• More capable frontline defenders. • Reduced burnout and improved retention. • Stronger threat detection and response capability. • Better mobility into higher-value roles (IR, threat hunting, engineering).

This rationale is explained in further detail below across each of the roles:

4.2.1 Cyber Security Architect

Cyber Security Architects are among the most strategically important and structurally under-defined roles in the Australian cyber workforce. They sit at the intersection of technology strategy, risk management, secure-by-design principles, and organisational transformation. Yet despite their importance, pathways into architecture roles remain unclear, inconsistent, and often inaccessible.

The accelerating skills burden stemming from emerging technologies directly impact architectural functions. Architects must design secure systems that integrate cloud, SaaS, OT/ICS, AI, and legacy environments, often simultaneously. The rapid adoption of AI without adequate architectural oversight, combined with the looming threat of quantum-enabled cryptographic disruption, as well as the convergence of IT and OT has intensified demand for skilled architects.

At the same time, secure-by-design principles are becoming central to government and industry expectations. Architects are the primary custodians of these principles, yet Australia lacks a consistent competency model to define what “good” looks like in this role or clear pathways into that role.

Cyber Security Architects are traditionally among the most expensive and difficult-to-source cyber professionals. Many organisations, particularly government agencies and critical infrastructure providers, rely heavily on contractors to fill architectural gaps. This creates several systemic risks including:

- High cost and low sustainability
- Loss of organisational knowledge when contractors depart
- Accumulation of technical debt due to inconsistent architectural oversight
- Limited internal mobility pathways, reducing retention

With architecture forming the foundation for good cyber security culture and practice, and with a stated aim of professionalisation being reducing harm from unqualified practitioners creates a sound rationale for this role being included in the CyberPath MVP. Architecture is a prime example of a role where without clear standards, organisations struggle to distinguish between experienced architects and individuals who have simply accumulated technical experience.

Architecture roles are significantly underrepresented by women and other diverse groups. As per the 2023-2030 Australian Cyber Security Strategy, unclear roles and inconsistent expectations disproportionately affect underrepresented groups. Architecture is a textbook case: ambiguous pathways, opaque expectations, and reliance on informal networks create barriers to entry.

Cyber Security Architect is an ideal MVP occupation because it is:

- high-risk, high-demand, and strategically essential
- suffers from unclear pathways and inconsistent expectations
- a role where professional standards can materially reduce national cyber risk
- an enabler for internal mobility, reducing reliance on expensive contractors
- key for national priorities around secure-by-design, AI, and quantum readiness
- a strong test case for competency-based assessment at advanced proficiency levels

A competency-based professionalisation model can:

- Clarify pathways into architecture
- Recognise diverse prior experience
- Reduce reliance on informal gatekeeping
- Support targeted development programs

Note that Cyber Security Architect may be considered as a broad category however individuals may specialise or focus in particular areas with titles such as Solution Architect, Cloud Security Architect, OT/ICS Security Architect, and AI/ML Security Architect. From an accreditation and professional title perspective, the core competency requirements for a Cyber Security Architect as defined by CyberPath remains the same across these, however there may be additional technical skill and knowledge requirements to specialise across those areas.

Selecting this occupation for the MVP demonstrates CyberPath's ability to uplift complex, senior, and strategically important roles while supporting diversity, workforce sustainability, and national resilience. At the same time, this creates capacity within the workforce to bring junior talent in.

4.2.2 GRC Analyst

Governance, Risk, and Compliance (GRC) Analysts represent one of the most common and accessible entry points into the cyber security profession. The role is well-defined globally, yet in Australia it is shaped by unique regulatory, sectoral, and regional requirements. This makes it an ideal occupation for early professionalisation.

GRC Analyst roles are often viewed as accessible for early-career practitioners because they require strong analytical skills, communication capability, and foundational cyber knowledge. However, many practitioners report difficulty progressing beyond entry-level tasks due to limited technical exposure and confidence. A competency-based model can help practitioners:

- Build technical depth
- Understand risk in operational contexts and across sectors

- Transition into more advanced roles such as risk advisors, compliance leads, or specialist roles

This also helps combat imposter syndrome, which is often further disproportionately experienced by underrepresented groups in GRC pathways.

While GRC roles are globally recognised, Australia's regulatory environment introduces unique dimensions. Consequently, GRC is a role area where sector tailoring within a national standard is highly relevant. The CyberPath competency model should consider the knowledge, context and obligations under different legislation such as:

- APRA CPS 234
- SOCI Act requirements
- Privacy Act reforms
- ISM/IRAP schemes
- State-based regulatory obligations
- Sector-specific standards (e.g., health, finance, energy)

Defining baseline requirements under common frameworks such as this creates an opportunity to better set up aspiring practitioners for success and provides the extra value beyond generic globally aligned qualifications and training pathways.

Demand for GRC Analysts continues to grow as boards and executives face increasing accountability and tightening regulatory requirements. Recent policy reforms and evolving regulatory requirements around areas such as AI have created accountability mechanisms where boards and executives must now treat cyber as a core governance responsibility. This has driven a surge in demand for practitioners who can translate technical risk into business language and ensure organisations meet their compliance obligations. This is often delegated to GRC analyst roles, which will likely see growth in demand for this area.

As with the Cyber Security Architect occupation/role, the GRC Analyst professional title has a core set of competencies, however a GRC Analyst may choose to focus or specialise in a particular sub-discipline such as Compliance Analyst, Risk Analyst, Policy & Assurance Analyst, and Privacy & Data Protection Analyst.

GRC Analyst is an ideal MVP occupation because:

- It is a high-volume, high-demand entry pathway
- It allows CyberPath to demonstrate sector-specific tailoring
- It supports diversity and inclusion, particularly for women entering cyber
- It provides a clear test case for competency-based progression beyond entry level with pathways into more technical domains.

- It aligns with national priorities around governance, accountability, and risk reduction

Selecting GRC Analyst for the MVP allows CyberPath to demonstrate immediate value for early-career practitioners, employers, and regulators.

4.2.3 Chief Information Security Officer

The Chief Information Security Officer (CISO) role holds organisational accountability for cyber security outcomes. They translate strategy into action, oversee teams, manage risk, and ensure compliance. Yet despite the critical nature of this role, expectations are inconsistent and often tied to certification requirements that create barriers for diverse practitioners.

A hallmark of professionalisation schemes is the stipulation around *ethics codes, complaints and disciplinary processes*. The other characteristic trait around ongoing development and performance checks is critical for CISOs who need continuous professional development to remain current on the outcomes they are accountable for in a changing regulatory, threat and technology landscape.

They are responsible for:

- Setting organisational cyber direction
- Managing budgets and resources
- Ensuring compliance with regulatory obligations
- Overseeing incident response
- Advising executives and boards
- Managing teams and developing talent

Given this level of responsibility and the potential impacts of cyber events on a business as well as the broader supply chain means that professional standards are essential. Similarly, this role is critical to national resilience by ensuring that organisations can:

- Prevent and respond to incidents
- Meet regulatory obligations and consumer expectations
- Build sustainable cyber capability
- Mobilise during national-level events

When considering the potential requirement for rapid mobilisation of trusted practitioners during major incidents, CISOs are essential to support and coordinate that mobilisation.

CISO roles are frequently advertised with requirements such as the $(ISC)^2$ CISSP or ISACA CISM certifications. While valuable, these certifications are expensive, require years of experience, are exam-centric rather than competency-centric, and can create barriers for women, career changers, and regional practitioners. If a stated aim of

CyberPath is encouragement of inclusive and diverse workplace cultures whilst reducing unnecessary barriers to participation, a competency-based professionalisation model can provide a more inclusive alternative to certification-only pathways.

The CISO role is an ideal MVP occupation because:

- It is a high-accountability, high-impact role
- It requires professional standards, ethics, and ongoing development
- It is central to governance, risk management, and national resilience
- It provides a test case for reducing certification-based barriers
- It supports leadership development and workforce retention

Selecting this occupation demonstrates CyberPath's commitment to uplifting leadership roles and embedding ethical, accountable practice across the profession.

4.2.4 SOC Analyst

Security Operations Centre (SOC) Analysts are one of the most common entry points into technical cyber security. However, despite the volume of training programs and certifications available, many new entrants are not adequately prepared for real-world SOC environments.

SOC roles are essential for intelligence led operations, threat detection, incident response, and continuous monitoring. A recurring theme throughout the CyberPath consultation process was that *graduates and workforce entrants are not job ready and often require further on-the-job training*. This is particularly evident in SOC environments, where analysts must:

- Interpret alerts
- Understand attacker behaviour
- Recognise lateral movement
- Correlate events across systems
- Communicate findings to stakeholders

Many training programs focus on tools rather than context, leaving analysts reliant on playbooks rather than developing deeper analytical capability. At the same time, many training programs rely on simulated environments, which are often not reflective of production environments, leaving to a lack of readiness. A CyberPath competency model for SOC Analysts can address several systemic issues:

- Lack of exposure to real-world scenarios
- Limited understanding of enterprise infrastructure
- Insufficient grounding in general IT fundamentals
- Over-reliance on vendor tools

- Limited business and commercial awareness
- Limited experience to incident management in an enterprise environment and engaging with business stakeholders

Further, SOC Analysts are exposed to a very broad range of potential incidents, and incidents may be infrequent but high complexity. Owing to the range of incidents and technical complexity, continuous learning and exposure to different scenarios and learning opportunities is critical to not only build SOC Analyst knowledge, but also to build resilience within a safe environment. This exactly the kind of structured development that CyberPath could offer.

Whilst mobility options may be well defined in larger organisations, many less mature and smaller organisations often lack well defined career development opportunities. This can lead to SOC Analysts often struggling to transition into adjacent complementary roles or more advanced technical roles such as threat hunting, incident response, or engineering. A competency-based model can:

- Clarify progression pathways
- Recognise practical experience
- Reduce attrition caused by burnout
- Support transitions into higher-value roles

SOC Analyst is an ideal MVP occupation because:

- It is a high-volume, high-demand entry role
- It highlights the need for practical, scenario-based competency assessment
- It supports career mobility and retention
- It demonstrates CyberPath's ability to uplift technical roles
- It aligns with national priorities around threat detection and response

Selecting SOC Analyst for the MVP allows CyberPath to demonstrate immediate value for early-career practitioners and employers while strengthening Australia's frontline cyber defence capability.

4.2.5 Future CyberPath Role Candidates

Once the MVP roles have been tested and accepted by industry and the broader CyberPath framework has been proven, potential candidates for the next iteration and their rationale is summarised in the table below:

Occupation	Why It's Needed	Alignment with Playbook
Cloud Security Engineer	Rapid cloud adoption; misconfiguration risk; shortage of skilled practitioners	Cloud security listed as a top in-demand skill area
IAM Specialist	Identity compromise is the #1 attack vector; zero-trust adoption	Identity security and access control highlighted as foundational capabilities
Incident Responder / Forensics Specialist	Rising incident volume; need for national surge capability	Incident response and digital forensics identified as critical shortage areas
Secure Software Developer / DevSecOps Engineer	Secure-by-design imperative; software supply chain risk	Secure coding and DevSecOps listed as priority skills
OT/ICS Security Specialist	Protects critical infrastructure; high-risk, high-scarcity role	OT/ICS security listed as a national priority capability
Data Security & Privacy Engineer	Rising data breaches; privacy reforms; AI data governance	Data protection and privacy engineering identified as key skill gaps
AI Security & Assurance Specialist	Rapid AI adoption; emerging attack vectors; regulatory focus	AI security, safety, and assurance listed as emerging high-demand skills

See for Appendix D for more details on future role candidates.

5.0 Public Consultation

Over the last four months, CyberPath Consortium Partners have hosted a national town hall series, conference events, small-group sessions, independent research and interviews, as well as attended external engagements and meetings to develop the CyberPath Occupations Framework. While these activities have gathered valuable insights, feedback, and questions from a broad group of stakeholders, CyberPath recognises that not everyone has had the opportunity to participate in these activities.

This public consultation provides an open and structured opportunity for all interested parties to contribute feedback on the CyberPath Occupations Framework Discussion Paper before the CyberPath Framework and pilot design is finalised. Any individual, organisation, or stakeholder with an interest in Australia's cyber workforce, is welcome to respond.

1. **Select at least one Consultation Theme.** Respondents must nominate at least one theme from the list below. Multiple themes may be selected.
2. **Prepare a written response.** Responses should be organised by the selected theme(s). Please limit your response to 500 words per theme.
3. **Submit your response via the Web Form by 5:00 PM AEST on 30 June 2026** found at: cyberpath.acs.org.au/insights.html

4. **(Optional) Register your interest.** Keep up to date on CyberPath activities, events, future consultation rounds, and pilot design.

Please refer to the CyberPath Occupations Framework Discussion Web Form for full terms and conditions, including ACS's Privacy Policy and Data Collection Notice. For questions or additional support, email the CyberPath Program Team at cyberpath@acs.org.au

Table of Consultation Themes (select at least one):

Consultation Themes	Scope of Feedback Sought
1. Framework Scalability, Fit, and Application	Whether the overall occupation/role model and approach reflects how Australian organisations operate — including gaps, mismatches, and potential risks in the proposed design *(refer to Sections 3.2 and 3.3)*. This includes whether the framework appropriately accounts for hybrid or multi-disciplinary roles where practitioners span more than one defined role, as well as how this ontology could be applied to help organisations.
2. Standardised Role Descriptions	CyberPath has proposed a standardised way to build role descriptions *(refer to Section 3.3)* accommodating both industry and custom fields to support their use across a variety of stakeholders and organisations. Are the proposed fields accurate, complete, and feasible for future adoption in industry or your organisation?
3. Functional Domains: Fit, Gaps, and Clarity	Whether the proposed functional domain groupings are intuitive and complete *(refer to Section 4.1)* — including their coverage and representation of cyber work, any overlap or grey areas for clarification, any missing domains, and consideration for sector-specific needs or nuance.
4. MVP CyberPath Roles	Whether the four roles provide a broad enough cross-section of the cyber workforce to pilot and test the CyberPath framework (i.e., technical, governance, operational, leadership). *Refer to Section 4.2*. If not, what should be added or modified to ensure the roles solve a current or emerging workforce capability problem? And are there any barriers or risks that must be considered to support inclusive design.
5. Global Frameworks	CyberPath has gathered insights from a range of global and Australian frameworks *(refer to Appendix B)*, but which frameworks should influence CyberPath as the program moves into Capability Framework development. What framework/s do your organisation currently use? What frameworks should be prioritised to influence design, alignment, and interoperability?
6. Organisation Adoption and Scalability	What organisations need to successfully adopt these pilot roles — including support, resources, incentives, and change management considerations across large orgs, government, critical infrastructure, and SMBs. Identified risks or unintended consequences during the pilot, and how success should be measured.

6.0 Looking Ahead

Competency areas form the next essential layer of the CyberPath occupations framework, sitting between high-level occupational groups and the specific tasks performed within individual roles. Competency Areas do not form part of this Occupations Framework Discussion Paper. They will be covered in the Capability Framework Discussion Paper, however the broad concept is being introduced here as a preamble for the next stage of consultation.

A competency area is a coherent domain of capability, a structured grouping of related knowledge, skills, abilities, behaviours, and attitudes that together describe a core dimension of professional practice, such as Threat Analysis, Risk Management, Secure System Design, or Incident Response. Unlike broad occupational groups (like the CyberPath Domains articulated above), which describe *what type of work* is being carried out, competency areas describe *the specific capabilities* required to perform that work effectively.

They break each occupational group into its underlying capability components, creating a stable, enduring structure that remains relevant even as technologies, tools, and job titles evolve. This middle layer enables a consistent, scalable approach to workforce development: small organisations can combine multiple competency areas into hybrid roles, while large organisations can distribute them across specialised positions. For HR teams, competency areas provide a shared language for mapping skills across roles, identifying gaps, designing development pathways, and supporting mobility.

They also underpin assessment, professional recognition, and education by defining observable behaviours and performance expectations that can be evaluated consistently. Competency areas even support procurement by giving organisations a precise way to articulate the capabilities they need to build internally or source externally.

Take for example the CyberPath Domain of “Security Testing and Assessment”. Under that, there may be a professional role titled “Penetration Tester”. This on its own if established as a professionalised role would not provide enough clarity for an individual to understand their career path, nor would it provide the detail for an employer to understand the capability of prospective talent. For example, a penetration tester could have specialisms in web applications, networks, wireless, or physical testing. These specialisms are what competency areas capture.

Established frameworks such as NIST NICE already use similar constructs in its *Specialty Areas* function as competency domains that anchor curricula, certifications, and workforce planning globally. In this way, competency areas translate high-level occupational structures into actionable capability expectations, forming the building blocks of a coherent, scalable, and future-ready professionalisation framework.

Appendix A – Evaluating OSCA

A.1 Evaluation of Occupation Lists

The 2022 ANZCO release replaced the 2013 version and recognised five cyber security professional occupations (ABS, 2022):

- 262114 Cyber Governance Risk and Compliance Specialist
- 262115 Cyber Security Advice and Assessment Specialist
- 262112 Cyber Security Analyst
- 262113 Cyber Security Architect
- 262116 Cyber Security Operations Coordinator

When OSCA replaced ANZSCO in 2024, it contained a "Cyber Security Professionals" unit group under OSCA category code 2711 (ABS, 2024). This recognised seven cyber security professional occupations which are:

- 271131 Cyber Governance Risk and Compliance Specialist
  Leads the governance, risk and compliance for cyber security.
- 271132 Cyber Security Advice and Assessment Specialist
  Conducts risk and security control assessments, interprets security policies, contributes to the development of standards and guidelines, reviews information system designs, provides guidance on security strategies to manage identified risks, provides specialist advice and explains systems security, strengths and weaknesses.
- 271133 Cyber Security Analyst
  Analyses and assesses vulnerability in infrastructure (software, hardware and networks), investigates available tools and countermeasures to remedy detected vulnerabilities, and recommends solutions and best practices. Analyses and assesses damage to data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions.
- 271134 Cyber Security Architect
  Designs a security system or major components of a security system, and may head a security design team building a new security system.
- 271135 Cyber Security Engineer
  Designs, develops, modifies, documents, tests, implements, installs and supports cyber security software applications and systems to ensure they are fully integrated.
- 271136 Cyber Security Operations Coordinator
  Leads the coordination and response to complex cyber security incidents and

hunt investigations, manages tasks across various teams for incident response and hunt operations, advises leadership on current operational collaborations, contributes toward strategic planning, facilitates incident response engagements, and assesses technical information to develop key messaging.

- 271137 Penetration Tester
  Creates test cases using in-depth technical analysis of risks and typical vulnerabilities, and produces test scripts, materials and packs to test new and existing software or services. Plans, coordinates and conducts cyber threat emulation activities in support of certification, accreditation and operational priorities to verify deficiencies in technical security controls.

A.2 Utility of OSCA for CyberPath

Although OSCA provides a consistent national framework for classifying occupations, it does not yet capture the full breadth and nuance of the cyber security workforce. Cyber roles evolve far more rapidly than traditional occupational taxonomies, and many emerging specialisations, such as threat hunting and OT/ICS security, either do not appear explicitly in OSCA or are grouped under broader ICT categories that fail to reflect their distinct skill sets. Similarly emerging specialisms within cyber around AI and quantum technologies have yet to be defined. This creates a structural lag between how cyber work is performed in practice and how it is represented in official labour market data. As a result, relying solely on OSCA can obscure important differences between cyber roles, limit the visibility of niche or emerging specialisations, and make it harder to design precise competency frameworks or assessment pathways.

For CyberPath, this means OSCA is a necessary but not sufficient foundation. It provides the backbone for alignment with government systems, but it cannot be the only source of occupational definitions. CyberPath must supplement OSCA with more detailed, industry validated role profiles that reflect the real complexity of cyber work. Occupations defined through CyberPath that are industry consulted and validated can then in turn be provided as inputs for future iterations of the OSCA framework.

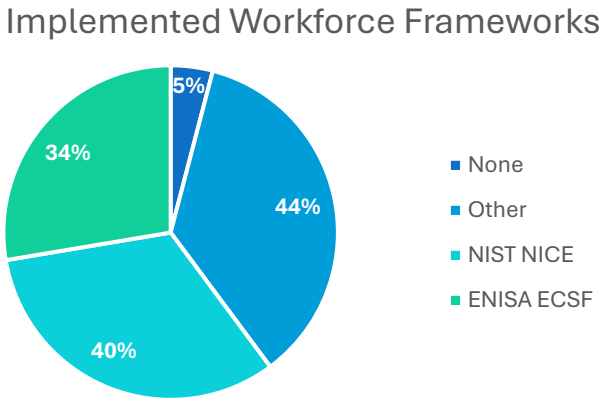
This dual approach ensures the program remains interoperable with national data systems while still being responsive to the dynamic nature of the cyber domain. It also allows the program to recognise new specialisations as they emerge, ensuring that professional standards remain relevant and that practitioners working in cutting-edge areas are not excluded simply because the national classification hasn’t caught up.

Appendix B – Reviewing Workforce Frameworks

Several mature cyber security workforce frameworks already exist with some containing functional domain classifications and some just containing occupations or general role definitions, whereas some go right down to specific occupations. In some cases, these are widely used for workforce planning and mature having been through various iterations allowing them to be leveraged as a reference point for professionalisation.

Some of these frameworks are global frameworks (e.g., SFIA), whereas others are jurisdiction specific. Some are focused on ICT and have embedded cyber security as distinct functional domain, whereas others are cyber specific. For example, Singapore's ICT Skills Framework (developed by SkillsFuture Singapore and IMDA) includes cyber security as a job family with defined roles, skills, and career pathways. Some countries have also opted for taking an established national framework such as NIST NICE, and adopted it for their own unique contexts (e.g., Canada and Saudi Arabia).

In the 2026 Cybersecurity Workforce Research Report, SANS conducted research globally across a sample of 947 respondents. When asking organisations what workforce frameworks the organisations were using to define cyber security role descriptions, many 44% used no recognised framework, 40% used NIST NICE, and 34% used ENISA ECSF:



B.1 NIST NICE Framework

One of the most prominent is the NIST NICE Workforce Framework for Cybersecurity (NICE Framework), maintained by the U.S. National Institute of Standards and Technology. It is published as NIST Special Publication 800-181r1 and defines a common lexicon for describing cybersecurity work across public, private, and academic sectors (NIST, 2020). The framework organises work into 7 high-level *categories*, 33 *Specialty Areas*, and 52 *Work Roles* (depending on version; some updates add or consolidate roles). Each work role is described through task, knowledge, and skill statements. Some work roles share common task, knowledge, and skill statements. Employers, government agencies, training providers, and certification bodies use NICE

as a reference for job design, curriculum development, and workforce planning, and it is increasingly used internationally as a de facto standard for cyber work role definition. The NIST NICE categories, speciality areas, and corresponding work roles are:

Category	Specialty Area	Work Role
Securely Provision (SP)	Software Development (SP-DEV)	SP-DEV-001: Software Developer
	Systems Architecture (SP-ARC)	SP-ARC-001: Enterprise Architect
	Systems Architecture (SP-ARC)	SP-ARC-002: Security Architect
	Systems Requirements Planning (SP-SYS)	SP-SYS-001: Systems Requirements Planner
	Test & Evaluation (SP-TST)	SP-TST-001: Systems Testing & Evaluation Specialist
	Technology R&D (SP-TRD)	SP-TRD-001: Research & Development Specialist
Operate & Maintain (OM)	Customer Service & Technical Support (OM-CST)	OM-CST-001: Technical Support Specialist
	Data Administration (OM-DAT)	OM-DAT-001: Database Administrator
	Knowledge Management (OM-KMG)	OM-KMG-001: Knowledge Manager
	Network Services (OM-NET)	OM-NET-001: Network Operations Specialist
	Systems Administration (OM-ADM)	OM-ADM-001: System Administrator
	Systems Analysis (OM-ANA)	OM-ANA-001: Systems Security Analyst
Oversee & Govern (OV)	Legal Advice & Advocacy (OV-LAW)	OV-LAW-001: Cyber Legal Advisor
	Legal Advice & Advocacy (OV-LAW)	OV-LAW-002: Privacy Officer
	Training, Education & Awareness (OV-TEA)	OV-TEA-001: Cyber Instructor
	Training, Education & Awareness (OV-TEA)	OV-TEA-002: Cyber Workforce Developer
	Training, Education & Awareness (OV-TEA)	OV-TEA-003: Cyber Workforce Analyst
	Cybersecurity Management (OV-MGT)	OV-MGT-001: Program Manager
	Cybersecurity Management (OV-MGT)	OV-MGT-002: IT Project Manager
	Cybersecurity Governance (OV-GOV)	OV-GOV-001: Cyber Policy & Strategy Planner
	Cybersecurity Governance (OV-GOV)	OV-GOV-002: Executive Cyber Leader
	Risk Management (OV-RMG)	OV-RMG-001: Security Control Assessor
	Risk Management (OV-RMG)	OV-RMG-002: Authorizing Official / Designated Representative
	Risk Management (OV-RMG)	OV-RMG-003: Enterprise Risk Manager
Protect & Defend (PR)	Cyber Defense Analysis (PR-CDA)	PR-CDA-001: Cyber Defense Analyst
	Cyber Defense Infrastructure Support (PR-INF)	PR-INF-001: Cyber Defense Infrastructure Support Specialist
	Incident Response (PR-IR)	PR-IR-001: Incident Responder
	Vulnerability Assessment & Management (PR-VAM)	PR-VAM-001: Vulnerability Analyst
Analyze (AN)	Threat Analysis (AN-TA)	AN-TA-001: Threat Analyst
	Exploitation Analysis (AN-EXP)	AN-EXP-001: Exploitation Analyst
	All-Source Analysis (AN-ASA)	AN-ASA-001: All-Source Analyst
	Targets (AN-TGT)	AN-TGT-001: Target Developer
	Targets (AN-TGT)	AN-TGT-002: Target Network Analyst
Collect & Operate (CO)	Collection Operations (CO-OPS)	CO-OPS-001: Collection Operations Specialist
	Cyber Operations (CO-COP)	CO-COP-001: Cyber Operator
	Cyber Operational Planning (CO-PLN)	CO-PLN-001: Cyber Operations Planner
Investigate (IN)	Digital Forensics (IN-FOR)	IN-FOR-001: Digital Forensics Analyst
	Cyber Investigation (IN-INV)	IN-INV-001: Cyber Crime Investigator

NIST also maintains an environmental scan of cybersecurity skills and workforce frameworks, which catalogues many of these approaches and explicitly distinguishes between skill frameworks (collections of skills, roles, and career paths) and workforce frameworks (organised descriptions of work and capabilities) on their website (NIST, 2024). This scan highlights that most mature frameworks converge on a similar pattern: high-level functional domains or job families, within which sit role profiles or work roles, each described by tasks, knowledge, and skills. HR and workforce planning teams use

these structures to create consistent role architectures, identify capability gaps, and design targeted development pathways, while professionalisation schemes use them as the backbone for competency standards and assessment design.

B.2 SFIA

The Skills Framework for the Information Age (SFIA) is a broader digital and ICT skills framework and is maintained by the SFIA Foundation, an international not-for-profit consortium. It includes a dedicated *Information and Cyber Security View* that effectively functions as a set of cyber-related functional domains (SFIA Foundation, 2026). It structures skills into levels of responsibility and capability, and the cyber view maps SFIA skills to NICE work roles, giving organisations a bridge between high-level job families and detailed cyber tasks. The SFIA 9 information and cyber security view has been reproduced in the table below, noting that the skills captured under each category are not cyber security specific skills, and instead contain broader digital skills that can be applied in cyber roles, or contain a cyber descriptor in their responsibilities:

Category	Relevant SFIA 9 Skills
Cybersecurity strategy and leadership	Strategic planning ITSP
	Information security SCTY
	Demand management DEMM
	Stakeholder relationship management RLMT
Cybersecurity architecture	Requirements definition and management REQM
	Enterprise and business architecture STPL
	Solution architecture ARCH
	Data management DATM
Cybersecurity research and intelligence	Research RSCH
	Vulnerability research VURE
	Threat intelligence THIN
Cybersecurity governance, risk and compliance	Governance GOVN
	Risk management BURM
	Audit AUDT
	Personal data protection PEDP
	Information management IRMG
	Information assurance INAS
	Quality management QUMG
	Measurement MEAS
Cybersecurity advice and guidance	Consultancy CNSL
	Specialist advice TECH
Secure software and systems development	Systems development management DLMG
	Systems and software life cycle engineering SLEN
	Systems design DESN
	Software design SWDN
	Network design NTDS
	Hardware design HWDE
	Programming/software development PROG
	Systems integration and build SINT
	Testing TEST
	Real-time/embedded systems development RESD
	Penetration testing PENT
Cybersecurity change programmes	Programme management PGMG
	Project management PRMG
Secure supply chain	Sourcing SORC
	Supplier management SUPP

Secure infrastructure management	Technology service management ITMG
	IT infrastructure ITOP
	Network support NTAS
	Database administration DBAD
	Release and deployment RELM
	Storage management STMG
Cybersecurity resilience	Security operations SCAD
	Continuity management COPL
	Incident management USUP
	Change control CHMG
	Asset management ASMG
	Vulnerability assessment VUAS
	Digital forensics DGFS
Cybersecurity talent management	Performance management PEMT
	Employee experience EEXP
	Professional development PDSV
	Workforce planning WFPL
	Resourcing RESC
Cybersecurity education and training	Knowledge management KNOW
	Learning and development management ETMG
	Certification scheme operation CSOP
	Teaching TEAC
	Subject formation SUBF

Both NIST NICE and SFIA are commonly used by HR teams, CISOs, and learning and development functions to align role profiles, career paths, and learning curriculum. There is also mapping available between SFIA's skills framework and NICE's cyber-specific work roles. In practice, this mapping looks like a matrix where SFIA skills (e.g., information security, penetration testing, incident management) can be cross-referenced against NICE work roles, enabling integrated workforce planning across both ICT and cyber, creating internal mobility pathways.

B.3 UK CSC Framework

UK has used the NICE Framework and related work to inform the UK Cyber Security Council's (UK CSC) *specialisms* and *professional titles*. It is worth pointing out that these specialisms can be viewed as occupation groupings as many will incorporate many individual occupations. The specialisms include:

B.4 ASD Cyber Skills Framework

In 2009, the ASD adopted an internal cyber capabilities framework known as the *ASD Streams*. ASD Streams defined specialist professional capabilities in a broad occupational group related to a particular skill area (ASD, 2020).

The 2016 Defence White Paper (Defence, 2016) outlined the need for an additional 800 cyber practitioners to combat increased threats and intrusions in the cyber domain. To meet this increased demand, practitioners and recruiters alike required a framework to understand the skills that are necessary to perform the roles and duties of the cyber mission.

A review of the ASD Streams in 2018 assessed the relevance of the defined roles, capabilities, skills and proficiency levels, and the way in which these related to current industry and government frameworks and standards. As a result, the *ASD Cyber Skills Framework* was formed: nine roles were defined using a set of underlying core capabilities and related skills and proficiency levels.

The ASD released the ASD Cyber Skills Framework v.1.0 in July 2019 as an iterative framework designed to be used as a tool to assess, maintain and monitor the skills, knowledge and attributes of the ASD cyber workforce.

A second iteration of the ASD Cyber Skills Framework was released in 2020 which captured updates from the frameworks that support it; the Skills Framework for the Information Age 7 (SFIA 7), the Chartered Institute for Information Security (CIISec) Framework v.2.4 and the APS Integrated Leadership System (ILS).

For background context in how the framework came together:

- CIISec is the leading information security professional industry body in the United Kingdom. ASD uses the CIISec Skills Framework to define most cyber capabilities and skills within the ASD Cyber Skills Framework. The CIISec Skills Framework was also essential in establishing the skill proficiency levels adopted in the ASD Cyber Skills Framework.
- The ASD, along with many other government departments and ICT industry stakeholders, implements SFIA as a tool to assess technical ICT proficiencies. This was chosen because of SFIA's recognition as a leading framework to describe capabilities and skill proficiencies for information technology professionals. SFIA is used to define several core ICT capabilities and skills within the ASD Cyber Skills Framework.
- The ILS is the Australian government-approved standard for personnel capability development. The ILS is adopted for all skills relating to the management, leadership, business, and communication capability within the ASD Cyber Skills Framework. (APSC, 2021)

The ASD Cyber Skills Framework focuses on the capabilities, skills and levels of nine cyber roles which have been grouped under four functional groupings:

Disciplines	ASD Roles	Expectations
CYBER SECURITY ANALYSIS	**CYBER THREAT ANALYST** A Cyber Threat Analyst performs cyber security research, analysis, and strategic threat assessments. A Cyber Threat Analyst undertakes detailed cyber event analysis, intelligence assessments, and professional and policy advice for identified cyber threats.	• Prepare and deliver briefs and cyber threat intelligence reports • Identify and undertake complex research and analysis of relevant cyber threat actors • Provide situational awareness on current and emerging threats • Analyse identified cyber threat event data and fuse with all-source intelligence • Understand and use analytical tools and techniques
	INTRUSION ANALYST An Intrusion Analyst plans, coordinates and conducts proactive cyber threat discovery activities to identify potential intrusion or anomalous behaviour based on cyber threat intelligence. An Intrusion Analyst assesses and evaluates cyber threat intelligence for indicators of compromise, and provides detailed planning, analysis and reporting on current and emerging threats to information systems.	• Plan, coordinate and conduct network and system activity • Understand and apply cyber threat models • Assess and evaluate cyber threat intelligence • Communicate technical findings and recommendations • Design and develop complex technical and procedural systems
	MALWARE ANALYST A Malware Analyst analyses the functionality, origin and potential impacts of malware, through reverse-engineering, development and research of design systems and software components, to defend networks against malicious threats.	• Analyse the functionality, origin and potential impacts of malware • Provide detailed and specific advice regarding the application of malware analysis • Contribute to incident response and digital forensic investigations • Communicate technical findings and recommendations

Disciplines	ASD Roles	Expectations
		• Design, code, verify, test, document, amend and refactor complex programs, scripts and integration software services • Design system and software components using appropriate modelling techniques
CYBER SECURITY OPERATIONS	**INCIDENT RESPONSE** An Incident Responder performs analysis and investigations of cyber security incidents, often malicious, to remediate networks and provide mitigation advice to protect and secure systems.	• Investigate information and cyber security incidents • Analyse and resolve identified security incidents • Contribute to digital forensic investigations • Communicate technical findings and recommendations • Provide assistance with the development of technical remediation plan
	OPERATIONS COORDINATOR An Operations Coordinator manages tasks associated with cyber security incidents across various teams for incident response and hunt operations, including setting priorities and engaging with customers. An Operations Coordinator provides detailed technical advice and contributes to policy development, strategic planning, and program and project management.	• Lead the coordination, governance and response to complex cyber security incidents and hunt investigations • Manage tasks across various teams for incident response and hunt operations • Advise leadership on current operational collaborations and contribute toward strategic planning • Facilitiate incident response engagements • Assess technical information to develop key messaging
CYBER SECURITY ARCHITECTURE	**CYBER SECURITY ADVICE AND ASSESSMENT** A Cyber Security Advice and Assessment (Blue Team) role performs cyber and information security risk assessments and provides detailed technical, professional and policy advice and guidance on the application and operation of procedural security controls.	• Conduct risk and security control assessments • Interpret security policy and contribute to the development of standards and guidelines • Review information system designs • Provide guidance on security strategies to manage identified risks • Provide specialist advice • Explain systems security and the strengths and weaknesses
	VULNERABILITY RESEARCHER A Vulnerability Researcher plans, coordinates and conducts cyber vulnerability research activities to identify deficiencies and impacts on systems and emerging technologies, develop proof of concept exploits, and support certification, accreditation and operational priorities.	• Plan and coordinate vulnerability research assessments • Conduct cyber research activities in order to identify deficiencies and impact on systems • Conduct complex applied research • Identify and evaluate alternative design options • Design, code, verify, test, document, amend and refactor complex programs/scripts and integration software services • Communicate technical findings and recommendations
CYBER SECURITY TESTING	**PENETRATION TESTER** A Penetration Tester (Red Team) performs cyber security exploitation, penetration testing and red team activities. A Penetration Tester creates test cases using in-depth technical analysis of risks and typical vulnerabilities and produce test scripts, materials and packs to test new and existing software or services. A Penetration Tester plans, coordinates and conducts cyber threat emulation activities in support of certification,	• Plan, coordinate and conduct cyber threat emulation activities • Provide complex technical advice, recommendations and consultancy • Communicate technical findings and recommendations • Create test cases using in-depth technical analysis of risks and typical vulnerabilities • Assess cyber threat intelligence and interpret threat reporting

Disciplines	ASD Roles	Expectations
	accreditation, and operational priorities to verify deficiencies in technical security controls. A Penetration Tester provides remediation, technical advice, recommendations and consultancy on networks, infrastructure, products and services supplied to system owners.	
	VULNERABILITY ASSESSOR A Vulnerability Assessor performs technical security investigations on a wide array of assets and devices that directly relate to security infrastructure. A Vulnerability Assessor evaluates and assists with the application and compliance of security controls, reviews information systems for actual or potential security vulnerabilities, and explains threat profiles of a variety of electronic devices. A Vulnerability Assessor contributes to the development of systems design policies and standards, and selection of architecture components.	• Perform complex security investigations • Assess and explain threat profiles for a variety of electronic devices • Evaluate and assist with the application and compliance of security controls • Review information systems for actual or potential security vulnerabilities • Design, code, verify, test, document, amend and refactor complex programs, scripts and integration software services

The biggest limitation of the ASD Cyber Skills Framework is that it has not been publicly updated since the 2020 version 2.0 release, and it was designed specifically to reflect the workforce needs of ASD, and not necessarily reflective of the broader set of work role requirements across the entire sector.

B.5 SCyWF

As another comparative example, in developing the Saudi Cybersecurity Workforce Framework (SCyWF), the Kingdom of Saudi Arabia adopted a similar approach to NIST NICE, defining a three-tier model that includes functional grouping at a category level, speciality area level, and finally, the job roles. Each layer has a letter/number grouping that allows codification down to the job level. This is like the codification used for NIST NICE and makes it easier to reference parts of the framework. For example:

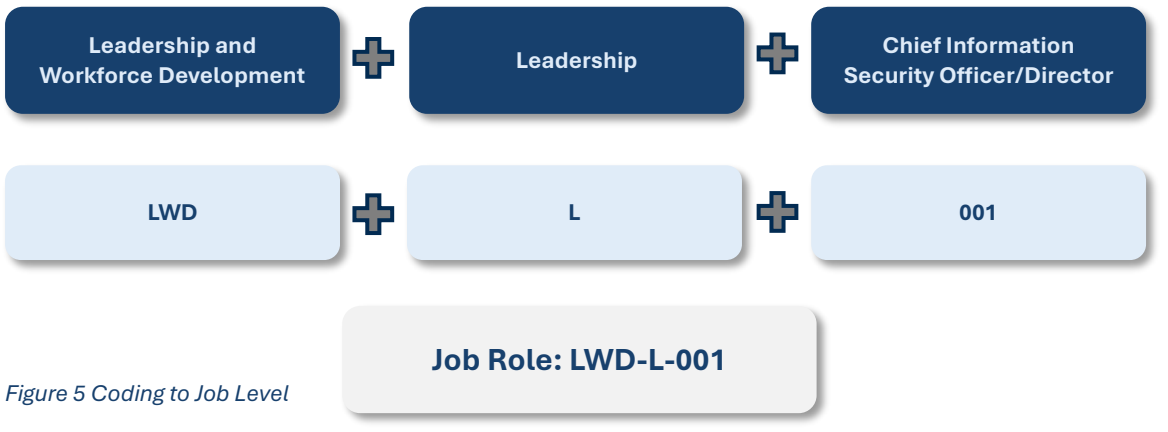


Figure 5 Coding to Job Level

The full SCyWF framework follows:

Category	Specialty	Job Roles
Cybersecurity Architecture, Research and Development Conducts cybersecurity design, architecture, research and development activities.	**Cybersecurity Architecture** Designs and oversees the development and implementation of cybersecurity systems and/or the cybersecurity components of IT systems and networks.	**Cybersecurity Architect** Designs and oversees the development, implementation and configuration of cybersecurity systems and networks.
		Secure Cloud Specialist Designs, implements and operates secure cloud computing systems and develops secure cloud policies.
	Cybersecurity Research and Development Conducts cybersecurity research and development.	**Systems Security Development Specialist** Designs, develops, tests and evaluates security of information systems throughout the development life-cycle.
		Cybersecurity Developer Develops cybersecurity software, applications, systems and products.
		Secure Software Assessor Assesses the security of computer applications, software, code or programs and provides actionable results.
		Cybersecurity Researcher Conducts scientific research in the cybersecurity field.
		Cybersecurity Data Science Specialist 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.
		Cybersecurity Artificial Intelligence Specialist 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.
Leadership and Workforce Development Leads cybersecurity teams and work. Develops cybersecurity human capital.	**Leadership** Supervises, manages and leads cybersecurity teams and work.	**Chief Information Security Officer/Director** Directs cybersecurity work within an organization, establishes vision and direction for its cybersecurity and related strategies, resources and activities and advises the leadership on the effective management of the organization's cyber risks.
		Cybersecurity Manager Manages the security of information systems and functions within an organization. Leads a cybersecurity team, unit and/or enterprise level function.
		Cybersecurity Advisor Provides expert consultancy and advice on cybersecurity topics to an organization's leadership and to its cybersecurity leadership and teams.
	Workforce Development Applies knowledge and skills of cybersecurity, human resources development and teaching methodologies to develop, manage, retain and	**Cybersecurity Human Capital Manager** Develops plans, strategies and guidance within an organization to support the development and management of the cybersecurity workforce.
		Cybersecurity Instructional Curriculum Developer Develops, plans, coordinates and evaluates

Category	Specialty	Job Roles
	improve the skills of the cybersecurity workforce.	cybersecurity training and education programs, courses, contents, methods and techniques based on instructional needs.
		Cybersecurity Instructor Teaches, trains, develops and tests people in cybersecurity topics.
Governance, Risk, Compliance and Laws Develops organizational cybersecurity policies. Governs cybersecurity structures and processes, manages cyber risks and assures compliance with the organization's cybersecurity, risk management and related legal requirements.	**Governance, Risk and Compliance** Governs cybersecurity structures and processes. Manages cyber risks and assures IT systems against the organization's cybersecurity and risk management requirements. Develops and updates the organization's cybersecurity policies.	**Cybersecurity Risk Officer** Identifies, assesses and manages an organization's cybersecurity risks to protect its information and technology assets in line with organizational policies and procedures and related laws and regulations.
		Cybersecurity Compliance Officer Ensures an organization's cybersecurity program complies with applicable requirements, policies and standards.
		Cybersecurity Policy Officer Develops, updates and maintains cybersecurity policies to support and align with an organization's cybersecurity requirements.
		Security Controls Assessor Analyzes cybersecurity controls and assesses their effectiveness.
		Cybersecurity Auditor Designs, performs and manages cybersecurity audits to assess an organization's compliance with applicable requirements, policies, standards and controls. Prepares audit reports and communicates them to authorized parties.
	Laws and Data Protection Ensures the organization complies with cybersecurity and data protection laws and regulations.	**Cybersecurity Legal Specialist** Provides legal services on topics related to cyber laws and regulations.
		Privacy/Data Protection Officer Studies personal data schemes and the applicable privacy laws and regulations. Analyzes privacy risks. Develops and oversees the implementation of an organization's privacy and data protection compliance program and internal policies. Supports organizational response to a privacy or data protection incident.
Protection and Defense Identifies, analyzes, monitors, mitigates and manages threats and vulnerabilities to IT systems and networks. Uses defensive measures and multi-source information to report events and respond to incidents.	**Defense** Uses monitoring and analysis tools to identify and analyze events and to detect incidents.	**Cybersecurity Defense Analyst** Uses data collected from cyber defense tools to analyze events that occur within their organization to detect and mitigate cyber threats.
		Cybersecurity Infrastructure Specialist Tests, implements, deploys, maintains and administers hardware and software that protect and defend systems and networks against cybersecurity threats.
		Cybersecurity Specialist Provides general cybersecurity support. Assists in cybersecurity tasks.
	Protection Uses cybersecurity tools to protect information, systems and networks from cyber threats.	**Cryptography Specialist** Develops, evaluates, analyzes and identifies weaknesses of, and improvements to, cryptography systems and algorithms.
		Identity and Access Management Specialist Manages individuals and entities identities and access to resources through applying

Category	Specialty	Job Roles
		identification, authentication and authorization systems and processes.
		Systems Security Analyst Develops, tests and maintains systems' security. Analyzes security of operations and integrated systems.
	Vulnerability Assessment Tests IT systems and networks and assesses their threats and vulnerabilities.	**Vulnerability Assessment Specialist** 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.
		Penetration Tester/Red Team Specialist Conducts authorized attempts to penetrate computer systems or networks and physical premises, using realistic threat techniques, to evaluate their security and detect potential vulnerabilities.
	Incident Response Investigates, analyzes and responds to cyber incidents.	**Cybersecurity Incident Responder** Investigates, analyzes and responds to cybersecurity incidents.
		Digital Forensics Specialist Collects and analyzes digital evidence, investigates cybersecurity incidents to derive useful information to mitigate system and network vulnerabilities.
		Cyber Crime Investigator Identifies, collects, examines and preserves evidence using controlled and documented analytical and investigative techniques.
	Threat Management Collects and analyzes information about threats, searches for undetected threats and provides actionable insights to support cybersecurity decision-making.	**Threat Intelligence Analyst** Collects and analyzes information about threats and provides actionable insights to support cybersecurity decision-making.
		Threat Hunter Searches proactively for undetected threats within the organization's environment and provides insights to support cybersecurity decision-making.
Industrial Control Systems and Operational Technologies Conducts cybersecurity tasks for Industrial Control Systems and Operational Technologies (ICS/OT).	**Industrial Control Systems and Operational Technologies** Performs work related to cybersecurity governance, risk management and compliance; design and development; operations and administration; protection and defense for OT systems such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.	**ICS/OT Cybersecurity Architect** Designs and oversees cybersecurity architecture for ICS/OT environments including SCADA systems.
		ICS/OT Cybersecurity Infrastructure Specialist Implements and administers cybersecurity infrastructure protecting ICS/OT systems.
		ICS/OT Cybersecurity Defense Analyst Monitors and analyzes events within ICS/OT environments to detect incidents.
		ICS/OT Cybersecurity Risk Officer Identifies, assesses and manages cybersecurity risks specific to ICS/OT systems.
		ICS/OT Cybersecurity Incident Responder Investigates, analyzes and responds to cyber incidents affecting ICS/OT environments.

B.6 ENISA ECSF

In Europe on the other hand, the European Cybersecurity Skills Framework (ECSF), developed under the auspices of ENISA (the European Union Agency for Cybersecurity), provides a structured set of role definitions. ENISA maintains and updates the ECSF in consultation with EU member states, industry, and academia. It does not use functional groupings or domains. Instead, the ECSF is built around role profiles, not domains.

These profiles represent the core functional areas of cybersecurity work across Europe. Each profile includes detailed tasks, competences, skills, and knowledge areas. The profiles also contain alternative titles which suggests depending on the context, there is flexibility of the role definition. ECSF is used by European governments, education providers, and employers to harmonise cyber role definitions, support curriculum design, and inform national skills strategies.

The core components of the ECSF professional roles definition include:

ECSF Cyber Professional Roles	Alternative Title(s)	Summary statement	Mission	Deliverables(s)
Chief Information Security Officer (CISO)	• Chief Information Security Officer (CISO) • Cybersecurity Programme Director • Head of Information Security • Information Security Manager • Information Security Officer (ISO) • IT/ICT Security Officer	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.	• Cybersecurity Policy • Cybersecurity Strategy
Cyber Incident Responder	• Cyber Crisis Expert • Cyber Fighter /Defender • Cyber Incident Handler • Cyber Incident Responder • Cybersecurity SIEM Manager • Incident Response Engineer • Security Operation Analyst (SOC Analyst) • Security Operations Center (SOC) Analyst	Monitor the organisation's cybersecurity state, handle incidents during cyber-attacks and assure the continued operations of ICT systems.	Monitors and assesses systems' cybersecurity state. Analyses, evaluates and mitigates the impact of cybersecurity incidents. Identifies cyber incidents root causes and malicious actors. According to the organisation's Incident Response Plan, restores systems' and processes' functionalities to an operational state, collecting evidences and documenting actions taken.	• Cyber Incident Report • Incident Response Plan
Cyber Legal, Policy & Compliance Officer	• Cyber Law Consultant • Cyber Legal Advisor • Cyber Legal, Policy & Compliance Officer • Cybersecurity Legal Officer • Data Compliance Officer • Data Protection Officer (DPO) • Governance Risk Compliance (GRC) Consultant • Information Governance Officer • IT/ICT Compliance Manager • Privacy Protection Officer	Manages compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organisation's strategy and legal requirements.	Oversees and assures compliance with cybersecurity- and data-related legal, regulatory frameworks and policies in line with the organisation's strategy and legal requirements. Contributes to the organisation's data protection related actions. Provides legal advice in the development of the organisation's cybersecurity governance processes and recommended remediation strategies/solutions to ensure compliance.	• Compliance Manual • Compliance Report
Cyber Threat Intelligence Specialist	• Cyber Intelligence Analyst • Cyber Threat Intelligence Specialist • Cyber Threat Modeller	Collect, process, analyse data and information to produce actionable intelligence reports and disseminate them to target stakeholders.	Manages cyber threat intelligence life cycle including cyber threat information collection, analysis and production of actionable intelligence and dissemination to security stakeholders and the CTI community, at a tactical, operational and strategic level. Identifies and monitors the Tactics, Techniques and Procedures	• Cyber Threat Intelligence Manual • Cyber Threat Report

ECSF Cyber Professional Roles	Alternative Title(s)	Summary statement	Mission	Deliverables(s)
			(TTPs) used by cyber threat actors and their trends, track threat actors' activities and observe how non-cyber events can influence cyber-related actions.	
Cybersecurity Architect	• Cybersecurity Architect • Cybersecurity Designer • Cybersecurity Solutions Architect • Data Security Architect	Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls.	Designs solutions based on security-by-design and privacy-by-design principles. Creates and continuously improves architectural models and develops appropriate architectural documentation and specifications. Coordinate secure development, integration and maintenance of cybersecurity components in line with standards and other related requirements.	• Cybersecurity Architecture Diagram • Cybersecurity Requirements Report
Cybersecurity Auditor	• Cybersecurity Audit Manager • Cybersecurity Auditor • Cybersecurity Procedures and Processes Auditor • Data Protection Assessment Analyst • Governance Risk Compliance (GRC) Auditor • Information Security Auditor (IT or Legal Auditor) • Information Security Risk and Compliance Auditor	Perform cybersecurity audits on the organisation's ecosystem. Ensuring compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices.	Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organisation's legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations.	• Cybersecurity Audit Plan • Cybersecurity Audit Report
Cybersecurity Educator	• Cybersecurity Awareness Specialist • Cybersecurity Educator • Cybersecurity Trainer • Faculty in Cybersecurity (Professor, Lecturer)	Improves cybersecurity knowledge, skills and competencies of humans.	Designs, develops and conducts awareness, training and educational programmes in cybersecurity and data protection-related topics. Uses appropriate teaching and training methods, techniques and instruments to communicate and enhance the cybersecurity culture, capabilities, knowledge and skills of human resources. Promotes the importance of cybersecurity and consolidates it into the organisation.	• Cybersecurity Awareness Program • Cybersecurity Training Material
Cybersecurity Implementer	• Cybersecurity Developer	Develop, deploy and operate	Provides cybersecurity-related technical development,	• Cybersecurity Solutions

ECSF Cyber Professional Roles	Alternative Title(s)	Summary statement	Mission	Deliverables(s)
	• Cybersecurity Engineer • Cybersecurity Implementer • Cybersecurity Solutions Expert • Development, Security & Operations (DevSecOps) Engineer • Information Security Implementer	cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products.	integration, testing, implementation, operation, maintenance, monitoring and support of cybersecurity solutions. Ensures adherence to specifications and conformance requirements, assures sound performance and resolves technical issues required in the organisation's cybersecurity-related solutions (systems, assets, software, controls and services), infrastructures and products.	
Cybersecurity Researcher	• Chief Research Officer (CRO) in cybersecurity • Cybersecurity Research Engineer • Cybersecurity Researcher • Research and Development (R&D) Officer in cybersecurity • Research and Innovation Officer/Expert in cybersecurity • Research Fellow in cybersecurity • Scientific Staff in cybersecurity • Senior Research Officer in cybersecurity	Research the cybersecurity domain and incorporate results in cybersecurity solutions.	Conducts fundamental/basic and applied research and facilitates innovation in the cybersecurity domain through cooperation with other stakeholders. Analyses trends and scientific findings in cybersecurity.	• Publication in Cybersecurity
Cybersecurity Risk Manager	• Cyber Risk Manager • Cybersecurity Impact Analyst • Cybersecurity Risk Assessor • Cybersecurity Risk Assurance Consultant • Cybersecurity Risk Manager • Information Security Risk Analyst	Manage the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports.	Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls.	• Cybersecurity Risk Assessment Report • Cybersecurity Risk Remediation Action Plan

ECSF Cyber Professional Roles	Alternative Title(s)	Summary statement	Mission	Deliverables(s)
Digital Forensics Investigator	• Computer Forensics Consultant • Cybersecurity & Forensic Specialist • Digital Forensics Analyst • Digital Forensics Investigator	Ensure the cybercriminal investigation reveals all digital evidence to prove the malicious activity.	Connects artefacts to natural persons, captures, recovers, identifies and preserves data, including manifestations, inputs, outputs and processes of digital systems under investigation. Provides analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion. Presents an unbiased qualitative view without interpreting the resultant findings.	• Digital Forensics Analysis Results • Electronic Evidence
Penetration Tester	• Cybersecurity Tester • Defensive Cybersecurity Expert • Ethical Hacker • Offensive Cybersecurity Expert • Penetration Tester • Pentester • Red Team Expert • Red Teamer • Vulnerability Analyst	Assess the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.	Plans, designs, implements and executes penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures. Identifies vulnerabilities or failures on technical and organisational controls that affect the confidentiality, integrity and availability of ICT products (e.g. systems, hardware, software and services).	• Penetration Testing Report • Vulnerability Assessment Results Report

These frameworks are typically maintained by government skills agencies or national professional bodies and are used by HR teams, workforce planners, and education providers to align job families, qualifications, learning, and progression routes. Structurally, they tend to present cyber as one or more job families within a broader ICT or digital workforce architecture, with each family broken into roles, skills, and proficiency levels.

B.7 Other Frameworks Considered

The Chartered Institute of Information Security (CIISec) Skills Framework is a widely adopted, competency-based model that defines the knowledge, skills, and behaviours required of cyber and information security professionals. It is considered an industry standard for assessing capability, structuring career development, and aligning roles across the security profession.

CIISec created the framework to provide a structured, evidence-based way to measure and develop professional competence in information security. First released in 2006

and updated regularly (most recently as v2.4 in 2024), it is built through collaboration with public and private sector organisations, academics, and security leaders. Although the CIISec Framework was utilised as a foundation for establishing skills and proficiencies in the ASD Cyber Skills Framework, the CIISec Framework is not openly licensed and is positioned as a commercial, proprietary standard with legal protections.

At its core, the CIISec Framework:

- Defines a full spectrum of categories for skill areas
- Specifies skill levels that describe increasing proficiency and responsibility
- Focuses on practical capability, not just theoretical knowledge
- Includes mandatory and essential skills for all security professionals
- Underpins the CIISec Capability Development Methodology (CDM) used for organisational maturity and workforce planning

Although considered and mapping work has been undertaken, the CIISec Framework hasn't been reproduced within this discussion paper as it is a proprietary and commercial offering.

Appendix C – Mapping Domains to Frameworks

C.1 Mapping to NIST NICE

The functional domains proposed for CyberPath's Occupations Framework can be mapped to NIST NICE using a "best fit" approach to create a common language for organisations that have already invested into using NIST NICE, or for international harmonisation efforts of workforce frameworks. Going through this process ensures not only that there is a common language, but also that there are no gaps in the proposed structure for CyberPath as an end-to-end solution design. Indicative mapping is:

CyberPath Domain	Categories	Specialty Areas	Work Roles
Governance, Risk, Compliance & Policy	• Oversee & Govern (OV)	• Cybersecurity Governance (OVGOV) • Risk Management (OVRMG) • Legal Advice & Advocacy (OVLAW) • Training, Education & Awareness (OVTEA)	• Cyber Policy & Strategy Planner (OVGOV001) • Executive Cyber Leader (OVGOV002) • Security Control Assessor (OVRMG001) • Enterprise Risk Manager (OVRMG003) • Authorizing Official / Designated Representative (OVRMG002) • Cyber Legal Advisor (OVLAW001) • Privacy Officer (OVLAW002)
Secure Systems Architecture and Design	• Securely Provision (SP)	• Systems Architecture (SPARC) • Systems Requirements Planning (SPSYS) • Technology R&D (SPTRD)	• Security Architect (SPARC002) • Enterprise Architect (SPARC001) • Systems Requirements Planner (SPSYS001) • Research & Development Specialist (SPTRD001)

CyberPath Domain	Categories	Specialty Areas	Work Roles
Cyber Defence	• Protect & Defend (PR) • Operate & Maintain (OM)	• Cyber Defense Analysis (PRCDA) Cyber Defense Infrastructure Support (PRINF) • Incident Response (PRIR) • Vulnerability Assessment & Management (PRVAM) Network Services (OMNET) • Systems Administration (OMADM) • Systems Analysis (OMANA)	• Cyber Defense Analyst (PRCDA001) • Cyber Defense Infrastructure Support Specialist (PRINF001) • Incident Responder (PRIR001) • Vulnerability Analyst (PRVAM001) • Network Operations Specialist (OMNET001) • System Administrator (OMADM001) • Systems Security Analyst (OMANA001)
Threat Intelligence Research & Analysis	• Analyze (AN) • Collect & Operate (CO)	• Threat Analysis (ANTA) • All-Source Analysis (ANASA) • Exploitation Analysis (ANEXP) • Targets (ANTGT) • Collection Operations (COOPS)	• Threat Analyst (ANTA001) • All-Source Analyst (ANASA001) • Exploitation Analyst (ANEXP001) • Target Developer (ANTGT001) • Target Network Analyst (ANTGT002) • Collection Operations Specialist (COOPS001)
Security Testing and Assessment	• Protect & Defend (PR) • Securely Provision (SP)	• Vulnerability Assessment & Management (PRVAM) • Test & Evaluation (SPTST)	• Vulnerability Analyst (PRVAM001) • Systems Testing & Evaluation Specialist (SPTST001) • Penetration Tester (mapped via PRVAM/PRIR)
Identity, Access & Trust Services	• Securely Provision (SP) • Operate & Maintain (OM) • Protect & Defend (PR)	• Systems Administration (OMADM) • Network Services (OMNET) • Cyber Defense Infrastructure Support (PRINF)	• System Administrator (OMADM001) • Network Operations Specialist (OMNET001) • Cyber Defense Infrastructure Support Specialist (PRINF001)
Secure Systems Development and Operation	• Securely Provision (SP) • Operate & Maintain (OM)	• Software Development (SPDEV) • Systems Administration (OMADM) • Network Services (OMNET) • Knowledge Management (OMKMG)	• Software Developer (SPDEV001) • System Administrator (OMADM001) • Network Operations Specialist (OMNET001) Knowledge Manager (OMKMG001)
Secure Application Development	• Securely Provision (SP)	• Software Development (SPDEV) • Technology R&D (SPTRD)	• Software Developer (SPDEV001) • Research & Development Specialist (SPTRD001)
Education, Training, Awareness & Workforce Development	• Oversee & Govern (OV)	• Training, Education & Awareness (OVTEA)	• Cyber Instructor (OVTEA001) • Cyber Workforce Developer (OVTEA002) • Cyber Workforce Analyst (OVTEA003)
Cyber Security Leadership, Strategy, Consulting & Management	• Oversee & Govern (OV)	• Cybersecurity Management (OVMGT) • Cybersecurity Governance (OVGOV) • Risk Management (OVRMG) • Legal Advice & Advocacy (OVLAW)	• Program Manager (OVMGT001) • IT Project Manager (OVMGT002) • Executive Cyber Leader (OVGOV002) • Cyber Policy & Strategy Planner (OVGOV001) • Enterprise Risk Manager (OVRMG003) • Cyber Legal Advisor (OVLAW001)

C.2 Mapping to Other Frameworks

Similar to the NIST NICE mapping exercise, the CyberPath functional domains can be "best efforts" mapped to equivalents across the other frameworks. An indicative translation between frameworks is:

CyberPath Domains	CIISec Main Areas	UK CSC Specialisms	ENISA ECSF Roles	SCYWF Domains and Roles
Governance, Risk, Compliance & Policy	• Strategy & Governance, Risk Management • Compliance, Policy & Standards	• Cyber Governance & Risk Management • Cyber Audit & Assurance • Cyber Policy	• Information Security Manager • Cybersecurity Auditor • Cyber Legal & Policy Expert • Data Protection Officer	• Governance & Management domain: Cyber Governance Lead, Risk & Compliance Specialist, Policy & Standards Manager
Secure Systems Architecture and Design	• Security Architecture, Technical Security • Secure Design	• Secure System Architecture & Design • Secure Infrastructure Specialist	• Cybersecurity Architect • Security Engineer • Secure Infrastructure Specialist	• Architecture & Engineering domain: Cyber Security Architect, Secure Infrastructure Engineer
Cyber Defence	• Incident Management • Operations & Monitoring • Network Security	• Cyber Security Operations • Incident Response • SOC Analyst	• Cyber Incident Responder • Cyber Defence Operator • SOC Analyst • Cybersecurity Operator	• Defence & Operations domain: SOC Analyst, Cyber Defence Analyst, Incident Responder
Threat Intelligence Research & Analysis	• Threat Intelligence, Research & Analysis • Situational Awareness	• Cyber Threat Intelligence • Cyber Research & Analysis	• Cyber Threat Intelligence Specialist • Cyber Threat Analyst • Cybersecurity Researcher	• Intelligence & Analysis domain: Threat Intelligence Analyst, Cyber Researcher
Security Testing and Assessment	• Security Testing • Technical Assessment • Assurance & Audit	• Cyber Security Testing • Penetration Testing • Assurance & Audit	• Penetration Tester • Cybersecurity Auditor • Vulnerability Assessor	• Testing & Assurance domain: Penetration Tester, Vulnerability Assessor, Security Assessor
Identity, Access & Trust Services	• Identity & Access Management • Access Control • Authentication	• Identity & Access Management • Digital Trust & Identity	• Identity & Access Management Specialist • Access Control Administrator	• Identity & Access domain: IAM Specialist, Access Management Engineer, Trust Services Lead
Secure Systems Development and Operation	• Secure Systems Engineering • Secure Operations	• Secure Operations • Secure Platform Engineering	• Secure Systems Engineer	• Development & Operations domain: Secure Systems

CyberPath Domains	CIISec Main Areas	UK CSC Specialisms	ENISA ECSF Roles	SCYWF Domains and Roles
	• Configuration & Change	• DevSecOps	• Cybersecurity Operations Specialist • DevSecOps Engineer	Engineer, DevSecOps / SecOps Engineer
Secure Application Development	• Secure Application Development • Secure Coding • Application Security	• Application Security • Secure Software Engineering	• Application Security Specialist • Secure Software Developer	• Applications & Products domain: Secure Application Developer, Application Security Engineer
Education, Training, Awareness & Workforce Development	• Education & Training • Awareness & Culture	• Cyber Security Education & Training • Awareness & Culture	• Cybersecurity Trainer • Cybersecurity Awareness Specialist	• Workforce & Culture domain: Cyber Trainer, Awareness & Culture Lead
Cyber Security Leadership, Strategy, Consulting, and Management	• Management, Leadership, Business and Communications	• Cyber Security Management • Cyber Leadership • Cyber Consultancy	• Chief Information Security Officer (CISO) • Cybersecurity Manager • Cybersecurity Consultant	• Governance & Leadership domain: CISO, Cyber Programme Manager, Cyber Strategy Consultant

Appendix D – Future Role Candidates

Once CyberPath pilot roles have been tested and accepted by industry and the broader CyberPath framework has been proven, potential candidates for the next iteration are below:

1. Cloud Security Engineer

The Australian Cyber Workforce Playbook highlights cloud security as one of the most in-demand and fastest-growing skill areas across both government and industry. As organisations accelerate cloud adoption and increasingly across multiple providers, there is a critical need for practitioners who can design, implement, and maintain secure cloud environments. This role sees:

- **High national demand:** Cloud security is consistently listed as a top-priority capability area in the Playbook, driven by rapid migration to cloud-native architectures.
- **Skills shortage:** Many organisations lack internal cloud security expertise, relying heavily on vendors or consultants.
- **Critical to secure-by-design:** Cloud misconfigurations remain one of the leading causes of breaches, particularly with the increased adoption of SaaS based solutions. Professionalisation can reduce systemic risk.

- **Alignment with emerging tech:** Cloud security engineers increasingly require skills in container security, serverless architectures, and AI-enabled cloud services.
- **Supports mobility:** Provides a clear pathway from SOC, systems administration, or DevOps roles into advanced engineering positions.

2. Identity & Access Management (IAM) Specialist

The Playbook also identifies identity security as a foundational capability for modern cyber defence, especially as organisations adopt zero-trust architectures. IAM failures are a major contributor to breaches, and demand for IAM specialists continues to grow across all sectors. The rationale behind this includes:

- **Zero-trust adoption:** IAM is central to zero-trust strategies, which the Playbook emphasises as a national priority.
- **High-risk area:** Identity compromise remains the most common initial attack vector in Australia.
- **Specialised skillset:** Requires deep knowledge of authentication protocols, federation, privileged access management (PAM), and identity governance.
- **Cross-sector demand:** Critical for government, finance, health, and critical infrastructure.
- **Career pathway clarity:** IAM is often poorly understood as a profession; CyberPath can define clear competencies and pathways.
- **Cross organisational identity brokerage:** With the roll out of a national identity solution and increased expectations for integration with up/downstream identity custodians, trust and assurance of competent professionals

3. Digital Forensics and Incident Response Specialist

The Playbook emphasises the need for stronger national incident response capability, including surge capacity and advanced forensic skills. As cyber incidents increase in frequency and severity, organisations require practitioners who can rapidly contain, investigate, and recover from attacks. The justification behind this includes:

- **National resilience priority:** Incident response is central to the Australian Cyber Security Strategy and the Playbook's focus on preparedness. Exposure opportunities conducted by this role also validate the broader cyber defence readiness by highlighting skills and procedural gaps in a safe environment.
- **Growing threat landscape:** Ransomware, supply chain attacks, and destructive malware require advanced response capabilities.
- **Skill scarcity:** Forensic and IR specialists are among the hardest roles to recruit in Australia.
- **Supports surge capability:** Professionalisation can help establish trusted, readily deployable responders for national-level events.

- **Clear progression:** Provides a pathway from SOC Analyst roles into more advanced investigative positions.

4. DevSecOps Engineer

The Playbook identifies DevSecOps and secure software development as a critical capability gap, particularly as organisational culture shifts toward secure-by-design principles and modern software delivery pipelines. DevSecOps roles are essential for embedding security into development workflows. The thinking behind this includes:

- **Secure-by-design priority:** The Playbook stresses the need for secure coding, threat modelling, and secure SDLC practices.
- **High demand across sectors:** Government, fintech, SaaS providers, and critical infrastructure all require secure development capability.
- **Bridges cyber and engineering:** This role supports collaboration between developers, security teams, and operations.
- **Addresses systemic risk:** Vulnerabilities introduced during development remain a major source of compromise.
- **Supports innovation:** Ensures emerging technologies (AI, automation, cloud-native apps) are built securely from the outset.

5. OT/ICS Security Specialist

Operational Technology (OT) and Industrial Control Systems (ICS) security is one of the most strategically important and under-supplied skill areas in Australia. The Playbook highlights critical infrastructure protection as a national priority, especially under the SOCI Act, and with the resources sector being one of the major contributors to the Australian economy. Reasoning for inclusion of this role includes:

- **Critical infrastructure dependency:** Energy, water, transport, mining, and manufacturing all rely on OT systems vulnerable to cyber-physical disruption.
- **Growing threat landscape:** State-based actors increasingly target ICS environments, especially with the convergence of IT with these environments, requiring specialised defenders.
- **Unique skillset:** OT security requires knowledge of industrial protocols, safety systems, and legacy technologies not covered in traditional IT security roles. Similarly, defence tooling used in these environments is different to traditional IT security operations tooling.
- **Regulatory pressure:** SOCI Act obligations are driving demand for OT-specific risk, monitoring, and incident response capabilities.
- **Workforce scarcity:** The Playbook and CyberPath consultation has identified OT/ICS security as experiencing an acute skill shortage across Australia.

6. Data Security & Privacy Engineer

Data protection is a top priority across government and industry, especially with rising privacy expectations, major breach incidents, and upcoming Privacy Act reforms. The Playbook emphasises data security and privacy engineering as emerging high-demand skill areas.

- **High-impact breaches:** Recent large-scale data breaches have highlighted gaps in data lifecycle protection.
- **Regulatory change:** Privacy Act reforms, critical infrastructure obligations, and sector-specific requirements (e.g., health, finance) are increasing demand for specialised data security skills.
- **AI and data governance:** AI systems require strong data governance, secure data pipelines, and privacy-preserving design.
- **Cross-functional role:** Data Security Engineers bridge cyber, data engineering, legal, and governance functions.
- **Growing demand:** The Playbook identifies data protection, encryption, and privacy engineering as priority capability areas.

7. AI Security & Assurance Specialist

AI adoption is accelerating across Australian organisations, but AI security, safety, and assurance capabilities are still emerging. The Playbook identifies AI security and responsible AI as critical future skill areas. AI solutions are targeted by adversaries using different tactics, techniques, and procedures (TTPs) to traditional enterprise IT technologies. This is reflected with the MITRE ATLAS evolving as an independent framework complementing, rather than augmenting the MITRE ATT&CK framework. As this area is still evolving rapidly, any security operations teams find themselves with inadequate tooling, knowledge, processes, and skill in place to combat this growing threat confidently. The justification behind this role includes:

- **Emerging threat landscape:** AI introduces new attack surfaces (model poisoning, prompt injection, data leakage).
- **Regulatory momentum:** Australia is moving toward AI assurance frameworks and safety standards.
- **Cross-disciplinary expertise:** Combines cyber security, data science, risk management, and ethics.
- **High strategic value:** AI systems increasingly underpin critical decision-making, automation, and national security functions.
- **Future-proofing:** Establishing this occupation early positions Australia as a leader in safe and secure AI adoption.