Cyber engineering practice guide

ENGINEERS AUSTRALIA

March 2025

Version 1.1

Contents

This guide has been prepared with significant contributions from the following Cyber Engineering Working Group members:

Shireane McKinnie (Chair)
Prof Jill Slay
Lee Walsh
James Hine
Walter Green
Bruce Large
Paul Buckley
Edmund Kienast
David Manfield
Pat Gleadhill
Sean Murdoch
Roy Unny
Dipti Fouzder
CH LING

Feedback or enquiries:
aop@engineersaustralia.org.au

Foreword

Engineering practice guides provide guidance on requirements for competently practicing in a particular engineering Area of Practice.

The practice guides are designed to outline established best practices and principles to assist engineering practitioners.

This document was produced by a panel of experts after an extensive review of the existing literature. Practice guides are reviewed periodically and updated as required for continued accuracy and relevance.

Introduction

Cyber engineering practice guide was developed by the Engineers Australia Cyber Engineering Working Group (Working Group) in consultation with the Australian Signals Directorate, the Australian Computer Society and AustCyber.

In developing this practice guide, the Working Group has drawn from the National Institute of Standards and Technology (NIST)'s NICE framework, Skills for the Information Age Framework (SFIA), The Australian Computer Society Cyber Skills Framework, the International Council on Systems Engineering (INCOSE) Competency Framework and the UK Tech Power definitions.

It may be used by individuals to:

- assess their current competencies against industry benchmarks
- develop a professional development plan
- select training courses and learning opportunities
- use as a tool to help in conversations with their manager
- begin preparation for Chartered applications.

Employers and managers can use this guide to:

- assess current competency and capability of individuals and a team
- prepare selection or promotion criteria for staff
- prepare learning interventions
- select training providers
- customise learning content for cyber engineering teams
- adapt or incorporate these competencies into their current framework and practices.

Cyber engineering overview

Cyber engineering (sometimes referred to as cyber security engineering and cyber resiliency engineering) involves the design, implementation, operation, maintenance, response, and improvement of information security measures to protect the confidentiality, integrity, availability, and safety (CIAS) of systems (including autonomous systems) and system security measures to assure the security of hardware, software, firmware, and network components used to store, process, transmit, actuate and sense systems. System security measures are the security controls added to networks to protect confidentiality, integrity, availability and safety. Appendix 1 provides definitions and further information on CIAS.

Cyber engineering includes the understanding of a broad spectrum of security risks and threats that need to be eliminated or mitigated, when creating, designing, operating, modifying or evaluating systems using all types of digital technologies, consisting of hardware, firmware and software components or applications.

This includes, as an important focus, operational technology, industrial control systems, industrial automation, information technology, internet of things, industrial internet of things, and associated communications. It encompasses the engineering activities associated with protecting digital control and monitoring for the automation of plant such as electricity generation plants, electrical substations, water and wastewater pump stations and treatment plants, dams, oil and gas refineries, port operations, rail network coordination, road tunnel operations, hospitals, food production, and other critical infrastructure.

Cyber engineering by its nature is a cross disciplinary/interdisciplinary field of engineering practice. The use of digital technologies continues to grow at a rapid pace both in the development and implementation of designs across all engineering disciplines and the incorporation of digital technologies in system solutions.

This rapid growth in the use of digital technologies has also seen a rapid growth in cyber threats from multiple sources and of an ever-changing nature. These threats may arise from malicious actors, inadvertent human behaviour, or undetected system errors or interactions. To combat these threats, cyber engineers need to have a sound understanding of measures to protect information and minimise the potential exploitation of system vulnerabilities from cyber-attacks.

The nature of cyber is pervasive and intrusive, intertwined into multiple facets of engineered life and a failure of any engineering domain to appropriately consider cyber risks during the engineering process could have catastrophic outcomes. While there is certainly a place for a specialist cyber engineer within the engineering team many engineers will be applying cyber engineering principles within the critical understanding of their major engineering focus. For example, mechanical or electrical engineers must understand the risks that cyber security could pose to their designs, operations, and maintenance.

As we step into a world where the level of cyber-attacks continues to escalate it is almost certain that we will see more attacks like:

- The colonial pipeline (https://www.Bloomberg.Com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password#xj4y7vzkg)
- San Francisco water treatment (https://www.Nbcnews.Com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206)

- Taiwan oil refinery (https://portswigger.Net/daily-swig/taiwans-major-oil-refineries-struck-by-malware-causing-chaos-at-gas-stations)
- Microsoft hacked by russian hacking group who accessed email and source code (https://edition.Cnn.Com/2024/01/19/tech/microsoft-russian-hacking-executives/index.Html)
- Cyber attacks in australia (https://www.9news.Com.Au/cyber-attack)

The above attacks epitomise the cyber physical battlefield where advanced persistent threats are targeting systems and infrastructure that lack appropriate protections by design or exploiting operational control vulnerabilities. Additionally, modern systems can be vulnerable to inadvertent actions of users, operators, and maintainers.

The integration of cyber security into the engineering process is essential in achieving a secure by design future rather than adding security to systems after it has been completed.

Cyber engineering principles

Engineers practising cyber engineering need to understand and apply the following cyber engineering principles:

1. Take a whole of system, whole of lifecycle approach to secure design, manufacturing/production, operation, maintenance, and disposal. The whole system includes all technology, people, information, and processes. Technology includes all hardware, firmware and software and interconnected systems; people includes human interactions, human behaviour and skills to operate and maintain the systems; and processes includes in built controls and processes required to operate and maintain the system securely.
2. Implement an engineering management system linked to the enterprise governance framework that provides for clear accountability, authority and responsibility for secure design, manufacturing/production, operation, maintenance and disposal of the system.
3. Undertake continuous threat and vulnerability modelling to understand emerging security risks, to inform and build in physical and logical security measures that are readily evolvable to incorporate new technologies, changes to threats, user needs and assessed risks.
4. Tailor engineering processes and standards to system complexity and security needs.
5. Apply the engineering principles applicable to the context in which the system is to be designed, operated, maintained, and disposed. For example, cyber engineering principles for the design and deployment of cyber security systems.
6. Undertake analysis of both functional and non-functional requirements (e.g., performance, reliability, accuracy, timeliness, confidentiality, integrity, availability, safety, human factors) to understand priorities and trade-offs of stakeholder needs and document decision trade-offs. Safety and security are addressed as coordinated views when determining trade-offs. Stakeholder needs include system intended capability outcomes, economic and organisational needs, customer requirements, regulatory requirements and risk appetite.

7. Design and refine the system architecture to reduce the evolving threat attack surface, cognisant of strategic and operational performance, support, stakeholder needs and security risks.

8. Ensure all system elements are integrated in a logical sequence and tested to ensure that the system operates as intended.

9. Plan and implement verification and validation processes that provide objective evidence of system performance, identify residual security risks, determine and monitor actions required to mitigate or accept residual risks.

10. Establish processes to rigorously manage all interfaces (physical, logical and human), including interfaces to external systems or networks where the authenticity of the connected systems cannot be accurately determined or actively managed.

11. Assume that there will be successful attacks on the system and design in mechanisms to minimise the impact of and aid recovery from such attacks. Changes in sophistication, diversity and vectors of attacks must be expected. Plan for monitor and regularly exercise system recovery processes as part of the operations, support and maintenance regimes to assure system resilience.

12. Anticipate and expect human error that might create vulnerabilities (both intentional and unintentional).

13. Establish mechanisms to detect and eradicate counterfeit parts, components, firmware and software that may contain malicious or poor-quality code in the supply chain, e.g., through functional and physical configuration audits.

14. Design in mechanisms to detect and report unauthorised use, unusual or unpredicted system behaviour.

15. Define robust processes for introducing software and patches into the system to reduce the risk of unintended security impacts or adverse impacts on system safety or performance.

16. Implement security measures through a layered and multifactored approach.

17. Design and implement maintenance, support and disposal regimes that ensure secure configuration control, disciplined change management, system performance monitoring, and obsolescence management (including system updates and regular patching). Plan for and ensure the systematic management of system components (hardware, firmware, and software) that are likely or may become obsolete during the life of the system/product from introduction into service through to disposal.

Cyber workforce

The cyber workforce includes a wide range of people working across a broad range of disciplines including engineering, information technology, intelligence, legal, law enforcement, governance, talent management, operators and users.

Figure 1 provides a conceptual view of the relationship between engineering and other parts of the cyber workforce. In particular, it illustrates the relationship between the engineering workforce and the it workforce where the digitisation of organisations and industrial processes, significant convergence has occurred.

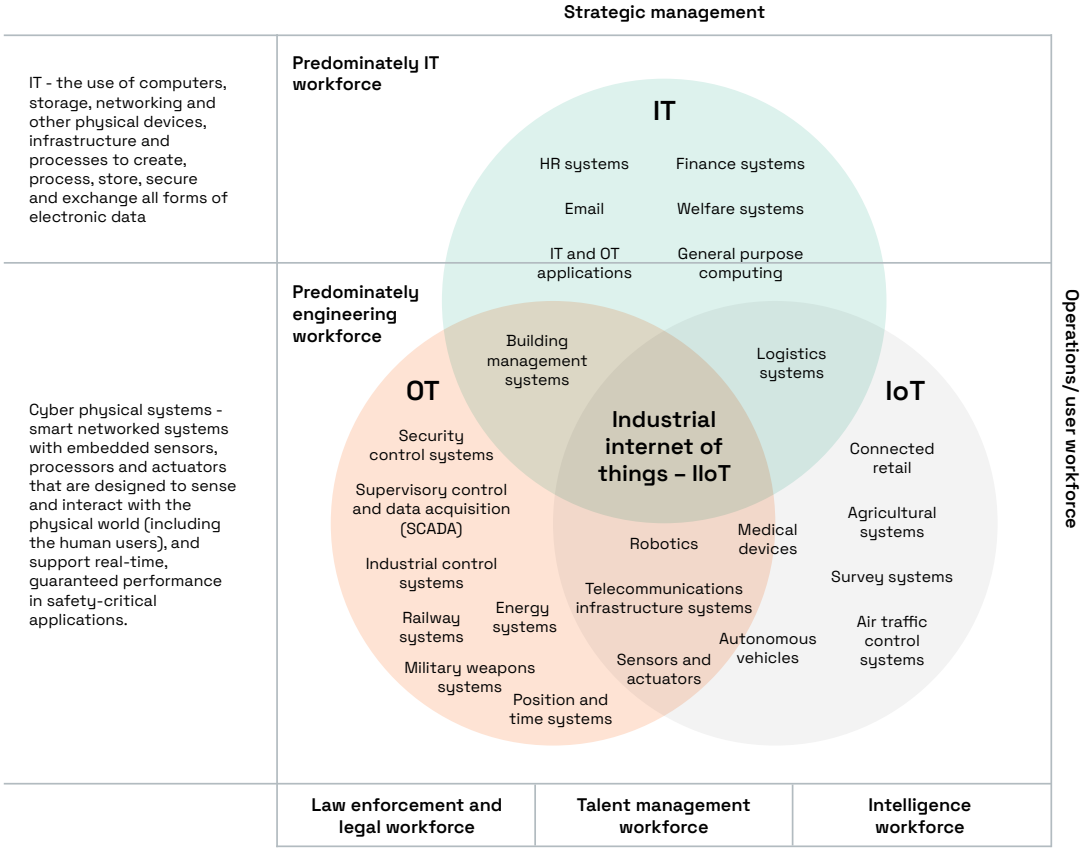

Figure 1: Workforce domain relationships

The cyber engineering workforce includes professional engineers, engineering technologists and engineering associates whose role is to define requirements, analyse solution options design, develop, implement, maintain and monitor cyber solutions within complex environments.

Typically, cyber engineers are involved in the full spectrum of cyber work including cyber security (self-defence and passive defence) and cyber operations (active defence, and offence*) and will:

- Identify systemic security issues based on the analysis of vulnerability, threat and secure configuration data. They apply risk management and safety principles to identify constraints and trade-offs to determine and adapt system and/or product requirements. They select and apply network product and control system security architecture concepts including topology, protocols, components, standards, and approaches to describe, analyse, and document digital technology architectures.

- Select and apply secure design tools, methods and techniques including automated systems analysis and design tools to design secure architectures using cyber and information security management systems knowledge and frameworks covering the entire system, including interconnected systems across the full life cycle of the system. They identify critical infrastructure systems which utilise digital technologies that were designed without system security considerations, then design and implement measures to remediate security vulnerabilities including using non-technical measures.

*offensive cyber operations are considered the domain of Government

- Perform security assurance activities such as specification and design of tests, including penetration tests, audit functions, security monitoring, resilience performance requirements and identifying, saving, protecting and storing information that will assist a cyber forensic investigation. This is to comprehensively confirm that all features are achieved to minimise the risk of attack by malicious or unwitting actors and provide information to prevent potential attacks and analyse cyber events to identify perpetrators. They select the parameters used for secure configuration management and identify features to support asset, patching and vulnerability management including backups, updates, configuration files, sample test and conformance data, fault finding and maintenance.

- Conduct supply chain risk assessments associated with system components, interconnected systems (within the enterprise and systems to which the enterprise is connected) and implement supply chain management plans to minimise the risk of introducing vulnerabilities from third parties.

- Apply incident response, disaster recovery and business continuity knowledge to design systems and processes to operate and maintain systems or products to continually protect confidentiality of information, integrity of system performance and maintain system availability.

Examples of a cyber engineer's work may include:

- Determining requirements for designing, implementing, operating and maintaining physical systems and assessing cyber risks that are posed by physical systems to the safety of people, the environment and systems.

- Determining requirements for designing, implementing, operating and maintaining cyber security controls in existing systems or network environments where the effects and risks of implementation must be assessed against network capability, capacity and security.

- Determining requirements for designing, implementing and maintaining physical (e.g., Biomedical devices, process control interfaces, network hardware, ICT, IoT) products that have networked interfaces where the engineer must ensure that appropriate security practices are developed and followed to ensure that the confidentiality, integrity, availability and safety of the product is not compromised.

- Assessing cyber security and cyber worthiness of industry products by providing design control, governance, risk management, compliance and assurances.

Career map

Figure 2 below provides an indicative career ecosystem for Professional Engineers, Engineering Technologists and Engineering Associates working in cyber engineering.

Professional Engineers typically work on complex engineering challenges within a broad discipline, Engineering Technologists typically work on broadly defined engineering challenges within a narrower engineering sub-discipline and Engineering Associates typically work on well-defined engineering challenges within a sub-discipline.

The red arrows indicate potential career pathways; they are not intended as a mandated career path. While this map indicates that Professional Engineers will largely be involved in the "Securely Design and Provision" and "Maintain and Protect" roles with Technologists and Associates primarily working in "Operate and Defend" and "Respond and Recover" work roles, it is envisaged that there will be lateral movement depending on complexity, safety, and level of criticality to the enterprise and the lifecycle.

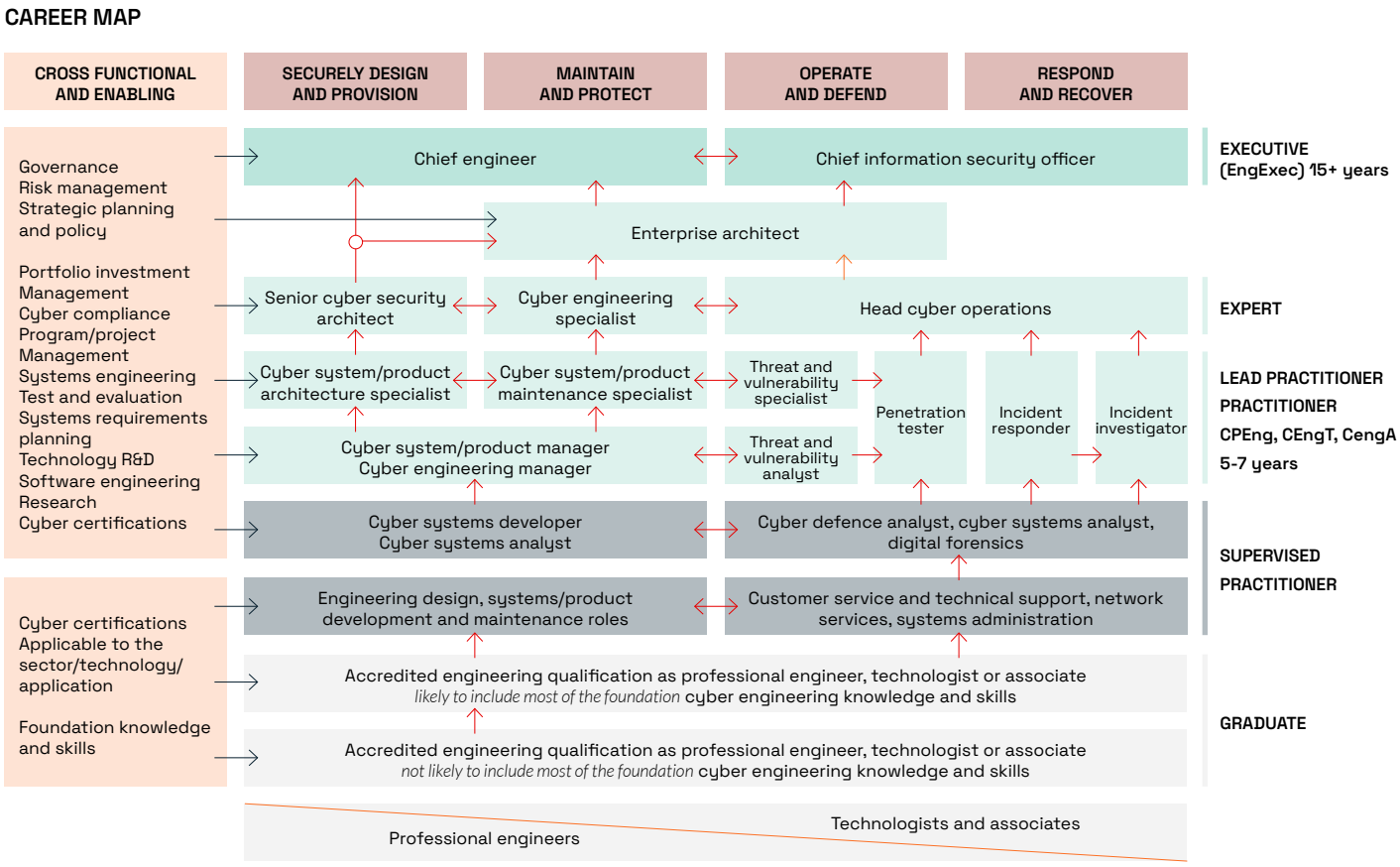

Figure 2: Indicative career map

Foundation skills and knowledge

People wishing to pursue a career in cyber engineering in Australia will first need to demonstrate entry-to-practice competency. This can be demonstrated by completing an accredited cognate degree or through an entry-to-practice competency assessment. This ensures that the individual has attained a thorough understanding of the body of engineering knowledge relevant to one's occupational category (Professional Engineer, Engineering Technologist, or Engineering Associate), with the ability to apply this knowledge.

Entry-to-practice competency elements represent the profession's expression of the knowledge and skill base, engineering application abilities, and professional skills, values and attitudes that must be demonstrated at the point of entry to practice.

For more details on entry-to-practice competencies visit:

Stage 1 Competency Standard for Professional Engineers

Stage 1 Competency Standard for Engineering Technologists

Stage 1 Competency Standard for Engineering Associates

The Independent practice (Stage 2) competencies are grounded on the entry-to-practice (Stage 1) competencies. Individuals are required to demonstrate Independent practice competency to attain the Chartered credential in their area of practice. More information on the Competency standards for independent practice can be found at the following links:

Stage 2 competency standard for Professional-Engineers

Stage 2 competency standard for Engineering Technologists

Stage 2 competency standard for Engineering Associates

The engineering programs listed below typically provide students and engineers wishing to pursue a cyber engineering career with a reasonable understanding of digital systems and the engineering process involved in cyber engineering and most of the foundation skills and knowledge. However, there may be some additional further specialisation training and work experience required to develop cyber specific competencies required to meet Engineers Australia Competency standards.

- Cyber Security Engineering
- Electronic and Communication Systems Engineering
- Mechatronic Systems Engineering
- Software Engineering
- Digital Systems and Telecommunications Communications Engineering
- Telecommunications Engineering Technology (Computer Systems Engineering)
- Engineering Technology (Electronics and Communication Engineering)
- Industrial and Systems Engineering
- Telecommunications Network Engineering

- Computer Systems Engineering
- Electronic and Communication Engineering
- Computer Systems and Networking Engineering
- Information Engineering
- Computer Engineering
- Computer Systems Engineering
- Information Technology and Telecommunications Cyber Security
- Network Engineering
- Internet Engineering
- Computer Network Engineering
- Computer Science and Engineering
- Industrial Computer Systems Engineering
- Network and Software Systems Engineering
- Information Technology and Telecommunications Engineering
- Electronic systems and Security Engineering
- Internet of Things Engineering
- Engineering Electrical and Information Processing Control and Instrumentation
- Electrical and Information Processing

The qualifications set out below acknowledge there will be aspects of cyber engineering necessary across all engineering disciplines. However, during their university education or vocational training, graduates from these programs are unlikely to have developed the critical formal foundation knowledge and skills related to digital systems and networks that is required by a cyber engineer. These engineers will likely require additional education, training, and work experience to gain the foundation skills and knowledge for a cyber engineer.

To accommodate the essential need for cyber engineers with contextual knowledge of their particular discipline, cyber engineers that graduated and trained in an engineering discipline (such as those listed below) are expected to have subsequently gained significant industry experience and attained industry certifications, micro-credentials, masters degrees or other qualifications that provide them with the critical knowledge and skills to practice cyber engineering.

- Biomedical Engineering
- Systems Engineering
- Electrical and Data Analytics Engineering
- Electrical Engineering
- Electrical Power and Control Engineering
- Internet of Things and Data Engineering
- Biomedical and Electronic Instrumentation and Control
- Information Technology and Data Analytics Engineering (Application Development)
- Robotics and Mechatronics
- Engineering Technology (Industrial Instrumentation Engineering)
- Industrial Automation

- Electrical Power Engineering
- Aerospace Engineering
- Mechanical Engineering
- Civil Engineering
- Marine and Maritime Engineering
- Materials Engineering

For information on Engineers Australia Accreditation and Accredited Programs, visit Accreditation.

Cyber engineering practice elements

Table 1 identifies the Practice Elements that Professional Engineers, Engineering Technologists and Engineering Associates should seek to acquire as part of their formal education, training, and experience. The skills and knowledge that form the competencies that underpin the practice elements would typically be acquired through the completion of an accredited engineering program and/or the completion of a range of additional certifications, micro credentials or master's degrees.

Examples of vendor independent certifications are provided in Table 2.

Table 1: Cyber engineering specific skills and knowledge for professional engineers, technologists and associates

Practice element	Indicators		
	Professional Engineer	Engineering Technologist	Engineering Associate
1. Threat modelling and risk analysis	**Develops and fluently applies** cyber threat assessment techniques, including threat modelling, and application of risk management principles to analyse trade-offs, constraints and determine system/product design requirements consistent with enterprise priorities and risk appetite. **Identifies and critically appraises** exploitation tactics, techniques, and methods to identify and prevent them. **Identifies and critically appraises** exploitation tactics, techniques, and methods to identify and prevent them.	**Fluently applies** cyber threat assessment techniques and application of risk management principles to analyse trade-offs, constraints and determine system/product design requirements consistent with enterprise priorities and risk appetite. **Identifies and critically appraises** exploitation techniques and methods to identify them. **Identifies and critically appraises** exploitation techniques and methods to identify them.	**Applies** prescribed threat assessment techniques and risk management principles. **Identifies and understands** exploitation techniques and methods to identify them. **Identifies and understands** exploitation techniques and methods to identify them.

Practice element	Indicators		
	Professional Engineer	Engineering Technologist	Engineering Associate
2. Security models and standards	**Appreciates** organisational security controls including cyber security management frameworks, standards, and best practices. **Develops and proficiently applies** knowledge of selection of appropriate security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). and data security requirements that apply to different types of data including legal requirement and privacy principles applying to data such as Personal Information Payment Card Information and Health Information. **Proficiently applies** standards such as ISA/IEC 62443 Security Process Hazard Analysis Reviews and the applicability of models to particular sectors.	**Appreciates** organisational security controls including cyber security management frameworks, standards, and best practices. **Proficiently applies** knowledge of selection of appropriate security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). and data security requirements that apply to different types of data including legal requirement and privacy principles applying to data such as Personal Information Payment Card Information and Health Information. **Understands and applies** standards such as ISA/IEC 62443 Security Process Hazard Analysis Reviews and the applicability of models to particular sectors.	**Understands** principles of organisational security controls including cyber security management frameworks, standards, and practices.
3. Human Factors	**Appreciates** social and behavioural factors impacting user attitudes toward security controls and human factors related to useability of security features. **Proficiently applies** human-computer interaction principles and the tools and techniques used to minimise the impact of human error.	**Appreciates** social and behavioural factors impacting user attitudes toward security controls and human factors related to useability of security features. **Proficiently applies** human-computer interaction principles and the tools and techniques used to minimise the impact of human error.	**Understands** social and behavioural factors impacting user attitudes toward security controls and human factors related to useability of security features. **Proficiently executes** human-computer interaction principles and the tools and techniques used to minimise the impact of human error.

Practice element	Indicators		
	Professional Engineer	Engineering Technologist	Engineering Associate
4. Computer networking	**Develops and proficiently applies** computer networking concepts and protocols, including bandwidth management, network security methodologies, resiliency and redundancy for local area and wide area networking. **Identifies and critically appraises** traffic flows across a network, network systems management principles, models, methods (e.g., end-to-end systems performance monitoring, cross-domain solutions, enforcement of unidirectional data flows, packet inspection, content filtering), and tools.	**Proficiently applies** computer networking concepts and protocols, including bandwidth management, network security methodologies, resiliency and redundancy for local area and wide area networking. **Identifies and applies** basic principles of traffic flows across a network, network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	**Proficiently executes** computer networking concepts and protocols, including bandwidth management, network security methodologies, resiliency and redundancy for local area and wide area networking. **Maintains a broad understanding** of traffic flows across a network, network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
5. Security architectures	**Identifies and critically appraises** security architecture concepts including minimising attack surface, topology, protocols, components, and principles and design countermeasures and monitoring systems for identified security risks.	**Identifies and applies** security architecture concepts including topology, protocols, components, and principles and design countermeasure for identified security risks.	**Maintains a broad understanding** of basic principles of security architecture concepts including topology, protocols, components, and principles and design countermeasure for identified security risks.
6. Cyber laws and regulations	**Identifies and understands** laws, regulations, policies, and ethics as they relate to cybersecurity, privacy, and organisational requirements .	**Identifies and understands** laws, regulations, policies, and ethics as they relate to cybersecurity, privacy, and organisational requirements.	**Understands** laws, regulations, policies, and ethics as they relate to cybersecurity, privacy, and organisational requirements .

Practice element	Indicators		
	Professional Engineer	Engineering Technologist	Engineering Associate
7. System, data protection and cryptographic systems	**Develops and fluently applies** techniques for the protection of data such as personal information, Payment Card Industry Personal Health Information. **Identifies and critically appraises** cryptography and its application.	**Fluently applies** techniques for the protection of personal information. **Identifies and understands** cryptography and its application.	**Applies** prescribed techniques for the protection of personal information. **Understands** cryptography and its application.
8. Advanced mathematical concepts	**Develops and fluently applies** mathematics (e.g., logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis), computer, coding theory for forward error correction, data compression, checksums, hash codes, encryption, and decryption algorithms.	**Fluently applies** cryptography in protecting information and systems.	**Rigorously and objectively applies** prescribed cryptography in protecting information and systems.

Practice element	Indicators		
	Professional Engineer	Engineering Technologist	Engineering Associate
9. Infrastructure security	**Identifies and critically appraises** software, hardware and firmware associated with digital technologies and including parallel and distributed computing concepts. **Identifies and critically appraises** cyber physical systems, industrial control systems and digital infrastructure their differing risk profiles and what cyber security mitigations can be applied to them. **Identifies and critically appraises** the infrastructure and systems associated with data centres their differing risk profiles and what cyber security mitigations can be applied to them. **Identifies and critically appraises** electromagnetic interference.	**Identifies and understands** software, hardware and firmware associated with digital technologies and parallel and distributed computing concepts. **Identifies and understands** cyber physical systems, industrial control systems and digital infrastructure security. **Identifies and understands** the infrastructure and systems associated with data centre security.	**Identifies and understands** software, hardware and firmware associated with digital technologies and parallel and distributed computing concepts. **Maintains a broad understanding** of cyber physical systems, industrial control systems and digital infrastructure security **Maintains a broad understanding** of the infrastructure and systems associated with data centre security.

Practice element	Indicators		
	Professional Engineer	Engineering Technologist	Engineering Associate
10. Authentication, authorisation and accountability	**Identifies and critically appraises** identification and authentication measures and support tools.	**Identifies and applies** identification, and authentication measures and support tools.	**Maintains a broad understanding** of identification and authentication measures and support tools.
	Develops and fluently applies access controls including logical access controls (Principle of least privilege, Segregation of duties, Discretionary access control (DAC), Mandatory access control (MAC), and Role-based access control (RBAC) and physical access controls. **Identifies and applies** access authentication and access management methods (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	**Fluently applies** access controls including logical access controls (Principle of least privilege, Segregation of duties, Discretionary access control (DAC), Mandatory access control (MAC), and Role-based access control (RBAC) and physical access controls.	**Proficiently executes** access controls including logical access controls (Principle of least privilege, Segregation of duties, Discretionary access control (DAC), Mandatory access control (MAC), and Role-based access control (RBAC) and physical access controls.
11. Systems engineering	**Develops and fluently applies** the principles of systems engineering including system life cycle management and system design standards applicable to safety, security, and mission criticality of systems. **Identifies and applies** safety and cyber security analyses and safety/security trade-off analysis techniques. **Develops and fluently applies** systems engineering practices to whole of life and whole of system, including interconnected systems, products, and components.	**Fluently applies** the principles and application of systems and software engineering and software development models including system life cycle management and system design standards applicable to safety, security, and mission criticality of systems. **Fluently applies** basic principles of systems engineering practices to whole of life and whole of system, including interconnected systems, products, and components	**Maintains a broad understanding** of systems engineering. **Proficiently executes** well defined activities within the lifecycle.

Practice element	Indicators		
	Professional Engineer	Engineering Technologist	Engineering Associate
12. Software Engineering	**Develops and fluently applies** requirements identification and specifications for both functional and non-functional requirements. **Develops and fluently applies** multi-factor protection and authorisation methods. **Develops and fluently applies** design methodologies for software specifications. **Develops and fluently applies** secure error logging, configuration and performance management techniques including the protection services for data used in cyber forensic investigations. **Develops and fluently applies** test methods to ensure the correct operation of systems. **Identifies and applies** safety and cyber security analyses and safety/security trade-off analysis techniques. **Develops and fluently applies** secure configuration management techniques.	**Fluently applies** data gathering services for Requirements identification and specifications for both functional and non-functional requirements. **Fluently applies** secure error logging, configuration and performance management data analysis techniques. **Fluently applies** prescribed analysis methods to ensure the correct operation of data storage and back-up services. **Fluently applies** methods to ensure the integrity and correct application of test procedures. **Fluently applies** methods to collate and prepare test results for audit analysis. **Fluently applies** secure configuration management techniques.	**Proficiently executes** prescribed secure error logging, configuration and performance management data analysis techniques. **Proficiently executes** prescribed analysis methods to ensure the correct operation of data storage and back-up services. **Fluently applies** test procedures to methods to ensure the integrity and correct application of the software. **Fluently applies** methods to document and collate test results. **Proficiently executes** prescribed secure configuration management techniques.

Practice element	Indicators		
	Professional Engineer	Engineering Technologist	Engineering Associate
13. Cyber system design	**Develops and proficiently applies** structured analysis principles, system and product design tools, methods, and techniques, including automated systems analysis and design tools and their application to cyber system design. **Develops and proficiently applies** structured analysis principles, system and product design tools, methods, and techniques for forensic analysis.	**Fluently applies** product design tools, methods, and techniques under broad guidance.	**Proficiently executes** prescribed activities within the design stage of the lifecycle.
14. Supply chain management	**Develops and fluently applies** supply chain risk management practices to outsourcing and procurement activities.	**Fluently applies** supply chain risk management processes to outsourcing and procurement activities.	**Proficiently executes** prescribed supply chain management to activities.
15. Business continuity and incident management	**Develops and fluently applies** Business Continuity (BC), Disaster Recovery (DR), Backup and Incident Response Concepts.	**Proficiently applies** Business Continuity (BC), Disaster Recovery (DR), Backup and Incident Response Concepts.	**Proficiently executes** prescribed Business Continuity (BC), Disaster Recovery (DR), Backup and Incident Response Concepts.
16. Emerging technologies	**Identifies and critically appraises** emerging technologies in the cybersecurity field, such as zero trust, secure by design or secure by default and how they can be applied to enhance security in engineering systems. Identifies and critically appraises the challenges associates with securing emerging applications such as blockchain, artificial intelligence, and machine learning, cloud.	**Identifies and understands** emerging technologies in the cybersecurity field, such as zero trust, secure by design or secure by default and how they can be applied to enhance security in engineering systems. Identifies and critically appraises the challenges associates with securing emerging applications such as blockchain, artificial intelligence, and machine learning, cloud.	**Understands** emerging technologies in the cybersecurity field, such as zero trust, secure by design or secure by default and how they can be applied to enhance security in engineering systems. Identifies and critically appraises the challenges associates with securing emerging applications such as blockchain, artificial intelligence, and machine learning, cloud.

Practice element	Indicators		
	Professional Engineer	Engineering Technologist	Engineering Associate
17. Vulnerability assessment and penetration testing	**Develops and fluently applies** vulnerability assessment and penetration testing regimes.	**Fluently applies** vulnerability assessment and penetration testing tools and techniques.	**Proficiently applies** vulnerability assessment and penetration testing tools and techniques.

Professional Engineers, Engineering Technologists and Engineering Associates wishing to pursue a career as a cyber engineer may need to acquire additional cyber specific credentials. While for particular jobs employers may require vendor specific credentials relevant to the products or systems employed within the enterprise, there are a number of vendor independent cyber certifications that employers and individuals may consider in order to gain additional cyber skills and knowledge to complement those acquired through formal education, training and on the job experience. Some examples of such certifications are set out in Table 2 below.

Table 2: Example vendor independent cyber certifications

Provider	Professional Engineer	Engineering Technologist	Engineering Associate
ISC2	CISSP - Certified Information Security Professional CISSP - ISSAP Cyber Information Security Professional – Information Systems Security Architecture Professional CISSP - ISSEP Cyber Information Security Professional – Information Systems Security Engineering Professional CCSP - Certified Cloud Security Professional	SSCP - Systems Security Certified Practitioner	SSCP - Systems Security Certified Practitioner
ISACA	CISM - Certified Information Security Manager CGEIT - Certified in Governance Enterprise Information Technology	CRISC - Certified in Risk and Information Systems Control CPDSE - Certified Data Privacy Solutions Engineer CISA- Certified Information Security Auditor	CRISC - Certified in Risk and Information Systems Control CPDSE - Certified Data Privacy Solutions Engineer CISA- Certified Information Security Auditor
CompTIA		CySA+ - Cyber Security Analyst Pentest+ - Penetration Test	Security+ - CySA+ Pentest+

Pathways to Chartered

The Chartered credential is the highest available technical credential for an engineering professional. It is nationally and internationally recognised as a measure of excellence and signifies a certain level of skill, talent and experience for competent, independent practice.

For more information on Engineers Australia's chartered application process for cyber engineering in different occupational categories (Professional Engineers, Engineering Technologists, and Engineering Associates), visit Chartered.

Within the overall competency framework and Indicative career map, Professional Engineers, Engineering Technologists and Engineering Associates undertaking the various cyber engineering work roles would be engaged in engineering practice to develop their cyber engineering competencies progressively over time, consistent with the typical career stages as set out in the below.

Table 3: Indicative career stages and levels of authority, responsibility and competence

Graduate	Works under close direction. The person displays knowledge of key ideas associated with each competency area and understands key issues and their implications.
Supervised Practitioner	Works under routine direction. The person displays an understanding of each competency area and has some limited experience.
Practitioner	Works under general direction. The person displays both knowledge and practical experience of each competency area and can function without supervision on a day-to-day basis. More experienced practitioners work under general direction within a clear framework of accountability.
Lead Practitioner	Works under broad direction. The person displays extensive and substantial practical knowledge and experience of each competency area and provides guidance to others including practitioners encountering unusual situations.
Expert	Has defined authority and accountability for actions and decisions within a significant area of work, including technical, financial, and quality aspects. In addition to extensive and substantial practical experience and applied knowledge of each competency area, this individual contributes to and is recognised beyond the organisational or business boundary.
Executive	Sets strategy, inspires, and mobilises resources. In addition to extensive and substantial practical experience and applied knowledge of each competency area this person has authority over all aspects of a significant area of work, including policy formation and application.

Figure 3 below provides indicative years of experience that Professional Engineers, Technologists and Associates would need to have in order to demonstrate the requisite knowledge, skills and experience to achieve Chartered status. Typically, the competencies for Chartered would be demonstrated at 5 to 7 years of experience and would be achieve at the practitioner and lead practitioner level.

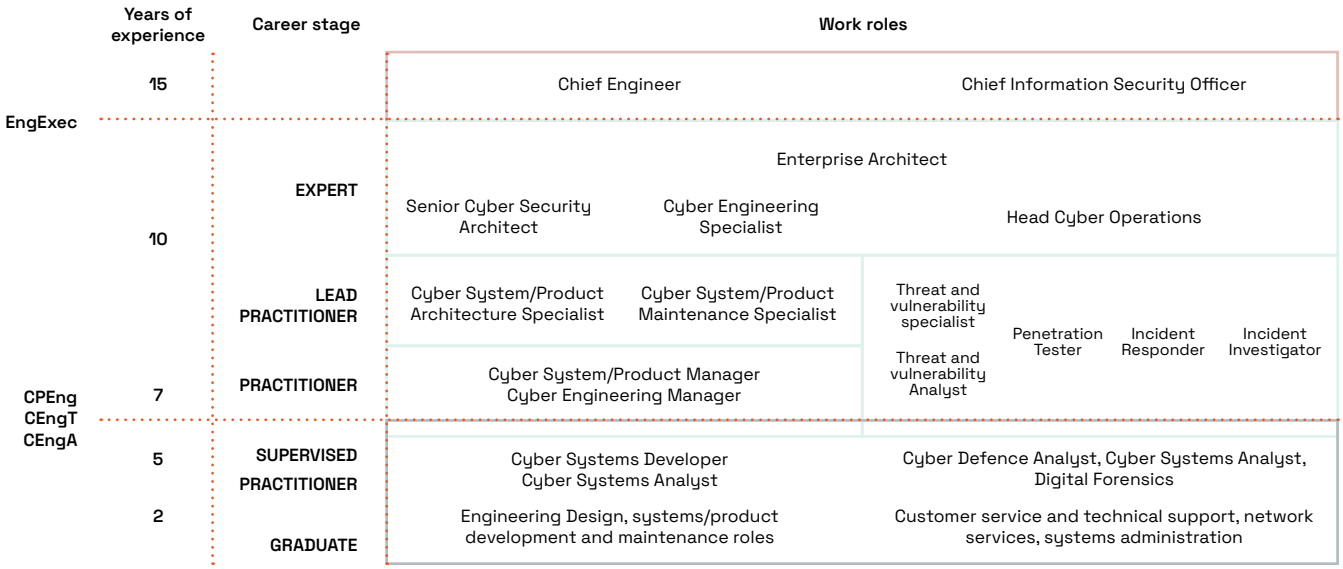

Figure 3: Indicative pathway to Chartered and EngExec

Articulation and alternative pathways

Engineering articulation is open to Engineering Technologists and Engineering Associates who want to advance their career by moving to a higher occupational category. Alternative pathways are relevant for those who have not completed a relevant accredited qualification. For more information, visit Articulation

Those that do not meet all the requirements for full membership with Engineers Australia as a Professional Engineer, Engineering Technologist or Engineering Associate but are working in the cyber engineering field can complete a competency assessment in order to be recognised for entry to practice as an engineer. This assessment is used where people have qualifications in fields related to cyber engineering, for example, computer science, and have post-graduate qualifications and substantial engineering experience.

For more information, visit Competency assessment

Work roles and indicative skills

Below are the indicative skills and work roles that are likely to be required to practise in a competent manner in the indicated roles for cyber engineering.

The typical functions and indicative skills for each work role in the career map are set out below. These can be tailored by employers to the needs of the enterprise when developing job descriptions and skills requirements for particular positions. Individuals can also use these to identify likely skills they will need to develop in their career journey.

The work roles presented here are drawn from the indicative career map at Figure 2 for each career stage with the indicative cyber skills derived consistent with typical career progression and levels of resposibility and authority outlined in Table 3 and Figure 3 above.

Table 4: Typical function and skills for cyber engineering

Work role: Chief Engineer	Career stage
Functions: Responsible for leading engineering activities across an enterprise.	**Executive**
Indicative skills: — Champions and leads the application of the cyber engineering principles at the enterprise level. — Has authority over all aspects of engineering work, including policy formation and application. Is fully accountable for actions taken and decisions made, both by self and others to whom responsibilities have been assigned. — Inspires the organisation, and influences developments within the industry at the highest levels. Makes decisions critical to organisational success. Develops long-term strategic relationships with customers, partners, industry leaders and government. — Collaborates with leadership stakeholders ensuring alignment to corporate vision and strategy. — Applies the highest level of leadership to the formulation and implementation of strategy. Performs extensive strategic leadership in delivering business value through vision, governance, and executive management. Has a deep understanding of the industry and the implications of emerging technologies for the wider business environment. — Has a full range of strategic management and leadership skills. — Communicates the potential impact of emerging practices and technologies on organisations and individuals and assesses the risks of using or not using such practices and technologies. — Establishes governance to address business risk. — Ensures proposals align with the strategic direction of the organisation. — Fosters a learning and growth culture across the organisation. — Assess the impact of legislation and actively promotes compliance and inclusivity. — Advances the knowledge and/or exploitation of technology within one or more organisations. — Champions creativity and innovation in driving strategy development to enable business opportunities. — Communicates persuasively and convincingly across own organisation, industry, and government to audiences at all levels. — Learning and professional development — ensures that the organisation develops and mobilises the full range of required skills and capabilities. — Security, privacy, and ethics — provides clear direction and strategic leadership for the implementation of working practices and culture throughout the organisation. — Has established a broad and deep business knowledge including the activities and practices of own organisation and a broad knowledge of those of suppliers, partners, competitors, and clients. — Fosters a culture to encourage the strategic application of engineering bodies of knowledge within their own area of influence.	

Work role: Enterprise Architect	Career stage
Functions: Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) and operational technology (OT) rules and requirements that describe baseline and target architectures.	**Expert**
Indicative skills: — Champions and leads the application of the cyber engineering principles. — Develops enterprise-wide architecture and processes to embed the strategic application of change in the management of the organisation. — Leads the creation and review of a systems capability strategy that meets the strategic requirements of the business. Ensures the buy-in of all key stakeholders. — Captures and prioritises market and environmental trends, business strategies and objectives, and identifies the business benefits of alternative strategies. Develops and presents business cases for approval, funding, and prioritisation of high-level initiatives. — Sets strategies, policies, standards, and practices to ensure compliance between business strategies, technology strategies, and enterprise transformation activities. — Champions the importance and value of requirements management principles and selecting effective requirements management life cycle models. — Develops organisational policies, standards, and guidelines for requirements definition and management. — Plans and leads scoping, requirements definition and priority setting for complex, strategic programmes. — Drives adoption of, and adherence to, policies and standards. Develops new methods and organisational capabilities for requirements management. — Advises on the suitability of the approach to system architectural design. — Advises and arbitrates on complex or sensitive system architecture-related issues. — Advises in techniques for concept generation. — Coaches lead practitioners in system architectural design.	

Work role: Senior Cyber Security Architect	Career stage
Functions: Ensures that the stakeholder security requirements necessary to protect the organisation's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.	**Expert**
Indicative skills: — Champions and leads the application of the cyber engineering principles. — Develops and communicates corporate information security policy, standards, and guidelines. — Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards, and guidelines. — Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits, and risks. — Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts. — Develops enterprise-wide architecture and processes to embed the strategic application of change in the management of the organisation. — Leads the creation and review of a systems capability strategy that meets the strategic requirements of the business. Ensures the buy-in of all key stakeholders. — Captures and prioritises market and environmental trends, business strategies and objectives, and identifies the business benefits of alternative strategies. Develops and presents business cases for approval, funding, and prioritisation of high-level initiatives. — Sets strategies, policies, standards, and practices to ensure compliance between business strategies, technology strategies, and enterprise transformation activities. — Leads the development of architectures for complex solutions ensuring consistency with agreed requirements. — Establishes policies, principles, and practices for the selection of solution architecture components. — Manages trade-offs and balances functional, service quality and systems management requirements within a significant area of the organisation. Communicates proposed decisions to stakeholders. — Coordinates and manages the target architecture across multiple projects or initiatives. Maintains a stable, viable architecture and ensures consistency of design and adherence to appropriate standards across multiple projects or initiatives. — Champions the importance and value of requirements management principles and selecting effective requirements management life cycle models. — Develops organisational policies, standards, and guidelines for requirements definition and management. — Plans and leads scoping, requirements definition and priority setting for complex, strategic programmes. — Drives adoption of, and adherence to, policies and standards. Develops new methods and organisational capabilities for requirements management. — Demonstrates a full understanding of architectural design and functional analysis techniques and their appropriateness, given the levels of complexity of the system of interest. — Reviews and judges the suitability of architecture designs and associated analyses. — Realises systems using a model that comprises a complete, coherent, and consistent architectural design. — Coaches new and experienced practitioners in system architecture design.	

Work role: Cyber Engineering Specialist	Career stage
Functions: Provides expert guidance to others on the application of the Cyber Engineering principles including practitioners encountering unusual situations.	**Expert**
Indicative skills: — Recognised as an authority in cyber engineering principles and their application to systems design, operation, and maintenance. — Contributes to best practice in the application of cyber engineering principles to systems design operation and maintenance. — Influences key stakeholders beyond the enterprise boundary to support cyber engineering. — Develops new applications of mathematical methods, models, and techniques to cyber engineering practices. — Advises and arbitrates on issues which relate to complex cyber engineering principles. — Reflects and develops ideas of engineering approach based on experience and learning. — Maintains awareness of developments in sciences, technologies, and related engineering disciplines, recognising areas where new developments might be applicable within cyber engineering or the enterprise. — Champions the introduction of novel cyber engineering practices and techniques, producing measurable improvements. — Coaches lead practitioners in applying engineering approaches to their work. — Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation of complex information or operational technology systems. — Defines and documents enterprise-level cyber engineering policies, procedures, guidance, and best practice for cyber engineering activities, including associated tools. — Reviews and judges the tailoring of enterprise-level engineering processes to meet the needs of a cyber project or to accommodate novel, complex, or difficult system/product situations or problems. — Reviews and judges the suitability of plans to be used throughout the lifecycle. — Reviews and judges the suitability of cyber solutions and the planned approach against key cyber engineering design parameters. — Carries out sensitivity analyses on confidentiality, integrity, availability, safety, and risk trade-off criteria. — Liaises and arbitrates when there are conflicts in the definition of interfaces or their management. — Reviews and judges the tailoring of enterprise-level acquisition and supply processes and associated work products to mitigate supply chain risks. — Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software. — Ensures that operational procedures and diagnostics for products/system are current, accessible, and well understood. — Influences key stakeholders within the enterprise to support and maintain the technical cyber capability and strategy of the enterprise.	

Work role: Cyber System/Product Architecture Specialist	Career stage
Functions: Ensures that the stakeholder security requirements necessary to protect the organisation's mission and business processes are adequately addressed in all aspects of product/system architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.	**Lead Practitioner**
Indicative skills: — Leads the application of cyber engineering principles to the design, development operation and maintenance of products/systems. — Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. — Contributes to development of information security policy, standards, and guidelines. — Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security and recommends appropriate control improvements. — Develops new architectures that mitigate the risks posed by new technologies and business practices. — Develops and communicates corporate information security policy, standards, and guidelines. — Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards, and guidelines. — Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits, and risks. — Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts. — Develops models and plans to drive the execution of the business strategy, taking advantage of opportunities to improve business performance. — Contributes to creating and reviewing a systems capability strategy which meets the business's strategic requirements. — Determines requirements and specifies effective business processes, through improvements in technology, information or data practices, organisation, roles, procedures, and equipment. — Leads the development of solution architectures in specific business, infrastructure, or functional areas. — Leads the preparation of technical plans and ensures that appropriate technical resources are made available. Ensures that appropriate tools and methods are available, understood and employed in architecture development. — Provides technical guidance and governance on solution development and integration. Evaluates requests for changes and deviations from specifications and recommends actions. — Ensures that relevant technical strategies, policies, standards, and practices (including security) are applied correctly. — Plans and drives scoping, requirements definition and prioritisation activities for large, complex initiatives. — Selects, adopts, and adapts appropriate requirements definition and management methods, tools, and techniques. Contributes to the development of organisational methods and standards for requirements management. — Obtains input from, and agreement to requirements from a diverse range of stakeholders. Negotiates with stakeholders to manage competing priorities and conflicts. — Establishes requirements baselines. Ensures changes to requirements are investigated and managed. — Reviews and judges the tailoring of enterprise-level system architectural design processes to meet the needs of a project. — Demonstrates a full understanding of architectural design and functional analysis techniques and their appropriateness, given the levels of complexity of the system of interest. — Reviews and judges the suitability of architecture designs and associated analyses. — Realises systems using a model that comprises a complete, coherent, and consistent architectural design. — Coaches new and experienced practitioners in system architecture design.	

Work role: Cyber System/Product Maintenance Specialist	Career stage
Functions: Leads maintenance and administration efforts for products/systems by utilising their strong understanding of the products/systems and the cyber security environment in which they operate. Develop and/or deploy mitigation techniques to effectively defend against cyber threats and vulnerabilities.	**Lead Practitioner**
Indicative skills: — Expertly applies cyber engineering principles to the maintenance of products/systems under management. — Ensures that appropriate action is taken to anticipate, investigate and resolve problems in systems and services. — Ensures that such problems are fully documented within the relevant reporting systems. — Enables development of problem solutions. Coordinates the implementation of agreed remedies and preventative measures. — Analyses patterns and trends and improves problem management processes. — Monitors the application and compliance of security operations procedures. — Reviews actual or potential security breaches and vulnerabilities and ensures that they are promptly and thoroughly investigated. Recommends actions and appropriate control improvements. — Ensures that security records are accurate and complete and that requests for support are dealt with according to agreed procedures. — Contributes to the creation and maintenance of policy, standards, procedures, and documentation for security. — Plans and manages vulnerability assessment activities within the organisation. — Evaluates and selects, reviews vulnerability assessment tools and techniques. — Provides expert advice and guidance to support the adoption of agreed approaches. — Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. — Ensures that system software is provisioned and configured to facilitate the achievement of service objectives. — Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software. — Investigates and coordinates the resolution of potential and actual service problems. — Ensures that operational procedures and diagnostics for system software are current, accessible, and well understood. — Drafts and maintains procedures and documentation for network support and operation. — Makes a significant contribution to the investigation, diagnosis, and resolution of network problems. — Ensures that all requests for support are dealt with according to set standards and procedures. — Takes responsibility for installation and/or decommissioning projects. — Provides effective team leadership, including information flow to and from the customer during project work. — Develops and implements quality plans and method statements. — Monitors the effectiveness of installations and ensures that appropriate recommendations for change are made. — Provides technical leadership to optimise the performance of IT infrastructure. — Investigates and manages the adoption of tools, techniques, and processes (including automation) for the management of systems and services. — Oversees the planning, installation, maintenance and acceptance of new and updated infrastructure components and infrastructure-based services. Aligns to service expectations, security requirements and other quality standards. — Ensures that operational procedures and documentation are fit for purpose and kept up to date. Ensures that operational issues are identified, recorded, monitored, and resolved. Provides appropriate status and other reports to specialists, users, and managers. — Recognised, within the enterprise, as an authority in maintenance, and support, contributing to best practice. — Defines and documents enterprise-level policies, procedures, guidance and best practice for operation and support, including associated tools. — Reviews and judges the tailoring of enterprise-level operation and support processes. — Applies advanced practices to the support of the system/product or service. — Assesses potential technology upgrades for a system, product or service and evaluates cost-benefit ratio for upgrading the design solution. — Leads support activities for a system, product, or service in operation. — identifies and executes plans for the disposal of a system, product, or service at end-of-life. — Influences key stakeholders to address identified enterprise-level system, product or service operation, maintenance, and support issues. — Coaches new and experienced practitioners in system, product or service operation, maintenance, and support.	

Work role: Cyber System/Product Manager	Career stage
Functions: Lead the efforts required to sustain operation and support of a system/product over time, especially as the result of failures, performance issues, evolving cyber threats, evolving needs, obsolescence, and technology changes and includes disposal of the system and its components when they reach end of life.	**Practitioner**
Indicative skills: — Applies cyber engineering principles to the products/systems they manage. — Defines governing operation and support plans, processes and appropriate tools and uses these to monitor and control system/product or service operation, maintenance, and support activities. — Develops and implements system, product or service operation, maintenance and support plans based upon standards and corporate processes. — Determines data to be collected to assess system, product, or service operational performance. — Assesses system failures or performance issues and initiates design change proposals to rectify failures. — Identifies system elements approaching obsolescence and conducts studies to identify suitable replacements. — Monitors and addresses changes to system operational environment or external interfaces. — Ensures technical support data (e.g., procedures, guidelines, checklists, training, and maintenance materials) remain current. — Guides supervised practitioners in system, product or service operation, and support. — Collates and analyses catalogues of information and technology assets for vulnerability assessment. — Performs vulnerability assessments and business impact analysis for medium complexity information systems. — Contributes to selection and deployment of vulnerability assessment tools and techniques. — Monitors system software metrics and adjusts configurations for optimum availability and performance. — Reviews system software updates and identifies those that merit action. — Configures system software for required functionality and performance. — Investigates and resolves system software problems, requesting action from supplier if required.	

Work role: Cyber Engineering Manager	Career stage
Functions: Manage cyber engineering activities across a range of small products/systems or a complex product/system across an enterprise.	**Practitioner**
Indicative skills: — Applies cyber engineering principles across the design development operation and maintenance of a range of products/system across an enterprise. — Defines governing operation and support plans, processes and appropriate tools and uses these to monitor and control system/product or service operation, maintenance, and support activities of allocated systems/products. — Develops and implements system, product or service operation, maintenance and support plans based upon standards and corporate processes. — Determines data to be collected to assess system, product, or service operational performance. — Assesses systems failures or performance issues and initiates design change proposals to rectify failures. — Identifies system elements approaching obsolescence and conducts studies to identify suitable replacements. — Monitors and addresses changes to system operational environment or external interfaces. — Ensures technical support data (e.g., procedures, guidelines, checklists, training, and maintenance materials) remain current. — Guides supervised practitioners in system, product or service operation, and support. — Collates and analyses catalogues of information and technology assets for vulnerability assessment. — Performs vulnerability assessments and business impact analysis for medium complexity information systems. — Contributes to selection and deployment of vulnerability assessment tools and techniques. — Monitors system software metrics and adjusts configurations for optimum availability and performance. — Reviews system software updates and identifies those that merit action. — Configures system software for required functionality and performance. — Investigates and resolves system software problems, requesting action from supplier if required.	

Work role: Cyber Systems Developer	Career stage
Functions: Designs, develops, tests, and evaluates information/operational system security throughout the systems development lifecycle.	**Supervised Practitioner**
Indicative skills: — Assists with the application of cyber engineering principles to development efforts. — Uses a governing process and appropriate tools to manage and control their own cyber engineering activities. — Identifies design attributes and describes how they influence the design. — Supports the selection and balancing of design attributes in support of cyber engineering needs. — Assists specialists in ensuring that the design attributes are addressed. — Assists with trade-off activities involving conflicting demands from design specialisms. — Assists with activities characterising the operational environment in support of cyber engineering activities. — Assists with trade studies which determine and characterise specialty characteristics of proposed solutions. — Identifies the relationships between the integration of specialisms within their project and provides examples. — Assists with the identification of constraints placed on the system because of the needs of design specialisms. — Uses techniques and tools to ensure delivery of designs meeting specialty needs. — Applies and maintains specific security controls as required by organisational policy and local risk assessments. — Communicates security risks and issues to business managers and others. Performs basic risk assessments for small information systems. — Contributes to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systems configurations in compliance with intended architectures. — Supports investigation of suspected attacks and security breaches. — Follows standard approaches to performs basic vulnerability assessments for small information systems. — Supports creation of catalogues of information and technology assets for vulnerability assessment.	

Work role: Cyber Systems Analyst	Career stage
Functions: Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.	**Supervised Practitioner**
Indicative skills: — Assists with the application of cyber engineering principles. — Applies and maintains specific security controls as required by organisational policy and local risk assessments. — Performs basic risk assessments for small information systems. — Contributes to the identification of risks that arise from potential technical solution architectures. — Suggests alternate solutions or countermeasures to mitigate risks. — Defines secure systems configurations in compliance with intended architectures. — Follows standard approaches to performs basic vulnerability assessments for small information systems. — Supports creation of catalogues of assets for vulnerability assessment. — Designs test cases and test scripts under own direction, mapping back to pre-determined criteria, recording and reporting test outcomes. — Participates in requirement, design, and specification reviews, and uses this information to design test plans and test conditions. — Applies agreed standards to specify and perform manual and automated testing. Automates testing tasks and builds test coverage through existing or new infrastructure. — Analyses and reports on test activities, results, issues, and risks.	

Work role: Engineering Design, systems/product development and maintenance roles	Career stage
Functions: Undertakes system design/product development in field of engineering consistent with accredited qualifications. Undertakes maintenance of systems/products.	**Supervised Practitioner**
Indicative skills: — Assists with the application of cyber engineering principles. — Uses a governing process and appropriate tools to manage and control their own specialty engineering activities. — Identifies design attributes and describes how they influence the design. — Supports the selection and balancing of design attributes in support of specialty engineering needs. — Assists specialists in ensuring that the design attributes are addressed. — Assists with trade-off activities involving conflicting demands from design specialisms. — Assists with activities characterising the operational environment in support of specialty engineering activities. — Assists with trade studies which determine and characterise specialty characteristics of proposed solutions. — Identifies the relationships between the integration of specialisms within their project and provides examples. — Assists with the identification of constraints placed on the system because of the needs of design specialisms. — Uses techniques and tools to ensure delivery of designs meeting specialty needs. — Uses a governing process and appropriate tools to plan and control their own system, product or service operations, maintenance, and support-related activities. — identifies and supports collection and review of operational data in order to assess system, product, or service performance. — Assists with the assessment of system failures or performance issues and the preparation of design change to rectify such failures. — Assists with the assessment of evolving user need, including activities assessing the feasibility of updates in response to the changed need. — Assists with assessments of new technologies and helps conduct studies to identify possible system updates. — Assists with assessments of components approaching obsolescence and helps conducts studies to identify suitable replacements. — Assists with updates of technical data (e.g., procedures, guidelines, checklists, training, and maintenance materials) to ensure they are current. — Identifies potential changes to system operational environment or external interfaces.	

Work role: Chief Information Security Officer	Career stage
Functions: **The establishment and oversight of an organisation's approach to the secure use of information, digital services, and associated technology.** **Includes responsibility for:** — Cyber risk management and incident response. — Provision of secure digital services. — Levels of service and service quality which meet current and future business requirements. — Policies and practices for conformance with mandatory legislation and regulations. — Strategic plans for technology to enable the organisation's business strategy; transparent decision making, leading to justification for investment, with appropriate balance between stakeholder benefits, opportunities, costs, and risks.	**Executive**
Indicative skills: — Recognised as an authority in cyber engineering principles and their application to systems design, operation, and maintenance. — Contributes to best practice in the application of cyber engineering principles to systems design operation and maintenance. — Influences key stakeholders beyond the enterprise boundary to support cyber engineering. — Has skills to direct information security governance activities and set the information security policy and strategy for an enterprise — Information security governance activities — Designing, implement and manage information security policies, procedures, processes, and controls required to manage information security at an enterprise level. — Advice to others so that an organisation's regulatory, legal, environmental, and operational information security requirements are complied with. — Direct operational information security management activities manage all aspects of secure operations and service delivery. — Be fully accountable for operational security policies and standards and coordinate information security operations activities across the organisation.	

Work role: Head Cyber Operations	Career stage
Functions: **Leads use of:** — Defensive measures and information collected from a variety of sources to identify, analyse, and report events that occur or might occur within the network to protect information, information systems, and networks from threats. — Testing, implementing, deployment, maintenance, reviews, and administration of the infrastructure hardware and software that are required to effectively manage the computer network defence service provider network and resources. — Monitors network to actively remediate unauthorised activities.	**Expert**
Indicative skills: — Develop content for cyber defence tools. — Characterise and analyse network traffic to identify anomalous activity and potential threats to network resources. — Coordinate with enterprise-wide cyber defence staff to validate network alerts. — Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. — Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment. — Perform cyber defence trend analysis and reporting. — Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. — Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. — Plan and recommend modifications or adjustments based on exercise results or system environment. — Provide daily summary reports of network events and activity relevant to cyber defence practices. — Receive and analyse network alerts from various sources within the enterprise and determine possible causes of such alerts. — Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities. — Use cyber defence tools for continual monitoring and analysis of system activity to identify malicious activity. — Analyse identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information. — Determine tactics, techniques, and procedures (TTPs) for intrusion sets. — Examine network topologies to understand data flows through the network. — Recommend computing environment vulnerability corrections. — Identify and analyse anomalies in network traffic using metadata. — Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings). — Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools. — Isolate and remove malware. — Identify applications and operating systems of a network device based on network traffic. — Reconstruct a malicious attack or activity based off network traffic. — Identify network mapping and operating system (OS) fingerprinting activities. — Assist in the construction of signatures which can be implemented on cyber defence network tools in response to new or observed threats within the network environment or enclave. — Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organisation's cyber incident response plan. — Analyse and report organisational security posture trends. — Analyse and report system security posture trends. — Assess adequate access controls based on principles of least privilege and need-to-know. — Monitor external data sources (e.g., cyber defence vendor sites, computer emergency response teams, security focus) to maintain currency of cyber defence threat condition and determine which security issues may have an impact on the enterprise. — Assess and monitor cybersecurity related to system implementation and testing practices. — Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. — Work with stakeholders to resolve computer security incidents and vulnerability compliance. — Provide advice and input for disaster recovery, contingency, and continuity of operations plans.	

Work role: Penetration Tester (Security Tester)	Career stage
Functions: **Network or infrastructure security testing, involves assessing network devices, servers, and other network infrastructure services such as Domain Name Service (DNS) for security vulnerabilities. Application security testing generally refers to testing custom or commercial software applications for security vulnerabilities. Web application security testing is specifically focused on testing web applications and mobile application security testing is specifically focused on testing mobile applications.**	**Lead Practitioner/ Practitioner**
Indicative skills: — Carry out information security testing activities. — Conduct security testing to contribute to the determination of the level of resilience of an information system to information security threats and vulnerabilities. — Select, plan, and apply testing methods, including penetration testing. — Write and present testing report to client.	

Work role: Incident Responder	Career stage
Functions: **Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximise survival of life, preservation of property, and information security. Investigates and analyses all relevant response activities.**	**Lead Practitioner/ Practitioner**
Skills to support the following functions: — Coordinate and provide expert technical support to enterprise-wide cyber defence technicians to resolve cyber defence incidents. — Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. — Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security. — Perform cyber defence incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation. — Perform cyber defence trend analysis and reporting. — Perform initial, forensically sound collection of images and inspect to discern possible mitigation/ remediation on enterprise systems. — Perform real-time cyber defence incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable incident response teams (IRTs). — Receive and analyse network alerts from various sources within the enterprise and determine possible causes of such alerts. — Track and document cyber defence incidents from initial detection through final resolution. — Write and publish cyber defence techniques, guidance, and reports on incident findings to appropriate constituencies. — Employ approved defence-in-depth principles and practices (e.g., defence-in-multiple places, layered defences, security robustness). — Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defence incidents within the enterprise. — Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. — Coordinate with intelligence analysts to correlate threat assessment data. — Write and publish after action reviews. — Monitor external data sources (e.g., cyber defence vendor sites, computer emergency response Teams, Security Focus) to maintain currency of cyber defence threat condition and determine which security issues may have an impact on the enterprise. — Coordinate incident response functions.	

Work role: Incident Investigator	Career stage
Functions: When information security incidents occur, organisations must respond quickly and effectively to protect themselves from attack and limit the damage and scope of attacks. To do this, they need to establish incident response investigative teams and define the policies and standards relating to developing, operating, and improving incident management capabilities. May also mean: Detection of information security issues, including breaches in network security. Any issues identified can be reviewed and escalated to incident response teams. Intrusion detection uses a range of automated tools to monitor information systems and networks in real time, and intrusion analysis will interpret the alerts generated by those tools. This involves correlating information from a variety of sources and then determining whether the alert represents a security breach. If a security breach has been detected, this is then escalated to an incident response team, providing both notification of the breach and associated evidence that a breach has occurred	Lead Practitioner/ Practitioner
Indicative skills: — Carry out information security incident investigation and management activities. — Carry out incident management activities related to identifying, eliminating, and preventing potential and current information security threats. May need following: — Carry out information security intrusion detection and analysis activities. — Detect and analyse information security anomalies in information systems and network security systems. — Implementing the escalation processes to the incident response function — Communicate information on information security intrusions with — internal and external stakeholders.	

Work role: **Cyber Defence Analyst**	Career stage
Functions: Uses defensive measures and information collected from a variety of sources to identify, analyse, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.	Supervised Practitioner
Skills to support following functions: — Develop content for cyber defence tools. — Characterise and analyse network traffic to identify anomalous activity and potential threats to network resources. — Coordinate with enterprise-wide cyber defence staff to validate network alerts. — Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. — Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment. — Perform cyber defence trend analysis and reporting. — Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. — Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. — Plan and recommend modifications or adjustments based on exercise results or system environment. — Provide daily summary reports of network events and activity relevant to cyber defence practices. — Receive and analyse network alerts from various sources within the enterprise and determine possible causes of such alerts. — Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities. — Use cyber defence tools for continual monitoring and analysis of system activity to identify malicious activity. — Analyse identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information. — Determine tactics, techniques, and procedures (TTPs) for intrusion sets. — Examine network topologies to understand data flows through the network. — Recommend computing environment vulnerability corrections. — Identify and analyse anomalies in network traffic using metadata. — Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings). — Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools. — Isolate and remove malware. — Identify applications and operating systems of a network device based on network traffic. — Reconstruct a malicious attack or activity based off network traffic. — Identify network mapping and operating system (OS) fingerprinting activities. — Assist in the construction of signatures which can be implemented on cyber defence network tools in response to new or observed threats within the network environment or enclave. — Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organisation's cyber incident response plan. — Analyse and report organisational security posture trends. — Analyse and report system security posture trends. — Assess adequate access controls based on principles of least privilege and need-to-know. — Monitor external data sources (e.g., cyber defence vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defence threat condition and determine which security issues may have an impact on the enterprise. — Assess and monitor cybersecurity related to system implementation and testing practices. — Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. — Work with stakeholders to resolve computer security incidents and vulnerability compliance. — Provide advice and input for disaster recovery, contingency, and continuity of operations plans.	

Work role: Digital Forensics Analyst	Career stage
Functions: **Digital forensic examination procedures are used to uncover and interpret electronic data to aid the investigation of information security issues.** **The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information for reconstructing past events.** **The context is most often for usage of data in a court of law, though digital forensics can be used in other instances.**	**Supervised Practitioner**
Indicative skills: — Manage digital forensic examination activities. — Master analysis of large and complex information systems using tools to acquire and analyse systems, collect, and document evidence. — Lead all aspects of digital forensic examination. Including managing resources, activities, and deliverables. — Specify the policies and processes for undertaking digital forensic examinations to determine the nature of the issue and to identify those responsible, — Define and implement organisational policies and standards concerning digital forensic examination.	

Work role: Cyber Systems Analyst	Career stage
Functions: **Tests, implements, deploys, maintains, reviews, and administers the infra-structure hardware and software that are required to effectively manage the computer network defence service provider network and resources.** **Monitors network to actively remediate unauthorised activities.**	**Supervised Practitioner**
Skills to support following functions: — Coordinate with cyber defence analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialised cyber defence applications. — Perform system administration on specialised cyber defence applications and systems (e.g., antivirus, audit, and remediation) or virtual private network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration. — Assist in identifying, prioritising, and coordinating the protection of critical cyber defence infrastructure and key resources. — Build, install, configure, and test dedicated cyber defence hardware. — Assist in assessing the impact of implementing and sustaining a dedicated cyber defence infrastructure. — Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/ signatures, access controls, and configurations of platforms managed by service provider(s). — Create, edit, and manage network access control lists on specialised cyber defence systems (e.g., firewalls and intrusion prevention systems). — Identify potential conflicts with implementation of any cyber defence tools (e.g., tool and signature testing and optimisation). — Implement risk management framework (RMF)/security assessment and authorisation (SA&A) requirements for dedicated cyber defence systems within the enterprise, and document and maintain records for them.	

APPENDIX 1

Confidentiality, integrity, availability and safety definitions and explanatory notes

Confidentiality – The assurance that information is disclosed only to authorised entities.

Confidentiality refers to the principle of need to know a system should not disclose information, data or controls to a user that doesn't need that information or control. For example, standard users should not be able to view a person's credit card or Medicare details when accessing a HR system. Another example would be to not publish personal data to public dashboards in control centres. Users should not be able to control functions or processes that they are not authorised to control.

Integrity – The assurance that information has been created, amended, or deleted only by authorised individuals.

Integrity refers to truth in data, systems, and processes. This include ensuring that the data is read correctly from sensors and ensuring that the data is not modified during transit or while stored. An example of integrity is the retention of log data relating to manufacturing ballistic products. The cooking process logs are to be retained for 10 years if this data is modified and a product is compromised then the supplier may be liable.

Availability – The assurance that systems and information are accessible and useable by authorised entities when required.

Availability refers to information and systems being able to be accessed if and where they need to be. Often this is seen through high availability design where cyber systems are designed with redundancy. This can also be reflected upon as business continuity having multiple copies of critical log data; or having access to critical control systems from multiple sites/locations but not the entire internet may be another example.

Safety – The state of being safe and protected from danger or harm.

Safety refers to the interaction between cyber systems and the physical world. If a compromised cyber system can result in real world impacts, then there is a safety consideration that must be assessed. An example of this would be the active interception of machine control code where the control code is modified to report incorrect location. This could result in the machine crashing into a person or other system causing death or significant damage with lasting financial and legal impacts. Similarly, if a corrupted signal was to enable an uncontrolled opening of dam gates, there could be profound consequences, including substantial environmental harm to ecological habitats, potential damage to commercial properties, and the risk of flooding in inhabited areas. Another example in a medical context is where limited availability of data may impact patient safety by limiting access to relevant critical information and affecting subsequent clinical decisions, or patient safety where critical alerts are not received, or medical equipment is controlled by an attacker.