Australian Government
Australian Signals Directorate

# ASD CYBER SKILLS FRAMEWORK

ASD

**For enquiries please contact asd.assist@defence.gov.au**

# CONTENTS

# ASD CYBER SKILLS FRAMEWORK

## HISTORY OF THE ASD CYBER SKILLS FRAMEWORK

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

The ASD Cyber Skills Framework v.2.0 captures updates from the frameworks that support it: Skills Framework for the Information Age 7 (SFIA 7) and the Chartered Institute for Information Security (CIISec) Framework v.2.4 (formerly the Institute for Information Security Professionals).

The ASD Cyber Skills Framework v.2.0 introduces additional elements, as follows:

- Role definitions and expectations
- Digital Career Pathways
- Learning and Development pathways
- National Initiative for Cybersecurity Education (NICE) work roles
- Australian Defence Force (ADF) professional framework.

## The context

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

## ASD Cyber Skills Framework

The ASD Cyber Skills Framework defines the roles, capabilities and skills proficiencies that are essential to cyber missions, and that can be used in both the security and offensive contexts.

The ASD Cyber Skills Framework enables targeted recruitment of cyber specialists, provides a development pathway for current and future cyber staff and aligns skills, knowledge and attributes with national and international industry standards.

The ASD Cyber Skills Framework is relevant to wider government, industry and academia which can be implemented and used as a tool for understanding and profiling cyber skills in any organisation.

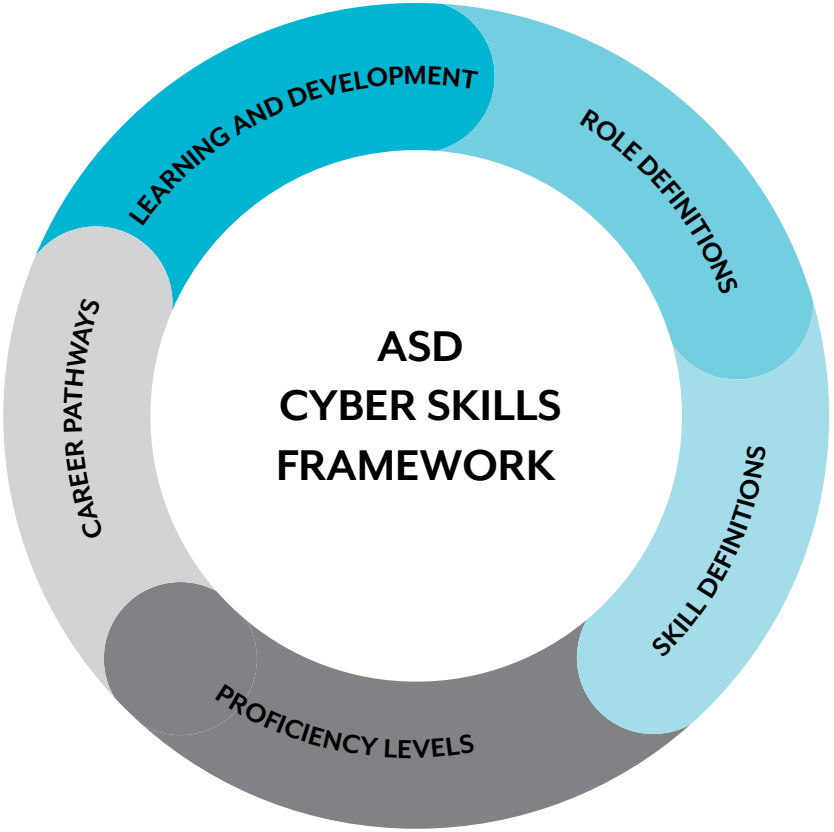
## The guiding document

The ASD Cyber Skills Framework is designed to be used as a guiding document and its different elements can be implemented as required to meet organisational and workforce goals and objectives.

## The foundation of the ASD Cyber Skills Framework

The foundation of the ASD Cyber Skills Framework is built on the following core elements:

- 9 Cyber role definitions
- 9 Capability and skill definitions
- 6 Proficiency levels
- 4 Career pathways
- 1 Learning and development pathway (example)



## The underlying frameworks

From 2009, ASD utilised an internal framework known as the ASD Streams. The ASD Streams defined the specialist professional capabilities in a broad occupational group that related to a skill area. In 2018, a review of the ASD Stream for Cyber and Information Security was undertaken in order to assess the relevance of the defined roles, capabilities, skills and proficiency levels, and the way in which these related to current industry and government frameworks and standards.

As a result of this review, the ASD Cyber Skills Framework was formed: nine roles were defined using a set of underlying core capabilities and related skills and proficiency levels. These concepts were developed from three core frameworks: Chartered Institute of Information Security (CIISec) Skills Framework; Skills Framework for the Information Age (SFIA); and Integrated Leadership System (ILS).

CIISec is the leading information security professional industry body in the United Kingdom. ASD uses the CIISec Skills Framework to define the majority of cyber capabilities and skills within the ASD Cyber Skills Framework. The CIISec Skills Framework was also essential in establishing the skill proficiency levels adopted in the ASD Cyber Skills Framework.

ASD, along with many other government departments and ICT industry stakeholders, implements SFIA as a tool to assess technical ICT proficiencies. SFIA is considered a leading framework to describe capabilities and skill proficiencies for information technology professionals. SFIA is used to define a number of core ICT capabilities and skills within the ASD Cyber Skills Framework.

The ILS is the Australian government-approved standard for personnel capability development. The ILS is adopted for all skills relating to the Management, Leadership, Business, and Communication capability within the ASD Cyber Skills Framework.

### What terminology is used in the framework?

**Capability: Broad grouping of occupational skills**

*Example: Incident management, investigation and digital forensics*

**Skills: Expertise or aptitude in a capability**

*Example: Intrusion Detection and Analysis*

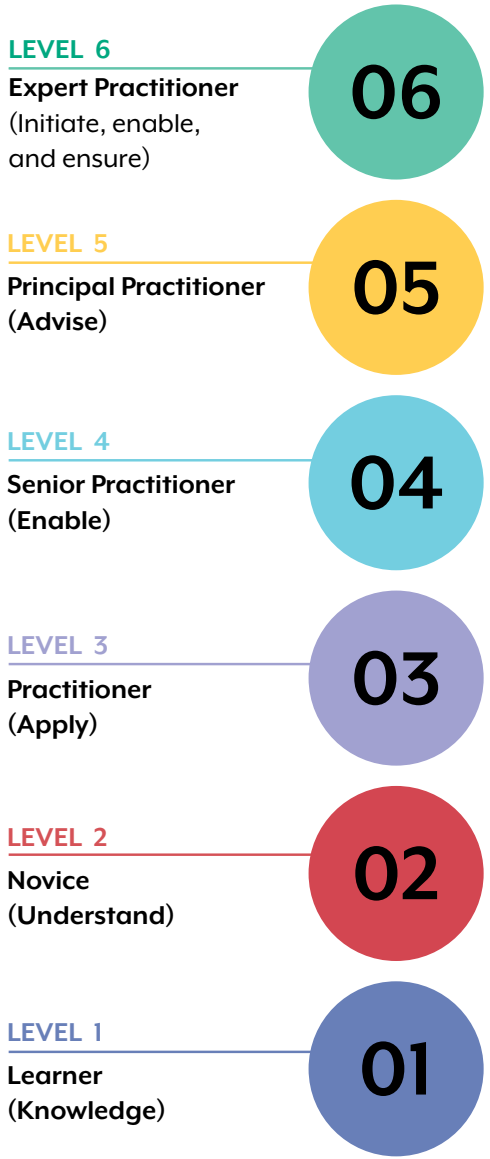
**Role: A job, position or function**

*Example: Incident Responder*

## Proficiency levels

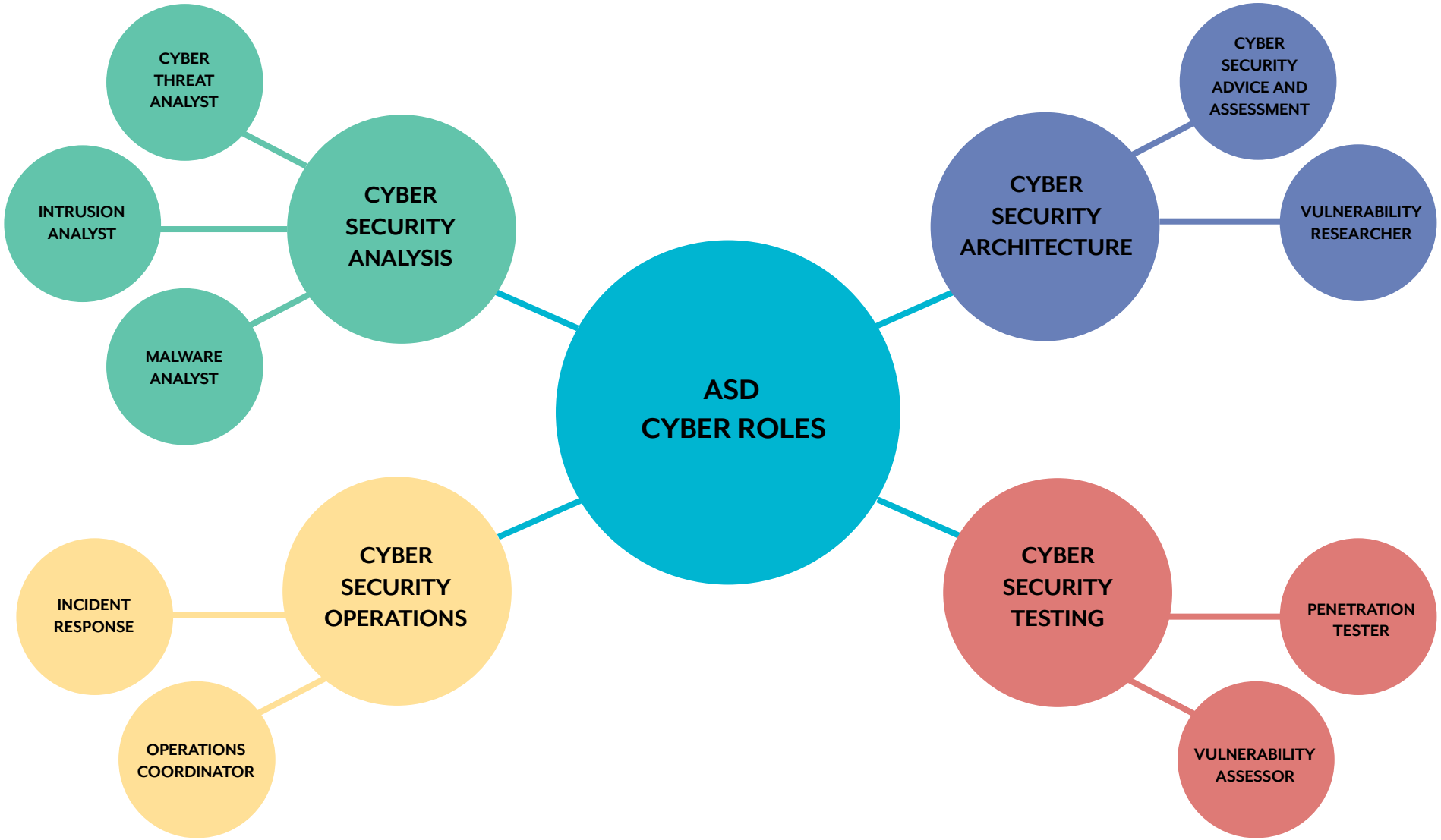
The table below displays the way in which the ASD Cyber Skills Framework maps the proficiency levels defined in ASD Streams, CIISec Skills Framework, and SFIA.

| ASD STREAMS | CIISec SKILLS FRAMEWORK | SFIA | NEW: ASD CYBER SKILLS FRAMEWORK |
|---|---|---|---|
| | Level 1 (Knowledge) | Level 1 (Follow) | Level 1 (Learner) |
| Level 1 (Novice) | Level 2 (Knowledge and Understanding) | Level 2 (Assist) | Level 2 (Novice) |
| | Level 3 (Apply) | Level 3 (Apply) | Level 3 (Practitioner) |
| Level 2 (Practitioner) | Level 4 (Enable) | Level 4 (Enable) | Level 4 (Senior Practitioner) |
| Level 3 (Expert) | Level 5 (Advise) | Level 5 (Advise, Ensure) | Level 5 (Principal Practitioner) |
| Level 4 (Leader) | Level 6 (Expert) | Level 6 (Initiate, Influence) | Level 6 (Expert Practitioner) |
| | | Level 7 (Set Strategy, Inspire, Mobilise) | |



# ASD Cyber Roles

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



# Core Capabilities

Nine core capabilities that are used to group related skills have been defined in the ASD Cyber Skills Framework. The capabilities and the related industry framework that informed them are:

1. Information Security Governance and Strategy
   *CIISec Skills Framework Section A: Information Security Governance and Management*
   - 1.1 A1: Governance
   - 1.2 A2: Policy and Standards
   - 1.3 A3: Information Security Strategy
   - 1.4 A5: Behavioural Change
   - 1.5 A6: Legal and Regulatory Environment and Compliance
   - 1.6 A7: Third Party Management

2. Threat Assessment and Information Risk Management
   *CIISec Skills Framework Section B: Threat Assessment and Information Risk Management*
   - 2.1 B1: Threat Intelligence, Assessment and Threat Modelling
   - 2.2 B2: Risk Assessment
   - 2.3 B3: Information Risk Management

3. Systems Development and Implementation
   *SFIA: Systems Development*
   - 3.1 DLMG: Systems Development Management
   - 3.2 DESN: Systems Design
   - 3.3 SWDN: Software Design
   - 3.4 PROG: Programming/Software Development

4. Assurance: Audit, Compliance and Testing
   *CIISec Skills Framework Section D: Assurance: Audit, Compliance and Testing*
   - 4.1 D1: Internal and Statutory Audit
   - 4.2 D2: Compliance Monitoring and Controls Testing
   - 4.3 D3: Security Evaluation and Functionality Testing

   *SFIA: Service Operation*
   - 4.4 PENT: Penetration Testing

5. Operational Security Management
   *CIISec Skills Framework Section E: Operational Security Management*
   - 5.1 E1: Secure Operations Management
   - 5.2 E2: Secure Operations and Service Delivery

6. Incident Management, Investigation and Forensics
   *CIISec Skills Framework Section F: Incident Management, Investigation and Digital Forensics*
   - 6.1 F1: Intrusion Detection and Analysis
   - 6.2 F2: Incident Management, Incident Investigation and Response

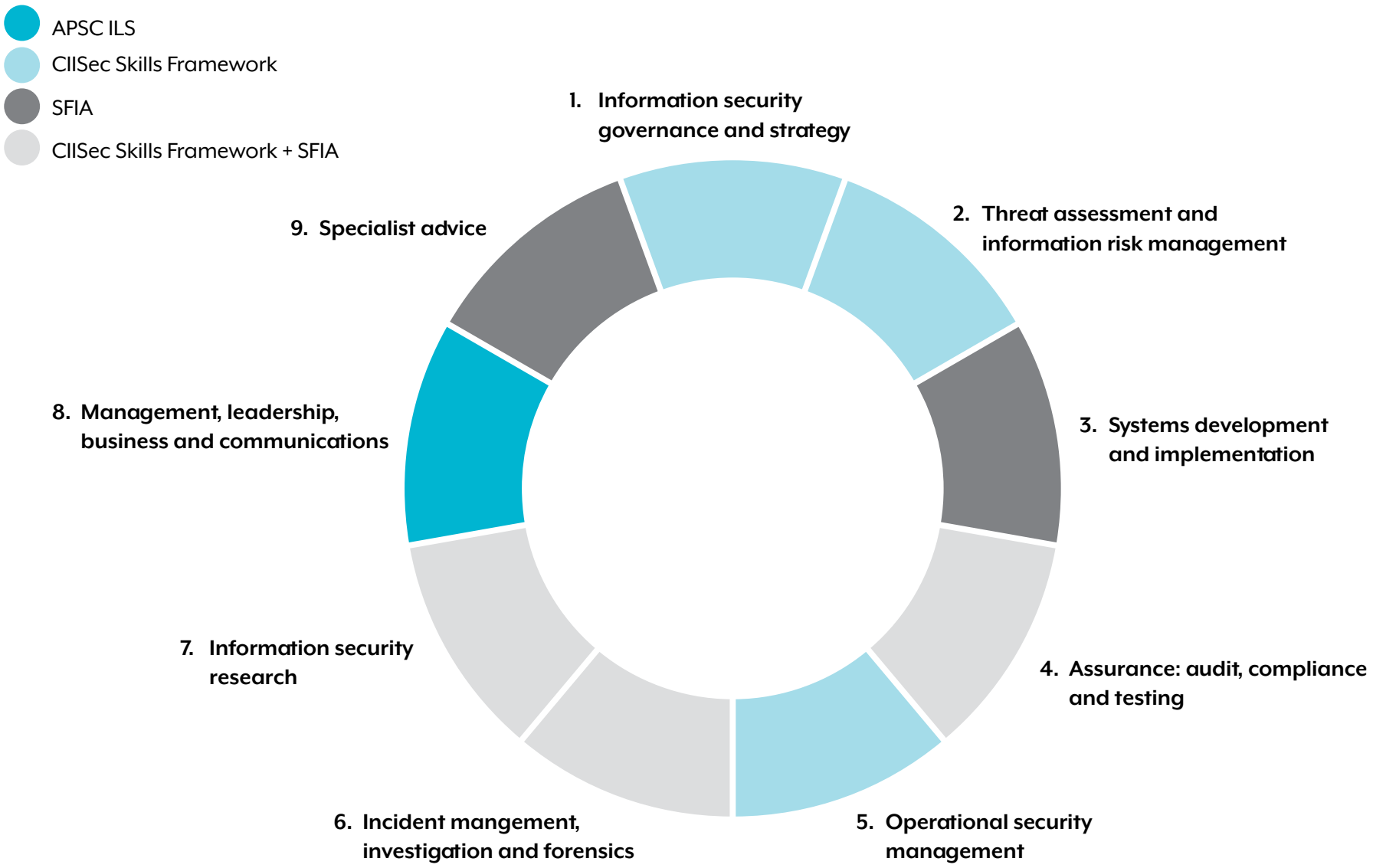
   *SFIA: Quality and Conformance*
   - 6.3 DGSF: Digital Forensics

7. Information Security Research
   *SFIA: Business Strategy and Planning*
   - 7.1 RSCH: Research

   *CIISec Skills Framework Section I: Information Security Research*
   - 7.2 I2: Applied Research

8. Management, Leadership, Business and Communications
   *Australian Public Service Integrated Leadership System*

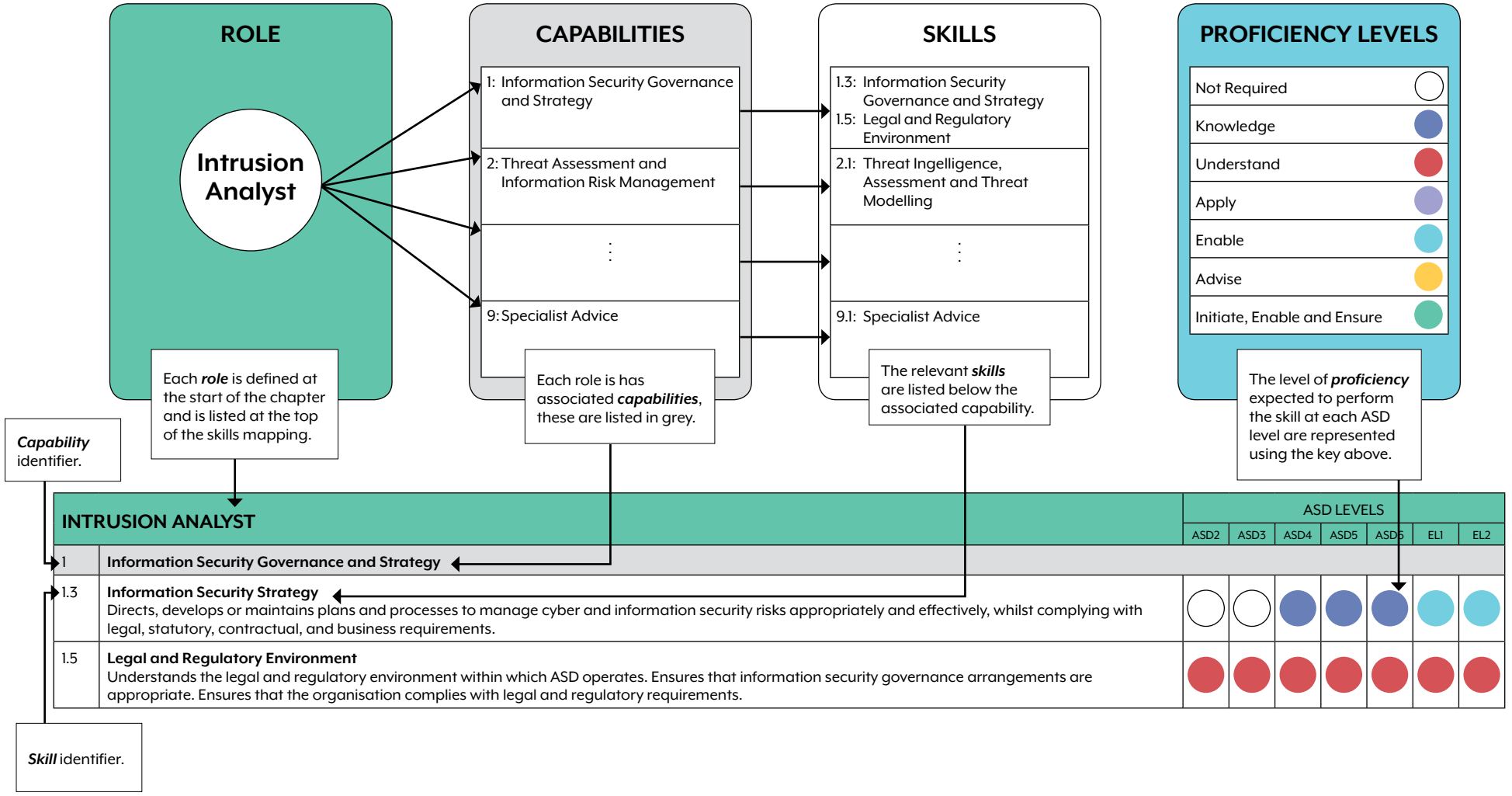
9. Specialist Advice
   *SFIA: Advice and Guidance*
   - 9.1 TECH: Specialist Advice


APSC ILS
CIISec Skills Framework
SFIA
CIISec Skills Framework + SFIA
1. Information security governance and strategy
2. Threat assessment and information risk management
3. Systems development and implementation
4. Assurance: audit, compliance and testing
5. Operational security management
6. Incident mangement, investigation and forensics
7. Information security research
8. Management, leadership, business and communications
9. Specialist advice

# ASD CYBER ROLES, CAPABILITIES, SKILLS AND PROFICIENCY LEVELS

# ASD CYBER SKILLS FRAMEWORK GUIDE

To understand how to properly use and apply the ASD Cyber Skills Framework, each defined ***role*** has the required ***capabilities*** and associated ***skills*** listed. The level of ***proficiency*** required to perform that skill for that role is defined against the ASD level using the indicators on the right (levels increase from most junior to most senior; ASD 2 through to Executive Level 2).



# CYBER SECURITY ANALYSIS ROLES

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

| CYBER THREAT ANALYST | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 1 | **Information Security Governance and Strategy** | | | | | | | |
| 1.1 | **Governance**<br>Directs, oversees, designs, implements or operates within the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage cyber and information security at an organisational level; thereby supporting ASD's immediate and future regulatory, legal, risk, environmental and operational requirements and ensuring compliance with those requirements. | ○ | ○ | Apply | Apply | Apply | Apply | Apply |
| 1.5 | **Legal and Regulatory Environment**<br>Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements. | Understand | Understand | Understand | Understand | Understand | Understand | Understand |
| 2 | **Threat Assessment and Information Risk Management** | | | | | | | |
| 2.1 | **Threat Intelligence, Assessment and Threat Modelling**<br>Assesses and validates information from several sources on current and potential cyber and information security threats to the business, analysing trends and highlighting information security issues relevant to ASD. Processes, collates and exploits data, taking into account its relevance and reliability to develop and maintain 'situational awareness'. Predicts and prioritises threats to ASD, Australian government agencies, critical infrastructure and businesses, and their methods of attack. Analyses the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities. Predicts and prioritises threats to an organisation and their methods of attack. Uses human factor analysis in the assessment of threats. Prepares and disseminates intelligence reports, providing threat indicators and warnings. | ○ | ○ | Apply | Enable | Enable | Advise | Initiate, Enable and Ensure |
| 2.2 | **Risk Assessment**<br>Identifies and assesses information assets. Uses this information and relevant threat assessments, business impacts, business benefits and costs to conduct risk assessments and identify and assess potential vulnerabilities. | ○ | ○ | Apply | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 2.3 | **Information Risk Management**<br>Develops cyber and information security risk management strategies and controls, taking into account business needs and risk assessments, and balancing technical, physical, procedural and personnel controls. | ○ | ○ | Understand | Understand | Understand | Understand | Understand |
| 6 | **Incident Management, Investigation and Forensics** | | | | | | | |
| 6.1 | **Intrusion Detection and Analysis**<br>Monitors network and system activity to identify potential intrusion or other anomalous behaviour. Analyses the information and initiates an appropriate response, escalating as necessary. Uses security analytics, including the outputs from intelligence analysis, predictive research and root cause analysis in order to search for and detect potential breaches or identify recognised indicators and warnings. Monitors, collates and filters external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes. Ensures that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available. Produces warning material in a manner that is both timely and intelligible to the target audience(s). | ○ | ○ | Apply | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 7 | **Information Security Research** | | | | | | | |
| 7.1 | **Research**<br>The systematic creation of new knowledge by data gathering, innovation, experimentation, evaluation and dissemination. The determination of research goals and the method by which the research will be conducted. The active participation in a community of researchers; communicating formally and informally through digital media, conferences, journals, books and seminars. | ○ | ○ | Apply | Apply | Enable | Enable | Enable |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

| CYBER THREAT ANALYST | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 8 | **Management, Leadership, Business and Communications** | | | | | | | |
| 8.1 | **Supports Strategic Direction**<br>Supports shared purpose and direction; thinks strategically; harnesses information and opportunities; shows judgement, intelligence and common-sense. | ● | ● | ● | ● | ● | ● | ● |
| 8.2 | **Achieves Results**<br>Builds ASD and the ACSC's capability and responsiveness by identifying, applying and building professional expertise; responds positively to change; takes responsibility for managing work projects to achieve results. | ● | ● | ● | ● | ● | ● | ● |
| 8.3 | **Supports Productive Working Relationships**<br>Nurtures internal relationships; listens to, understands and recognises the needs of others; values individual differences and diversity; shares learning and supports others. | ● | ● | ● | ● | ● | ● | ● |
| 8.4 | **Displays Personal Drive and Integrity**<br>Demonstrates public service professionalism and probity; engages with risk and shows personal courage; commits to action; promotes and adopts a positive and balanced approach to work; demonstrates self-awareness and a commitment to personal development. | ● | ● | ● | ● | ● | ● | ● |
| 8.5 | **Communicates with Influence**<br>Communicates clearly; listens, understands and adapts to audience; negotiates confidently. | ● | ● | ● | ● | ● | ● | ● |
| 9 | **Specialist Advice** | | | | | | | |
| 9.1 | **Specialist Advice**<br>The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice. | ○ | ○ | ○ | ○ | ○ | ● | ● |

○ Not required ● Knowledge ● Understand ● Apply ● Enable ● Advise ● Initiate, Enable and Ensure

| INTRUSION ANALYST | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 1 | **Information Security Governance and Strategy** | | | | | | | |
| 1.3 | **Information Security Strategy**<br>Directs, develops or maintains plans and processes to manage cyber and information security risks appropriately and effectively, whilst complying with legal, statutory, contractual, and business requirements. | ○ | ○ | Knowledge | Knowledge | Knowledge | Enable | Enable |
| 1.5 | **Legal and Regulatory Environment**<br>Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements. | Understand | Understand | Understand | Understand | Understand | Understand | Understand |
| 2 | **Threat Assessment and Information Risk Management** | | | | | | | |
| 2.1 | **Threat Intelligence, Assessment and Threat Modelling**<br>Assesses and validates information from several sources on current and potential cyber and information security threats to the business, analysing trends and highlighting information security issues relevant to ASD. Processes, collates and exploits data, taking into account its relevance and reliability to develop and maintain 'situational awareness'. Predicts and prioritises threats to ASD, Australian government agencies, critical infrastructure and businesses, and their methods of attack. Analyses the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities. Predicts and prioritises threats to an organisation and their methods of attack. Uses human factor analysis in the assessment of threats. Prepares and disseminates intelligence reports, providing threat indicators and warnings. | ○ | ○ | Apply | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 4 | **Assurance: Audit, Compliance and Testing** | | | | | | | |
| 4.4 | **Penetration Testing**<br>The assessment of organisational vulnerabilities through the design and execution of penetration tests that demonstrate how an adversary can either subvert the organisation's security goals or achieve specific adversarial objectives. Penetration testing may be a stand-alone activity or an aspect of acceptance testing prior to an approval to operate. The identification of deeper insights into the business risks of various vulnerabilities. | ○ | ○ | Apply | Apply | Apply | Apply | Apply |
| 6 | **Incident Management, Investigation and Forensics** | | | | | | | |
| 6.1 | **Intrusion Detection and Analysis**<br>Monitors network and system activity to identify potential intrusion or other anomalous behaviour. Analyses the information and initiates an appropriate response, escalating as necessary. Uses security analytics, including the outputs from intelligence analysis, predictive research and root cause analysis in order to search for and detect potential breaches or identify recognised indicators and warnings. Monitors, collates and filters external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes. Ensures that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available. Produces warning material in a manner that is both timely and intelligible to the target audience(s). | ○ | ○ | Apply | Enable | Advise | Initiate, Enable and Ensure | Initiate, Enable and Ensure |
| 6.2 | **Incident Management, Incident Investigation and Response**<br>Engages with the overall organisation Incident Management process to ensure that cyber security incidents are handled appropriately. Defines and implements processes and procedures for detecting and investigating cyber security incidents. Establishes and maintains Incident Response teams to respond to and mitigate the risks of cyber security incidents. Working within the legal constraints imposed by the jurisdictions in which ASD carries out investigations of cyber security incidents using all relevant sources of information. Assesses the need for forensic activity, and coordinates the activities of specialist forensic personnel within the overall response activities, engaging with the relevant organisational processes to ensure that forensic services are deployed appropriately. Provides a full information security investigation capability where third parties, managed service providers, etc., are involved. | ○ | ○ | ○ | ○ | Apply | Enable | Enable |
| 6.3 | **Forensics**<br>The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings, including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations. | ○ | ○ | Apply | Apply | Apply | Apply | Apply |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

| INTRUSION ANALYST | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 7 | **Information Security Research** | | | | | | | |
| 7.1 | **Research**<br>The systematic creation of new knowledge by data gathering, innovation, experimentation, evaluation and dissemination. The determination of research goals and the method by which the research will be conducted. The active participation in a community of researchers; communicating formally and informally through digital media, conferences, journals, books and seminars. | ○ | ○ | Understand | Understand | Understand | Understand | Understand |
| 8 | **Management, Leadership, Business and Communications** | | | | | | | |
| 8.1 | **Supports Strategic Direction**<br>Supports shared purpose and direction; thinks strategically; harnesses information and opportunities; shows judgement, intelligence and common-sense. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.2 | **Achieves Results**<br>Builds ASD and the ACSC's capability and responsiveness by identifying, applying and building professional expertise; responds positively to change; takes responsibility for managing work projects to achieve results. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.3 | **Supports Productive Working Relationships**<br>Nurtures internal relationships; listens to, understands and recognises the needs of others; values individual differences and diversity; shares learning and supports others. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.4 | **Displays Personal Drive and Integrity**<br>Demonstrates public service professionalism and probity; engages with risk and shows personal courage; commits to action; promotes and adopts a positive and balanced approach to work; demonstrates self-awareness and a commitment to personal development. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.5 | **Communicates with Influence**<br>Communicates clearly; listens, understands and adapts to audience; negotiates confidently. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 9 | **Specialist Advice** | | | | | | | |
| 9.1 | **Specialist Advice**<br>The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice. | ○ | ○ | ○ | ○ | ○ | Enable | Advise |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

| MALWARE ANALYST | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 1 | **Information Security Governance and Strategy** | | | | | | | |
| 1.5 | **Legal and Regulatory Environment**<br>Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements. | Understand | Understand | Understand | Understand | Understand | Understand | Understand |
| 2 | **Threat Assessment and Information Risk Management** | | | | | | | |
| 2.2 | **Risk Assessment**<br>Identifies and assesses information assets. Uses this information and relevant threat assessments, business impacts, business benefits and costs to conduct risk assessments and identify and assess potential vulnerabilities. | Not required | Not required | Not required | Understand | Apply | Enable | Advise |
| 3 | **Systems Development and Implementation** | | | | | | | |
| 3.2 | **Systems Design**<br>The design of systems to meet specified requirements, compatible with agreed systems architectures, adhering to corporate standards and within constraints of performance and feasibility. The identification of concepts and their translation into a design which forms the basis for systems construction and verification. The design or selection of components. The development of a complete set of detailed models, properties, and/or characteristics described in a form suitable for implementation. The adoption and adaptation of systems design lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Not required | Enable | Enable | Enable | Enable |
| 3.3 | **Software Design**<br>The specification and design of software to meet defined requirements by following agreed design standards and principles. The definition of software, components, interfaces and related characteristics. The identification of concepts and patterns and the translation into a design which provides a basis for software construction and verification. The evaluation of alternative solutions and trade-offs. The facilitation of design decisions within the constraints of systems designs, design standards, quality, feasibility, extensibility and maintainability. The development and iteration of prototypes/simulations to enable informed decision-making. The adoption and adaptation of software design models, tools and techniques based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Not required | Apply | Enable | Enable | Enable |
| 3.4 | **Programming/Software Development**<br>The planning, designing, creation, amending, verification, testing and documentation of new and amended software components in order to deliver agreed value to stakeholders. The identification, creation and application of agreed software development and security standards and processes. Adopting and adapting software development lifecycle models, based on the context of the work, and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Understand | Apply | Enable | Enable | Enable |
| 4 | **Assurance: Audit, Compliance and Testing** | | | | | | | |
| 4.2 | **Compliance Monitoring and Controls Testing**<br>Defines and implements processes to verify on-going conformance to security and/or legal and regulatory requirements. Carries out security compliance checks in accordance with an appropriate methodology. This skill group covers compliance checks and tests against technical, physical, procedural and personnel controls. | Not required | Not required | Not required | Not required | Understand | Understand | Understand |
| 4.4 | **Penetration Testing**<br>The assessment of organisational vulnerabilities through the design and execution of penetration tests that demonstrate how an adversary can either subvert the organisation's security goals or achieve specific adversarial objectives. Penetration testing may be a stand-alone activity or an aspect of acceptance testing prior to an approval to operate. The identification of deeper insights into the business risks of various vulnerabilities. | Not required | Not required | Not required | Not required | Enable | Enable | Enable |

Not required · Knowledge · Understand · Apply · Enable · Advise · Initiate, Enable and Ensure

| MALWARE ANALYST | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 5 | **Operational Security Management** | | | | | | | |
| 5.1 | **Secure Operations Management**<br>Establishes processes for maintaining the security of information throughout its existence, including establishing and maintaining security operating procedures in accordance with security policies, standards and procedures. Coordinates penetration and other testing on information processes. Assesses and responds to new technical, physical, personnel or procedural vulnerabilities. Engages with the change management process to ensure that vulnerabilities are mediated. Manages the implementation of cyber and information security programs, and co-ordinates security activities across the ACSC. | ○ | ○ | ○ | ○ | Understand | Understand | Understand |
| 5.2 | **Secure Operations and Service Delivery**<br>Securely configures and maintains information, control and communications equipment in accordance with relevant security policies, standards and guidelines. This includes the configuration of information security devices (e.g. firewalls) and protective monitoring tools (e.g. SIEM). Implements security policy (e.g. patching policies) and security operating procedures in respect of system and/or network management. Undertakes routine technical vulnerability assessments. Maintains security records and documentation in accordance with security operating procedures. Administers logical and physical user access rights. Monitors processes for violations of relevant security policies (e.g. acceptable use, security, etc.). | ○ | ○ | Understand | Apply | Enable | Enable | Advise |
| 6 | **Incident Management, Investigation and Forensics** | | | | | | | |
| 6.3 | **Forensics**<br>The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings, including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations. | ○ | ○ | Knowledge | Apply | Enable | Advise | Advise |
| 7 | **Information Security Research** | | | | | | | |
| 7.2 | **Applied Research**<br>Vulnerability research and discovery, leading to the development of exploits, reverse engineering and researching mitigation bypasses. Cryptographic research leading to the assessment of existing algorithms. In the information security field, uses existing knowledge in experimental development to produce new or substantially improved devices, products and processes. | ○ | ○ | Apply | Enable | Advise | Initiate, Enable and Ensure | Initiate, Enable and Ensure |
| 8 | **Management, Leadership, Business and Communications** | | | | | | | |
| 8.1 | **Supports Strategic Direction**<br>Supports shared purpose and direction; thinks strategically; harnesses information and opportunities; shows judgement, intelligence and common-sense. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.2 | **Achieves Results**<br>Builds ASD and the ACSC's capability and responsiveness by identifying, applying and building professional expertise; responds positively to change; takes responsibility for managing work projects to achieve results. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.3 | **Supports Productive Working Relationships**<br>Nurtures internal relationships; listens to, understands and recognises the needs of others; values individual differences and diversity; shares learning and supports others. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.4 | **Displays Personal Drive and Integrity**<br>Demonstrates public service professionalism and probity; engages with risk and shows personal courage; commits to action; promotes and adopts a positive and balanced approach to work; demonstrates self-awareness and a commitment to personal development. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.5 | **Communicates with Influence**<br>Communicates clearly; listens, understands and adapts to audience; negotiates confidently. | Knowledge | Knowledge | Understand | Knowledge | Enable | Advise | Initiate, Enable and Ensure |
| 9 | **Specialist Advice** | | | | | | | |
| 9.1 | **Specialist Advice**<br>The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice. | ○ | ○ | Enable | Enable | Enable | Enable | Advise |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

# CYBER SECURITY OPERATIONS ROLES

| Cyber Security Operations Roles | Expectations |
| --- | --- |
| **Incident Responder**<br>An Incident Responder performs analysis and investigations of cyber security incidents, often malicious, to remediate networks and provide mitigation advice to protect and secure systems. | • Investigate information and cyber security incidents<br>• Analyse and resolve identified security incidents<br>• Contribute to digital forensic investigations<br>• Communicate technical findings and recommendations<br>• Provide assistance with the development of technical remediation plan |
| **Operations Coordinator**<br>An Operations Coordinator manages tasks associated with cyber security incidents across various teams for incident response and hunt operations, including setting priorities and engaging with customers. An Operations Coordinator provides detailed technical advice and contributes to policy development, strategic planning, and program and project management. | • Lead the coordination, governance and response to complex cyber security incidents and hunt investigations<br>• Manage tasks across various teams for incident response and hunt operations<br>• Advise leadership on current operational collaborations and contribute toward strategic planning<br>• Facilitiate incident response engagements<br>• Assess technical information to develop key messaging |

| INCIDENT RESPONDER | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 1 | **Information Security Governance and Strategy** | | | | | | | |
| 1.5 | **Legal and Regulatory Environment**<br>Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements. | ○ | ○ | Knowledge | Understand | Understand | Understand | Understand |
| 2 | **Threat Assessment and Information Risk Management** | | | | | | | |
| 2.1 | **Threat Intelligence, Assessment and Threat Modelling**<br>Assesses and validates information from several sources on current and potential cyber and information security threats to the business, analysing trends and highlighting information security issues relevant to ASD. Processes, collates and exploits data, taking into account its relevance and reliability to develop and maintain 'situational awareness'. Predicts and prioritises threats to ASD, Australian government agencies, critical infrastructure and businesses, and their methods of attack. Analyses the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities. Predicts and prioritises threats to an organisation and their methods of attack. Uses human factor analysis in the assessment of threats. Prepares and disseminates intelligence reports, providing threat indicators and warnings. | ○ | ○ | Understand | Understand | Understand | Apply | Apply |
| 4 | **Assurance: Audit, Compliance and Testing** | | | | | | | |
| 4.4 | **Penetration Testing**<br>The assessment of organisational vulnerabilities through the design and execution of penetration tests that demonstrate how an adversary can either subvert the organisation's security goals or achieve specific adversarial objectives. Penetration testing may be a stand-alone activity or an aspect of acceptance testing prior to an approval to operate. The identification of deeper insights into the business risks of various vulnerabilities. | ○ | ○ | Understand | Understand | Understand | Understand | Understand |
| 5 | **Operational Security Management** | | | | | | | |
| 5.1 | **Secure Operations Management**<br>Establishes processes for maintaining the security of information throughout its existence, including establishing and maintaining security operating procedures in accordance with security policies, standards and procedures. Coordinates penetration and other testing on information processes. Assesses and responds to new technical, physical, personnel or procedural vulnerabilities. Engages with the change management process to ensure that vulnerabilities are mediated. Manages the implementation of cyber and information security programs, and co-ordinates security activities across the ACSC. | ○ | ○ | Understand | Apply | Enable | Initiate, Enable and Ensure | Initiate, Enable and Ensure |
| 6 | **Incident Management, Investigation and Forensics** | | | | | | | |
| 6.1 | **Intrusion Detection and Analysis**<br>Monitors network and system activity to identify potential intrusion or other anomalous behaviour. Analyses the information and initiates an appropriate response, escalating as necessary. Uses security analytics, including the outputs from intelligence analysis, predictive research and root cause analysis in order to search for and detect potential breaches or identify recognised indicators and warnings. Monitors, collates and filters external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes. Ensures that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available. Produces warning material in a manner that is both timely and intelligible to the target audience(s). | ○ | ○ | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 6.2 | **Incident Management, Incident Investigation and Response**<br>Engages with the overall organisation Incident Management process to ensure that cyber security incidents are handled appropriately. Defines and implements processes and procedures for detecting and investigating cyber security incidents. Establishes and maintains Incident Response teams to respond to and mitigate the risks of cyber security incidents. Working within the legal constraints imposed by the jurisdictions in which ASD carries out investigations of cyber security incidents using all relevant sources of information. Assesses the need for forensic activity, and coordinates the activities of specialist forensic personnel within the overall response activities, engaging with the relevant organisational processes to ensure that forensic services are deployed appropriately. Provides a full information security investigation capability where third parties, managed service providers, etc., are involved. | ○ | ○ | Understand | Apply | Advise | Initiate, Enable and Ensure | Initiate, Enable and Ensure |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

| INCIDENT RESPONDER | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 6.3 | **Forensics**<br>The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings, including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations. | ○ | ○ | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 7 | **Information Security Research** | | | | | | | |
| 7.2 | **Applied Research**<br>Vulnerability research and discovery, leading to the development of exploits, reverse engineering and researching mitigation bypasses. Cryptographic research leading to the assessment of existing algorithms. In the information security field, uses existing knowledge in experimental development to produce new or substantially improved devices, products and processes. | ○ | ○ | Knowledge | Understand | Understand | Understand | Understand |
| 8 | **Management, Leadership, Business and Communications** | | | | | | | |
| 8.1 | **Supports Strategic Direction**<br>Supports shared purpose and direction; thinks strategically; harnesses information and opportunities; shows judgement, intelligence and common-sense. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.2 | **Achieves Results**<br>Builds ASD and the ACSC's capability and responsiveness by identifying, applying and building professional expertise; responds positively to change; takes responsibility for managing work projects to achieve results. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.3 | **Supports Productive Working Relationships**<br>Nurtures internal relationships; listens to, understands and recognises the needs of others; values individual differences and diversity; shares learning and supports others. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.4 | **Displays Personal Drive and Integrity**<br>Demonstrates public service professionalism and probity; engages with risk and shows personal courage; commits to action; promotes and adopts a positive and balanced approach to work; demonstrates self-awareness and a commitment to personal development. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.5 | **Communicates with Influence**<br>Communicates clearly; listens, understands and adapts to audience; negotiates confidently. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 9 | **Specialist Advice** | | | | | | | |
| 9.1 | **Specialist Advice**<br>The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice. | ○ | ○ | ○ | ○ | ○ | Enable | Enable |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

| OPERATIONS COORDINATOR | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 1 | **Information Security Governance and Strategy** | | | | | | | |
| 1.4 | **Behavioural Change**<br>Identifies cyber and information security awareness, training and culture management needs in line with ASD security strategies, business needs and strategic direction, and gains the Senior Leadership's commitment and resources to support these needs. Manages the development or delivery of cyber and information security awareness and training, behavioural analysis programs and/or security culture management programs, applying analysis of human factors as appropriate. | ○ | ○ | Understand | Understand | Understand | Understand | Understand |
| 1.5 | **Legal and Regulatory Environment**<br>Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements. | ○ | ○ | Understand | Understand | Understand | Understand | Understand |
| 1.6 | **Third Party Management**<br>Identifies and advises on the technical, physical, personnel and procedural risks associated with third party relationships, including systems development and maintenance, contracts, end of service, outsourced service providers and business partners, and sub-contracting. Assesses the level of confidence that third-party cyber and information security capabilities/services operate as defined. | ○ | ○ | Apply | Apply | Enable | Enable | Advise |
| 2 | **Threat Assessment and Information Risk Management** | | | | | | | |
| 2.1 | **Threat Intelligence, Assessment and Threat Modelling**<br>Assesses and validates information from several sources on current and potential cyber and information security threats to the business, analysing trends and highlighting information security issues relevant to ASD. Processes, collates and exploits data, taking into account its relevance and reliability to develop and maintain 'situational awareness'. Predicts and prioritises threats to ASD, Australian government agencies, critical infrastructure and businesses, and their methods of attack. Analyses the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities. Predicts and prioritises threats to an organisation and their methods of attack. Uses human factor analysis in the assessment of threats. Prepares and disseminates intelligence reports, providing threat indicators and warnings. | ○ | ○ | Understand | Understand | Understand | Understand | Understand |
| 2.3 | **Information risk management**<br>Develops cyber and information security risk management strategies and controls, taking into account business needs and risk assessments, and balancing technical, physical, procedural and personnel controls. | ○ | ○ | Apply | Enable | Advise | Initiate, Enable and Ensure | Initiate, Enable and Ensure |
| 4 | **Assurance: Audit, Compliance and Testing** | | | | | | | |
| 4.1 | **Internal and Statutory Audit**<br>Verifies that information systems and processes meet the Australian government's security criteria (requirements or policy, standards and procedures). Assesses the business benefits of security controls. | ○ | ○ | Apply | Enable | Enable | Advise | Initiate, Enable and Ensure |
| 4.3 | **Security Evaluation and Functionality Testing**<br>Contributes to the security evaluation or testing of software. Evaluates security software by analysing the design documentation and code to identify potential vulnerabilities and testing to ascertain whether these are exploitable. Tests the security functionality of systems or applications for correctness in line with security policies, standards and procedures, and advises on corrective measures. Applies recognised evaluation/testing methodologies, tools and techniques, developing new ones where appropriate. Assesses the robustness of a system, product or technology. Applies commonly accepted governance practices and standards when testing in an operational environment. | ○ | ○ | Knowledge | Knowledge | Understand | Understand | Understand |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

| OPERATIONS COORDINATOR | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 5 | **Operational Security Management** | | | | | | | |
| 5.1 | **Secure Operations Management**<br>Establishes processes for maintaining the security of information throughout its existence, including establishing and maintaining security operating procedures in accordance with security policies, standards and procedures. Coordinates penetration and other testing on information processes. Assesses and responds to new technical, physical, personnel or procedural vulnerabilities. Engages with the change management process to ensure that vulnerabilities are mediated. Manages the implementation of cyber and information security programs, and co-ordinates security activities across the ACSC. | ○ | ○ | Understand | Understand | Understand | Understand | Understand |
| 6 | **Incident Management, Investigation and Forensics** | | | | | | | |
| 6.2 | **Incident Management, Incident Investigation and Response**<br>Engages with the overall organisation Incident Management process to ensure that cyber security incidents are handled appropriately. Defines and implements processes and procedures for detecting and investigating cyber security incidents. Establishes and maintains Incident Response teams to respond to and mitigate the risks of cyber security incidents. Working within the legal constraints imposed by the jurisdictions in which ASD carries out investigations of cyber security incidents using all relevant sources of information. Assesses the need for forensic activity, and coordinates the activities of specialist forensic personnel within the overall response activities, engaging with the relevant organisational processes to ensure that forensic services are deployed appropriately. Provides a full information security investigation capability where third parties, managed service providers, etc., are involved. | ○ | ○ | Apply | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8 | **Management, Leadership, Business and Communications** | | | | | | | |
| 8.1 | **Supports Strategic Direction**<br>Supports shared purpose and direction; thinks strategically; harnesses information and opportunities; shows judgement, intelligence and common-sense. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.2 | **Achieves Results**<br>Builds ASD and the ACSC's capability and responsiveness by identifying, applying and building professional expertise; responds positively to change; takes responsibility for managing work projects to achieve results. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.3 | **Supports Productive Working Relationships**<br>Nurtures internal relationships; listens to, understands and recognises the needs of others; values individual differences and diversity; shares learning and supports others. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.4 | **Displays Personal Drive and Integrity**<br>Demonstrates public service professionalism and probity; engages with risk and shows personal courage; commits to action; promotes and adopts a positive and balanced approach to work; demonstrates self-awareness and a commitment to personal development. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.5 | **Communicates with Influence**<br>Communicates clearly; listens, understands and adapts to audience; negotiates confidently. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 9 | **Specialist Advice** | | | | | | | |
| 9.1 | **Specialist Advice**<br>The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice. | ○ | ○ | ○ | ○ | ○ | Enable | Advise |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

# CYBER SECURITY TESTING ROLES

| Cyber Security Testing Roles | Expectations |
| --- | --- |
| **Penetration Tester**<br>A Penetration Tester (Red Team) performs cyber security exploitation, penetration testing and red team activities. A Penetration Tester creates test cases using in-depth technical analysis of risks and typical vulnerabilities and produce test scripts, materials and packs to test new and existing software or services. A Penetration Tester plans, coordinates and conducts cyber threat emulation activities in support of certification, accreditation, and operational priorities to verify deficiencies in technical security controls. A Penetration Tester provides remediation, technical advice, recommendations and consultancy on networks, infrastructure, products and services supplied to system owners. | • Plan, coordinate and conduct cyber threat emulation activities<br>• Provide complex technical advice, recommendations and consultancy<br>• Communicate technical findings and recommendations<br>• Create test cases using in-depth technical analysis of risks and typical vulnerabilities<br>• Assess cyber threat intelligence and interpret threat reporting |
| **Vulnerability Assessor**<br>A Vulnerability Assessor performs technical security investigations on a wide array of assets and devices that directly relate to security infrastructure. A Vulnerability Assessor evaluates and assists with the application and compliance of security controls, reviews information systems for actual or potential security vulnerabilities, and explains threat profiles of a variety of electronic devices. A Vulnerability Assessor contributes to the development of systems design policies and standards, and selection of architecture components. | • Perform complex security investigations<br>• Assess and explain threat profiles for a variety of electronic devices<br>• Evaluate and assist with the application and compliance of security controls<br>• Review information systems for actual or potential security vulnerabilities<br>• Design, code, verify, test, document, amend and refactor complex programs, scripts and integration software services |

| PENETRATION TESTER | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 1 | **Information Security Governance and Strategy** | | | | | | | |
| 1.5 | **Legal and Regulatory Environment**<br>Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements. | Understand | Understand | Understand | Understand | Understand | Understand | Understand |
| 2 | **Threat Assessment and Information Risk Management** | | | | | | | |
| 2.2 | **Risk Assessment**<br>Identifies and assesses information assets. Uses this information and relevant threat assessments, business impacts, business benefits and costs to conduct risk assessments and identify and assess potential vulnerabilities. | Not required | Not required | Understand | Understand | Understand | Apply | Enable |
| 3 | **Systems Development and Implementation** | | | | | | | |
| 3.2 | **Systems Design**<br>The design of systems to meet specified requirements, compatible with agreed systems architectures, adhering to corporate standards and within constraints of performance and feasibility. The identification of concepts and their translation into a design which forms the basis for systems construction and verification. The design or selection of components. The development of a complete set of detailed models, properties, and/or characteristics described in a form suitable for implementation. The adoption and adaptation of systems design lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Enable | Enable | Enable | Enable | Enable |
| 3.3 | **Software Design**<br>The specification and design of software to meet defined requirements by following agreed design standards and principles. The definition of software, components, interfaces and related characteristics. The identification of concepts and patterns and the translation into a design which provides a basis for software construction and verification. The evaluation of alternative solutions and trade-offs. The facilitation of design decisions within the constraints of systems designs, design standards, quality, feasibility, extensibility and maintainability. The development and iteration of prototypes/simulations to enable informed decision-making. The adoption and adaptation of software design models, tools and techniques based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Understand | Understand | Apply | Apply | Enable |
| 3.4 | **Programming/Software Development**<br>The planning, designing, creation, amending, verification, testing and documentation of new and amended software components in order to deliver agreed value to stakeholders. The identification, creation and application of agreed software development and security standards and processes. Adopting and adapting software development lifecycle models, based on the context of the work, and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Understand | Understand | Apply | Apply | Enable |
| 4 | **Assurance: Audit, Compliance and Testing** | | | | | | | |
| 4.2 | **Compliance Monitoring and Controls Testing**<br>Defines and implements processes to verify on-going conformance to security and/or legal and regulatory requirements. Carries out security compliance checks in accordance with an appropriate methodology. This skill group covers compliance checks and tests against technical, physical, procedural and personnel controls. | Not required | Not required | Understand | Understand | Apply | Apply | Apply |
| 4.4 | **Penetration Testing**<br>The assessment of organisational vulnerabilities through the design and execution of penetration tests that demonstrate how an adversary can either subvert the organisation's security goals or achieve specific adversarial objectives. Penetration testing may be a stand-alone activity or an aspect of acceptance testing prior to an approval to operate. The identification of deeper insights into the business risks of various vulnerabilities. | Not required | Not required | Apply | Enable | Enable | Advise | Initiate, Enable and Ensure |
| 5 | **Operational Security Management** | | | | | | | |
| 5.1 | **Secure Operations Management**<br>Establishes processes for maintaining the security of information throughout its existence, including establishing and maintaining security operating procedures in accordance with security policies, standards and procedures. Coordinates penetration and other testing on information processes. Assesses and responds to new technical, physical, personnel or procedural vulnerabilities. Engages with the change management process to ensure that vulnerabilities are mediated. Manages the implementation of cyber and information security programs, and co-ordinates security activities across the ACSC. | Not required | Not required | Understand | Understand | Apply | Apply | Enable |

Not required · Knowledge · Understand · Apply · Enable · Advise · Initiate, Enable and Ensure

| PENETRATION TESTER | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 5.2 | **Secure Operations and Service Delivery**<br>Securely configures and maintains information, control and communications equipment in accordance with relevant security policies, standards and guidelines. This includes the configuration of information security devices (e.g. firewalls) and protective monitoring tools (e.g. SIEM). Implements security policy (e.g. patching policies) and security operating procedures in respect of system and/or network management. Undertakes routine technical vulnerability assessments. Maintains security records and documentation in accordance with security operating procedures. Administers logical and physical user access rights. Monitors processes for violations of relevant security policies (e.g. acceptable use, security, etc.). | ○ | ○ | Understand | Understand | Apply | Enable | Advise |
| 6 | **Incident Management, Investigation and Forensics** | | | | | | | |
| 6.1 | **Intrusion Detection and Analysis**<br>Monitors network and system activity to identify potential intrusion or other anomalous behaviour. Analyses the information and initiates an appropriate response, escalating as necessary. Uses security analytics, including the outputs from intelligence analysis, predictive research and root cause analysis in order to search for and detect potential breaches or identify recognised indicators and warnings. Monitors, collates and filters external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes. Ensures that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available. Produces warning material in a manner that is both timely and intelligible to the target audience(s). | ○ | ○ | ○ | ○ | ○ | Understand | Understand |
| 6.3 | **Forensics**<br>The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings, including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations. | ○ | ○ | ○ | Apply | Apply | Enable | Advise |
| 7 | **Information Security Research** | | | | | | | |
| 7.2 | **Applied Research**<br>Vulnerability research and discovery, leading to the development of exploits, reverse engineering and researching mitigation bypasses. Cryptographic research leading to the assessment of existing algorithms. In the information security field, uses existing knowledge in experimental development to produce new or substantially improved devices, products and processes. | ○ | ○ | ○ | Apply | Apply | Enable | Enable |
| 8 | **Management, Leadership, Business and Communications** | | | | | | | |
| 8.1 | **Supports Strategic Direction**<br>Supports shared purpose and direction; thinks strategically; harnesses information and opportunities; shows judgement, intelligence and common-sense. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.2 | **Achieves Results**<br>Builds ASD and the ACSC's capability and responsiveness by identifying, applying and building professional expertise; responds positively to change; takes responsibility for managing work projects to achieve results. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.3 | **Supports Productive Working Relationships**<br>Nurtures internal relationships; listens to, understands and recognises the needs of others; values individual differences and diversity; shares learning and supports others. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.4 | **Displays Personal Drive and Integrity**<br>Demonstrates public service professionalism and probity; engages with risk and shows personal courage; commits to action; promotes and adopts a positive and balanced approach to work; demonstrates self-awareness and a commitment to personal development. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.5 | **Communicates with Influence**<br>Communicates clearly; listens, understands and adapts to audience; negotiates confidently. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 9 | **Specialist Advice** | | | | | | | |
| 9.1 | **Specialist Advice**<br>The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice. | ○ | ○ | ○ | ○ | ○ | Enable | Advise |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

| VULNERABILITY ASSESSOR | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 1 | **Information Security Governance and Strategy** | | | | | | | |
| 1.5 | **Legal and Regulatory Environment**<br>Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements. | Understand | Understand | Understand | Understand | Understand | Understand | Understand |
| 2 | **Threat Assessment and Information Risk Management** | | | | | | | |
| 2.1 | **Threat Intelligence, Assessment and Threat Modelling**<br>Assesses and validates information from several sources on current and potential cyber and information security threats to the business, analysing trends and highlighting information security issues relevant to ASD. Processes, collates and exploits data, taking into account its relevance and reliability to develop and maintain 'situational awareness'. Predicts and prioritises threats to ASD, Australian government agencies, critical infrastructure and businesses, and their methods of attack. Analyses the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities. Predicts and prioritises threats to an organisation and their methods of attack. Uses human factor analysis in the assessment of threats. Prepares and disseminates intelligence reports, providing threat indicators and warnings. | Not required | Not required | Apply | Apply | Enable | Advise | Advise |
| 2.2 | **Risk Assessment**<br>Identifies and assesses information assets. Uses this information and relevant threat assessments, business impacts, business benefits and costs to conduct risk assessments and identify and assess potential vulnerabilities. | Not required | Not required | Not required | Understand | Apply | Enable | Enable |
| 3 | **Systems Development and Implementation** | | | | | | | |
| 3.2 | **Systems Design**<br>The design of systems to meet specified requirements, compatible with agreed systems architectures, adhering to corporate standards and within constraints of performance and feasibility. The identification of concepts and their translation into a design which forms the basis for systems construction and verification. The design or selection of components. The development of a complete set of detailed models, properties, and/or characteristics described in a form suitable for implementation. The adoption and adaptation of systems design lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Enable | Advise | Advise | Initiate, Enable and Ensure | Initiate, Enable and Ensure |
| 3.3 | **Software Design**<br>The specification and design of software to meet defined requirements by following agreed design standards and principles. The definition of software, components, interfaces and related characteristics. The identification of concepts and patterns and the translation into a design which provides a basis for software construction and verification. The evaluation of alternative solutions and trade-offs. The facilitation of design decisions within the constraints of systems designs, design standards, quality, feasibility, extensibility and maintainability. The development and iteration of prototypes/simulations to enable informed decision-making. The adoption and adaptation of software design models, tools and techniques based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Not required | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 3.4 | **Programming/Software Development**<br>The planning, designing, creation, amending, verification, testing and documentation of new and amended software components in order to deliver agreed value to stakeholders. The identification, creation and application of agreed software development and security standards and processes. Adopting and adapting software development lifecycle models, based on the context of the work, and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Apply | Apply | Enable | Enable | Advise |
| 4 | **Assurance: Audit, Compliance and Testing** | | | | | | | |
| 4.1 | **Internal and Statutory Audit**<br>Verifies that information systems and processes meet the Australian government's security criteria (requirements or policy, standards and procedures). Assesses the business benefits of security controls. | Not required | Not required | Apply | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 4.2 | **Compliance Monitoring and Controls Testing**<br>Defines and implements processes to verify on-going conformance to security and/or legal and regulatory requirements. Carries out security compliance checks in accordance with an appropriate methodology. This skill group covers compliance checks and tests against technical, physical, procedural and personnel controls. | Not required | Not required | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |

Not required · Knowledge · Understand · Apply · Enable · Advise · Initiate, Enable and Ensure

| VULNERABILITY ASSESSOR | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 4.3 | **Security Evaluation and Functionality Testing**<br>Contributes to the security evaluation or testing of software. Evaluates security software by analysing the design documentation and code to identify potential vulnerabilities and testing to ascertain whether these are exploitable. Tests the security functionality of systems or applications for correctness in line with security policies, standards and procedures, and advises on corrective measures. Applies recognised evaluation/testing methodologies, tools and techniques, developing new ones where appropriate. Assesses the robustness of a system, product or technology. Applies commonly accepted governance practices and standards when testing in an operational environment. | ○ | ○ | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 4.4 | **Penetration Testing**<br>The assessment of organisational vulnerabilities through the design and execution of penetration tests that demonstrate how an adversary can either subvert the organisation's security goals or achieve specific adversarial objectives. Penetration testing may be a stand-alone activity or an aspect of acceptance testing prior to an approval to operate. The identification of deeper insights into the business risks of various vulnerabilities. | ○ | ○ | Apply | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 6 | **Incident Management, Investigation and Forensics** | | | | | | | |
| 6.1 | **Intrusion Detection and Analysis**<br>Monitors network and system activity to identify potential intrusion or other anomalous behaviour. Analyses the information and initiates an appropriate response, escalating as necessary. Uses security analytics, including the outputs from intelligence analysis, predictive research and root cause analysis in order to search for and detect potential breaches or identify recognised indicators and warnings. Monitors, collates and filters external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes. Ensures that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available. Produces warning material in a manner that is both timely and intelligible to the target audience(s). | ○ | ○ | Understand | Understand | Understand | Understand | Understand |
| 8 | **Management, Leadership, Business and Communications** | | | | | | | |
| 8.1 | **Supports Strategic Direction**<br>Supports shared purpose and direction; thinks strategically; harnesses information and opportunities; shows judgement, intelligence and common-sense. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.2 | **Achieves Results**<br>Builds ASD and the ACSC's capability and responsiveness by identifying, applying and building professional expertise; responds positively to change; takes responsibility for managing work projects to achieve results. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.3 | **Supports Productive Working Relationships**<br>Nurtures internal relationships; listens to, understands and recognises the needs of others; values individual differences and diversity; shares learning and supports others. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.4 | **Displays Personal Drive and Integrity**<br>Demonstrates public service professionalism and probity; engages with risk and shows personal courage; commits to action; promotes and adopts a positive and balanced approach to work; demonstrates self-awareness and a commitment to personal development. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.5 | **Communicates with Influence**<br>Communicates clearly; listens, understands and adapts to audience; negotiates confidently. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 9 | **Specialist Advice** | | | | | | | |
| 9.1 | **Specialist Advice**<br>The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice. | ○ | ○ | ○ | Enable | Advise | Initiate, Enable and Ensure | Initiate, Enable and Ensure |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

# CYBER SECURITY ARCHITECTURE ROLES

| Cyber Security Architecture Roles | Expectations |
| --- | --- |
| **Cyber Security Advice and Assessment**<br>A Cyber Security Advice and Assessment (Blue Team) role performs cyber and information security risk assessments and provides detailed technical, professional and policy advice and guidance on the application and operation of procedural security controls. | • Conduct risk and security control assessments<br>• Interpret security policy and contribute to the development of standards and guidelines<br>• Review information system designs<br>• Provide guidance on security strategies to manage identified risks<br>• Provide specialist advice<br>• Explain systems security and the strengths and weaknesses |
| **Vulnerability Researcher**<br>A Vulnerability Researcher plans, coordinates and conducts cyber vulnerability research activities to identify deficiencies and impacts on systems and emerging technologies, develop proof of concept exploits, and support certification, accreditation and operational priorities. | • Plan and coordinate vulnerability research assessments<br>• Conduct cyber research activities in order to identify deficiencies and impact on systems<br>• Conduct complex applied research<br>• Identify and evaluate alternative design options<br>• Design, code, verify, test, document, amend and refactor complex programs/scripts and integration software services<br>• Communicate technical findings and recommendations |

| CYBER SECURITY ADVICE AND ASSESSMENT | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 1 | **Information Security Governance and Strategy** | | | | | | | |
| 1.1 | **Governance**<br>Directs, oversees, designs, implements or operates within the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage cyber and information security at an organisational level; thereby supporting ASD's immediate and future regulatory, legal, risk, environmental and operational requirements and ensuring compliance with those requirements. | ○ | ○ | Understand | Understand | Apply | Advise | Initiate, Enable and Ensure |
| 1.2 | **Policy and Standards**<br>Directs, develops or maintains organisational cyber and information security policies, standards and processes using recognised standards (e.g. the ISM, DSPF, PSPF, ISO and NIST) where appropriate. Applies recognised cyber and information security standards and policies within ASD as an organisation, in addition to its programs, projects and operations. | ○ | ○ | Understand | Apply | Apply | Enable | Initiate, Enable and Ensure |
| 1.3 | **Information Security Strategy**<br>Directs, develops or maintains plans and processes to manage cyber and information security risks appropriately and effectively, whilst complying with legal, statutory, contractual, and business requirements. | ○ | ○ | Understand | Understand | Apply | Advise | Initiate, Enable and Ensure |
| 1.5 | **Legal and Regulatory Environment**<br>Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements. | ○ | ○ | Apply | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 2 | **Threat Assessment and Information Risk Management** | | | | | | | |
| 2.3 | **Information risk management**<br>Develops cyber and information security risk management strategies and controls, taking into account business needs and risk assessments, and balancing technical, physical, procedural and personnel controls. | ○ | ○ | Apply | Apply | Apply | Enable | Advise |
| 3 | **Systems Development and Implementation** | | | | | | | |
| 3.1 | **Systems Development and Management**<br>The planning, estimating and execution of programs of systems development work to time, budget and quality targets. The identification of the resources needed for systems development and how this will be met with an effective supply capacity. The alignment of systems development activity and deliverables with agreed architectures and standards. The development of roadmaps to communicate future systems development plans. The adoption and adaptation of systems development lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | ○ | ○ | ○ | ○ | ○ | Advise | Initiate, Enable and Ensure |
| 3.2 | **Systems Design**<br>The design of systems to meet specified requirements, compatible with agreed systems architectures, adhering to corporate standards and within constraints of performance and feasibility. The identification of concepts and their translation into a design which forms the basis for systems construction and verification. The design or selection of components. The development of a complete set of detailed models, properties, and/or characteristics described in a form suitable for implementation. The adoption and adaptation of systems design lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | ○ | ○ | ○ | Enable | Enable | Advise | Initiate, Enable and Ensure |
| 4 | **Assurance: Audit, Compliance and Testing** | | | | | | | |
| 4.1 | **Internal and Statutory Audit**<br>Verifies that information systems and processes meet the Australian government's security criteria (requirements or policy, standards and procedures). Assesses the business benefits of security controls. | ○ | ○ | Understand | Apply | Apply | Advise | Initiate, Enable and Ensure |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

| CYBER SECURITY ADVICE AND ASSESSMENT | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 5 | **Operational Security Management** | | | | | | | |
| 5.1 | **Secure Operations Management**<br>Establishes processes for maintaining the security of information throughout its existence, including establishing and maintaining security operating procedures in accordance with security policies, standards and procedures. Coordinates penetration and other testing on information processes. Assesses and responds to new technical, physical, personnel or procedural vulnerabilities. Engages with the change management process to ensure that vulnerabilities are mediated. Manages the implementation of cyber and information security programs, and co-ordinates security activities across the ACSC. | ○ | ○ | ○ | ○ | Apply | Enable | Initiate, Enable and Ensure |
| 7 | **Information Security Research** | | | | | | | |
| 7.1 | **Research**<br>The systematic creation of new knowledge by data gathering, innovation, experimentation, evaluation and dissemination. The determination of research goals and the method by which the research will be conducted. The active participation in a community of researchers; communicating formally and informally through digital media, conferences, journals, books and seminars. | ○ | ○ | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 7.2 | **Applied Research**<br>Vulnerability research and discovery, leading to the development of exploits, reverse engineering and researching mitigation bypasses. Cryptographic research leading to the assessment of existing algorithms. In the information security field, uses existing knowledge in experimental development to produce new or substantially improved devices, products and processes. | ○ | ○ | Understand | Understand | Understand | Understand | Understand |
| 8 | **Management, Leadership, Business and Communications** | | | | | | | |
| 8.1 | **Supports Strategic Direction**<br>Supports shared purpose and direction; thinks strategically; harnesses information and opportunities; shows judgement, intelligence and common-sense. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.2 | **Achieves Results**<br>Builds ASD and the ACSC's capability and responsiveness by identifying, applying and building professional expertise; responds positively to change; takes responsibility for managing work projects to achieve results. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.3 | **Supports Productive Working Relationships**<br>Nurtures internal relationships; listens to, understands and recognises the needs of others; values individual differences and diversity; shares learning and supports others. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.4 | **Displays Personal Drive and Integrity**<br>Demonstrates public service professionalism and probity; engages with risk and shows personal courage; commits to action; promotes and adopts a positive and balanced approach to work; demonstrates self-awareness and a commitment to personal development. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.5 | **Communicates with Influence**<br>Communicates clearly; listens, understands and adapts to audience; negotiates confidently. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 9 | **Specialist Advice** | | | | | | | |
| 9.1 | **Specialist Advice**<br>The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice. | ○ | ○ | Enable | Enable | Enable | Advise | Initiate, Enable and Ensure |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

| VULNERABILITY RESEARCHER | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 1 | **Information Security Governance and Strategy** | | | | | | | |
| 1.5 | **Legal and Regulatory Environment**<br>Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements. | Understand | Understand | Understand | Understand | Understand | Understand | Understand |
| 3 | **Systems Development and Implementation** | | | | | | | |
| 3.2 | **Systems Design**<br>The design of systems to meet specified requirements, compatible with agreed systems architectures, adhering to corporate standards and within constraints of performance and feasibility. The identification of concepts and their translation into a design which forms the basis for systems construction and verification. The design or selection of components. The development of a complete set of detailed models, properties, and/or characteristics described in a form suitable for implementation. The adoption and adaptation of systems design lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Not required | Enable | Enable | Enable | Enable |
| 3.3 | **Software Design**<br>The specification and design of software to meet defined requirements by following agreed design standards and principles. The definition of software, components, interfaces and related characteristics. The identification of concepts and patterns and the translation into a design which provides a basis for software construction and verification. The evaluation of alternative solutions and trade-offs. The facilitation of design decisions within the constraints of systems designs, design standards, quality, feasibility, extensibility and maintainability. The development and iteration of prototypes/simulations to enable informed decision-making. The adoption and adaptation of software design models, tools and techniques based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Understand | Apply | Apply | Enable | Enable |
| 3.4 | **Programming/Software Development**<br>The planning, designing, creation, amending, verification, testing and documentation of new and amended software components in order to deliver agreed value to stakeholders. The identification, creation and application of agreed software development and security standards and processes. Adopting and adapting software development lifecycle models, based on the context of the work, and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. | Not required | Not required | Understand | Apply | Enable | Advise | Advise |
| 4 | **Assurance: Audit, Compliance and Testing** | | | | | | | |
| 4.3 | **Security Evaluation and Functionality Testing**<br>Contributes to the security evaluation or testing of software. Evaluates security software by analysing the design documentation and code to identify potential vulnerabilities and testing to ascertain whether these are exploitable. Tests the security functionality of systems or applications for correctness in line with security policies, standards and procedures, and advises on corrective measures. Applies recognised evaluation/testing methodologies, tools and techniques, developing new ones where appropriate. Assesses the robustness of a system, product or technology. Applies commonly accepted governance practices and standards when testing in an operational environment. | Not required | Not required | Understand | Apply | Apply | Enable | Advise |
| 4.4 | **Penetration Testing**<br>The assessment of organisational vulnerabilities through the design and execution of penetration tests that demonstrate how an adversary can either subvert the organisation's security goals or achieve specific adversarial objectives. Penetration testing may be a stand-alone activity or an aspect of acceptance testing prior to an approval to operate. The identification of deeper insights into the business risks of various vulnerabilities | Not required | Not required | Not required | Apply | Apply | Enable | Enable |
| 5 | **Operational Security Management** | | | | | | | |
| 5.2 | **Secure Operations and Service Delivery**<br>Securely configures and maintains information, control and communications equipment in accordance with relevant security policies, standards and guidelines. This includes the configuration of information security devices (e.g. firewalls) and protective monitoring tools (e.g. SIEM). Implements security policy (e.g. patching policies) and security operating procedures in respect of system and/or network management. Undertakes routine technical vulnerability assessments. Maintains security records and documentation in accordance with security operating procedures. Administers logical and physical user access rights. Monitors processes for violations of relevant security policies (e.g. acceptable use, security, etc.). | Not required | Not required | Not required | Apply | Enable | Advise | Advise |

Not required · Knowledge · Understand · Apply · Enable · Advise · Initiate, Enable and Ensure

| VULNERABILITY RESEARCHER | | ASD LEVELS | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ASD2 | ASD3 | ASD4 | ASD5 | ASD6 | EL1 | EL2 |
| 6 | **Incident Management, Investigation and Forensics** | | | | | | | |
| 6.1 | **Intrusion Detection and Analysis**<br>Monitors network and system activity to identify potential intrusion or other anomalous behaviour. Analyses the information and initiates an appropriate response, escalating as necessary. Uses security analytics, including the outputs from intelligence analysis, predictive research and root cause analysis in order to search for and detect potential breaches or identify recognised indicators and warnings. Monitors, collates and filters external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes. Ensures that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available. Produces warning material in a manner that is both timely and intelligible to the target audience(s). | ○ | ○ | ○ | Understand | Understand | Understand | Understand |
| 7 | **Information Security Research** | | | | | | | |
| 7.1 | **Research**<br>The systematic creation of new knowledge by data gathering, innovation, experimentation, evaluation and dissemination. The determination of research goals and the method by which the research will be conducted. The active participation in a community of researchers; communicating formally and informally through digital media, conferences, journals, books and seminars. | ○ | ○ | Apply | Apply | Apply | Apply | Apply |
| 7.2 | **Applied Research**<br>Vulnerability research and discovery, leading to the development of exploits, reverse engineering and researching mitigation bypasses. Cryptographic research leading to the assessment of existing algorithms. In the information security field, uses existing knowledge in experimental development to produce new or substantially improved devices, products and processes. | ○ | ○ | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8 | **Management, Leadership, Business and Communications** | | | | | | | |
| 8.1 | **Supports Strategic Direction**<br>Supports shared purpose and direction; thinks strategically; harnesses information and opportunities; shows judgement, intelligence and common-sense. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.2 | **Achieves Results**<br>Builds ASD and the ACSC's capability and responsiveness by identifying, applying and building professional expertise; responds positively to change; takes responsibility for managing work projects to achieve results. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.3 | **Supports Productive Working Relationships**<br>Nurtures internal relationships; listens to, understands and recognises the needs of others; values individual differences and diversity; shares learning and supports others. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.4 | **Displays Personal Drive and Integrity**<br>Demonstrates public service professionalism and probity; engages with risk and shows personal courage; commits to action; promotes and adopts a positive and balanced approach to work; demonstrates self-awareness and a commitment to personal development. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 8.5 | **Communicates with Influence**<br>Communicates clearly; listens, understands and adapts to audience; negotiates confidently. | Knowledge | Knowledge | Understand | Apply | Enable | Advise | Initiate, Enable and Ensure |
| 9 | **Specialist Advice** | | | | | | | |
| 9.1 | **Specialist Advice**<br>The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice. | ○ | ○ | Enable | Enable | Enable | Advise | Initiate, Enable and Ensure |

○ Not required  Knowledge  Understand  Apply  Enable  Advise  Initiate, Enable and Ensure

# DIGITAL CAREER PATHWAYS

# DIGITAL CAREER PATHWAYS

To increase digital dexterity across the Australian Public Service (APS), in 2019, the Digital Transformation Agency worked closely with Commonwealth entities, including ASD, to develop the Digital Career Pathways for Information Security. The ASD Cyber Skills Framework was a guiding document for role and skill definitions, as well as proficiency levels within the Digital Career Pathways, and helped define the four underlying career pathways: Analysis, Architecture, Operations and Testing.

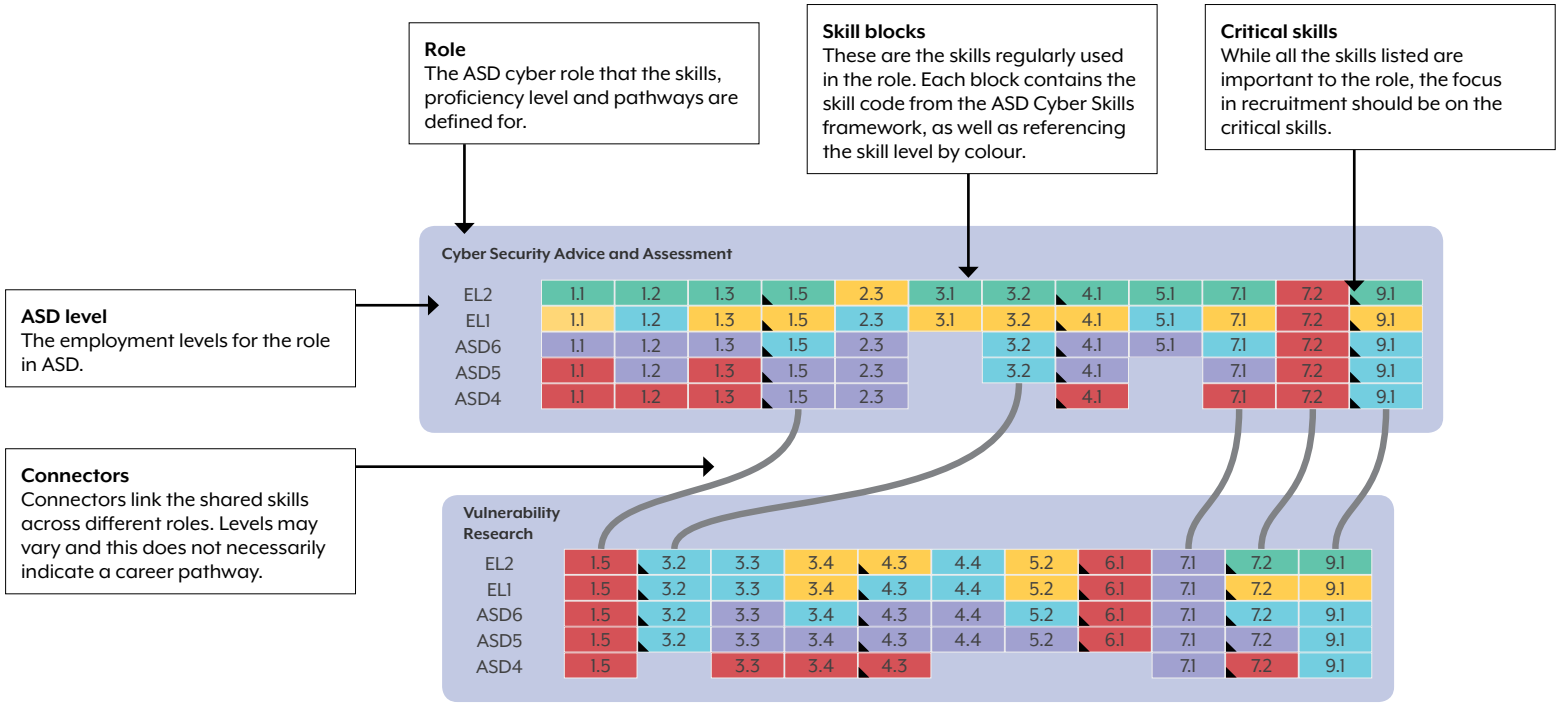
The Digital Career Pathways initiative aims to make career options within government flexible by providing employees with a clear view of where they are in their career and how to navigate their potential future. It provides guidance on how existing ICT skills can be utilised in other roles, and what new skills an employee might need in order to excel in those roles.

The Digital Career Pathways are designed to help answer two main questions for users:

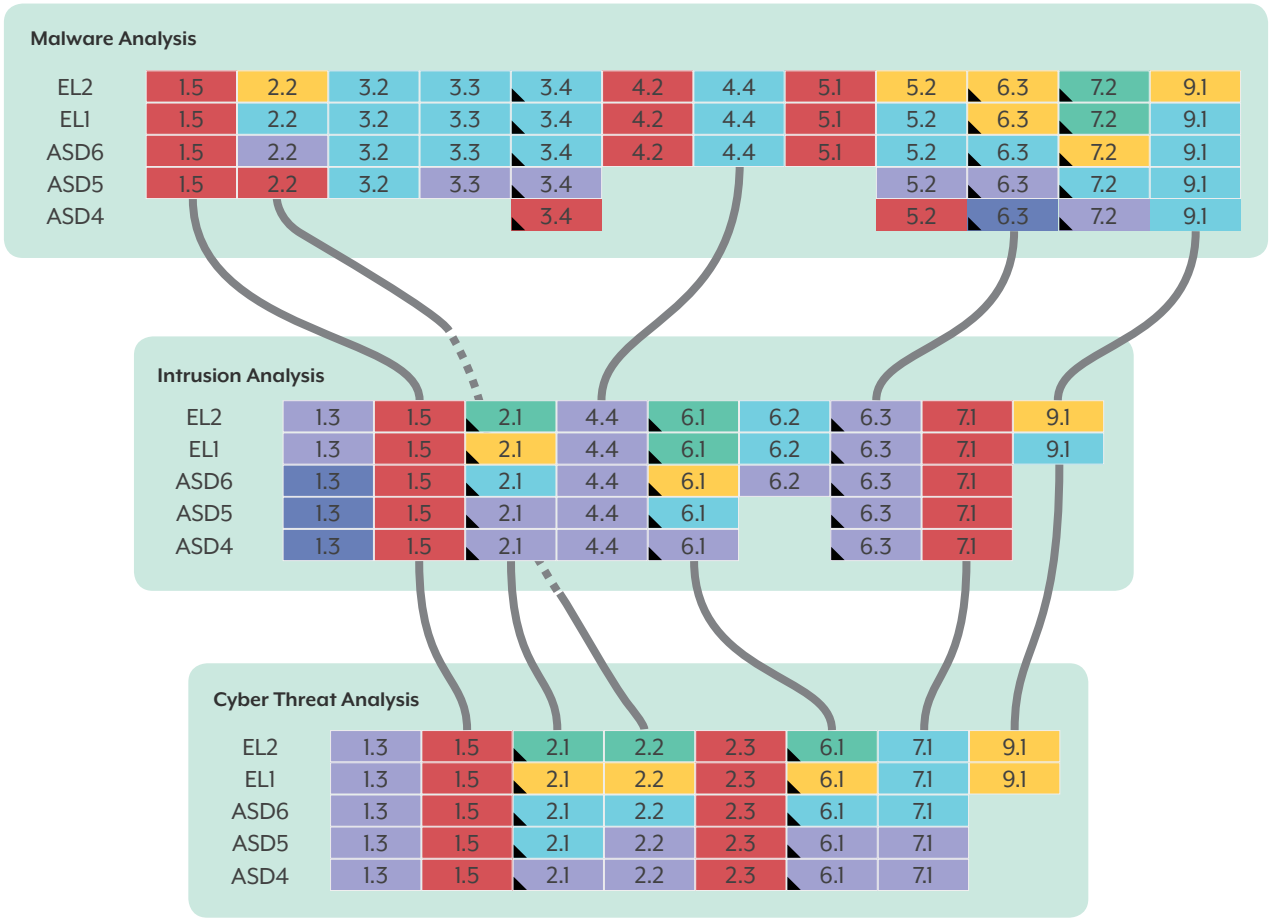
1. What skills and capabilities do you have?
2. What skills and capabilities do you need?

Exploring the Digital Career Pathways helps create a career pathway by identifying the roles available in cyber and what skills need to be developed in order to perform a role at a particular proficiency level.

# HOW TO READ A DIGITAL CAREER PATHWAY MAP



# CYBER SECURITY ANALYSIS CAREER MAP

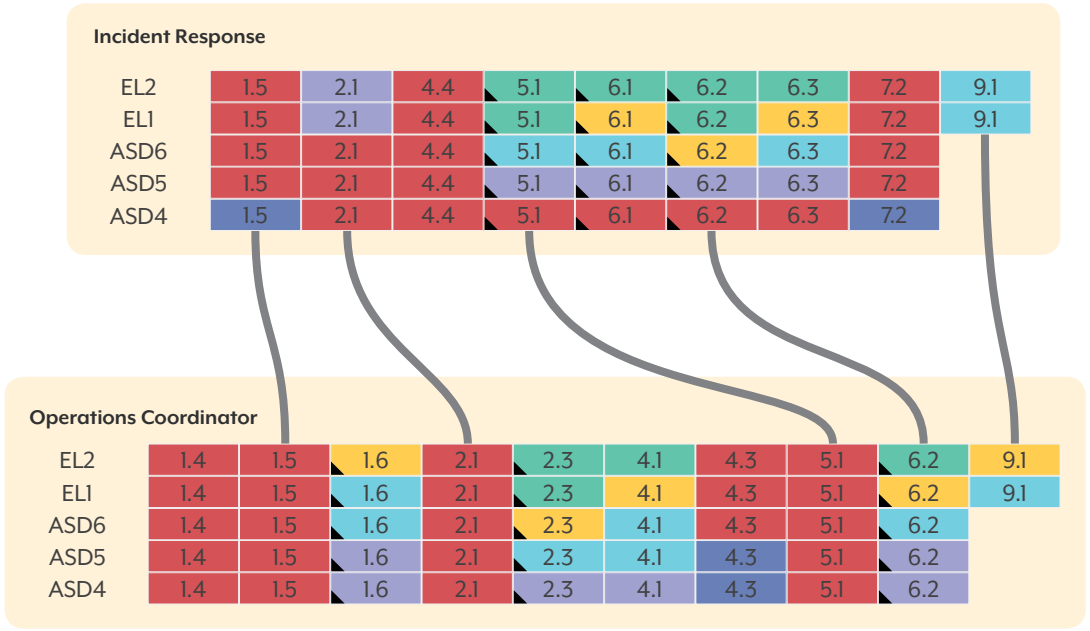



Initiate, Enable and Ensure
Advise
Enable
Apply
Understand
Knowledge

Critical skills
Indicated with black triangle

| Skills in detail | | |
|---|---|---|
| 1.1 Governance | 3.4 Programming/software development | 6.3 Digital Forensics |
| 1.2 Policy and Standards | 3.3 Software design | 7.1 Research |
| 1.3 Information Security Strategy | 4.2 Compliance Monitoring and Controls Testing | 7.2 Applied Research |
| 1.5 Legal & Regulatory Environment and Compliance | 4.4 Penetration Testing & conducting Simulated Attack Exercises | 9.1 Specialist advice |
| 2.1 Threat Intelligence, Assessment and Threat Modelling | 5.1 Secure Operations Management | |
| 2.2 Risk Assessment | 5.2 Secure Operations and Service Delivery | |
| 2.3 Information Risk Management | 6.1 Intrusion Detection and Analysis | |
| 3.2 Systems design | 6.2 Incident Management, Incident Investigation & Response | |

# CYBER SECURITY OPERATIONS CAREER PATHWAY

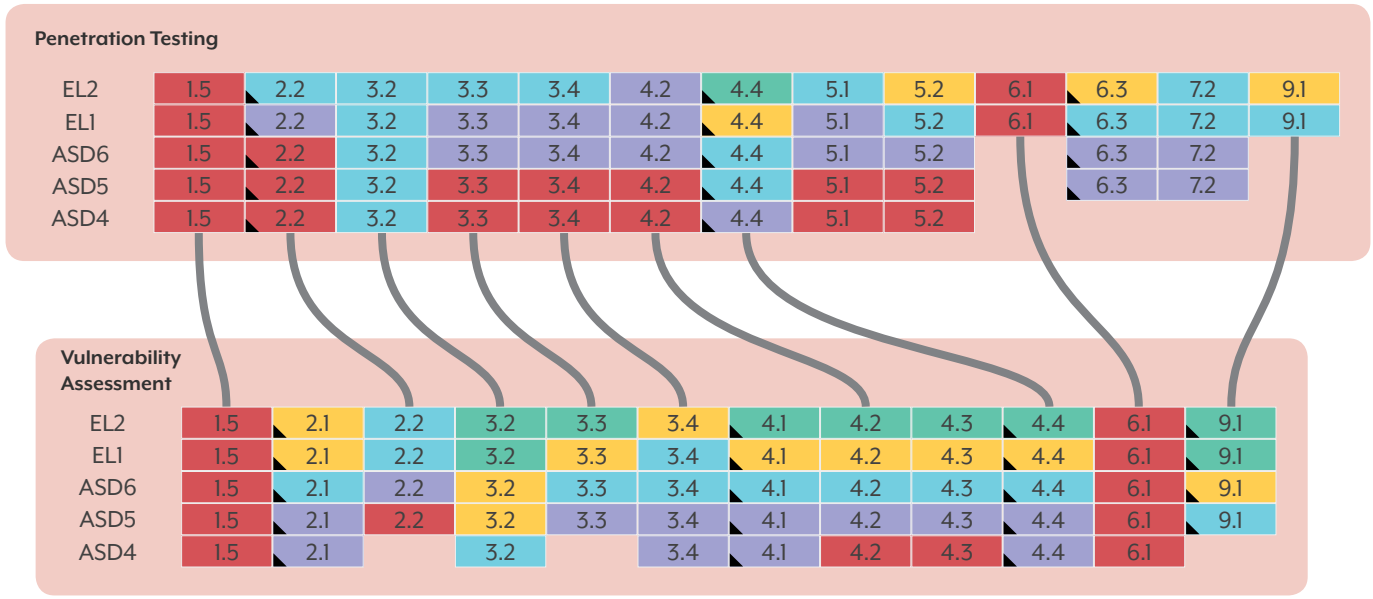



Initiate, Enable and Ensure
Advise
Enable
Apply
Understand
Knowledge

| Critical skills |
| --- |
| Indicated with black triangle |

| Skills in detail | | |
| --- | --- | --- |
| 1.4 Behavioural Change | 4.3 Security Evaluation and Functionality Testing | 7.2 Applied Research |
| 1.5 Legal & Regulatory Environment and Compliance | 4.4 Penetration Testing | 9.1 Specialist Advice |
| 1.6 Third Party Management | 5.1 Secure Operations Management | |
| 2.1 Threat Intelligence, Assessment and Threat Modelling | 6.1 Intrusion Detection and Analysis | |
| 2.3 Information Risk Management | 6.2 Incident Management, Incident Investigation & Response | |
| 4.1 Internal and Statutory Audit | 6.3 Forensics & Digital Forensics | |

# CYBER SECURITY TESTING CAREER PATHWAY

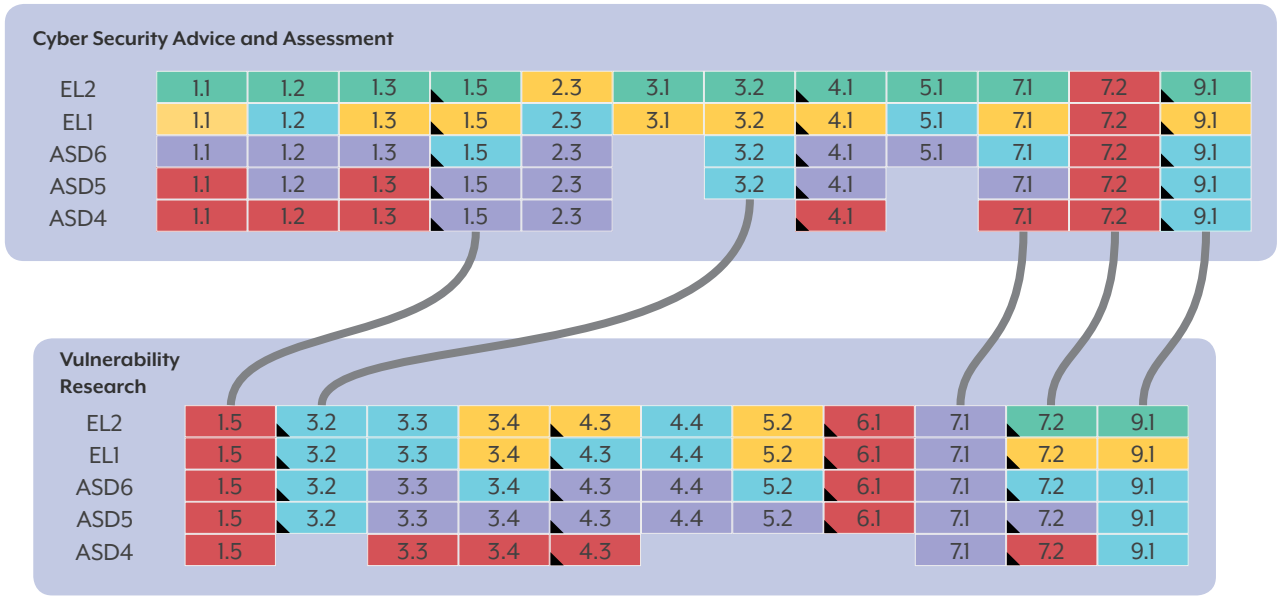



Initiate, Enable and Ensure
Advise
Enable
Apply
Understand
Knowledge

Critical skills
Indicated with black triangle

| Skills in detail | | |
|---|---|---|
| 1.5 Legal & Regulatory Environment and Compliance | 4.1 Internal and Statutory Audit | 5.2 Secure Operations and Service Delivery |
| 2.1 Threat Intelligence, Assessment and Threat Modelling | 4.2 Compliance Monitoring and Controls Testing | 6.1 Intrusion Detection and Analysis |
| 2.2 Risk Assessment | 4.3 Security Evaluation and Functionality Testing | 6.3 Digital Forensics |
| 3.2 Systems Design | 4.4 Penetration Testing & conducting Simulated Attack Exercises | 7.2 Applied Research |
| 3.3 Software Design | 5.1 Secure Operations Management | 9.1 Specialist Advice |
| 3.4 Programming/Software Development | 5.2 Secure Operations and Service Delivery | |

# CYBER SECURITY ARCHITECTURE CAREER PATHWAY




Initiate, Enable and Ensure
Advise
Enable
Apply
Understand
Knowledge

Critical skills
Indicated with black triangle

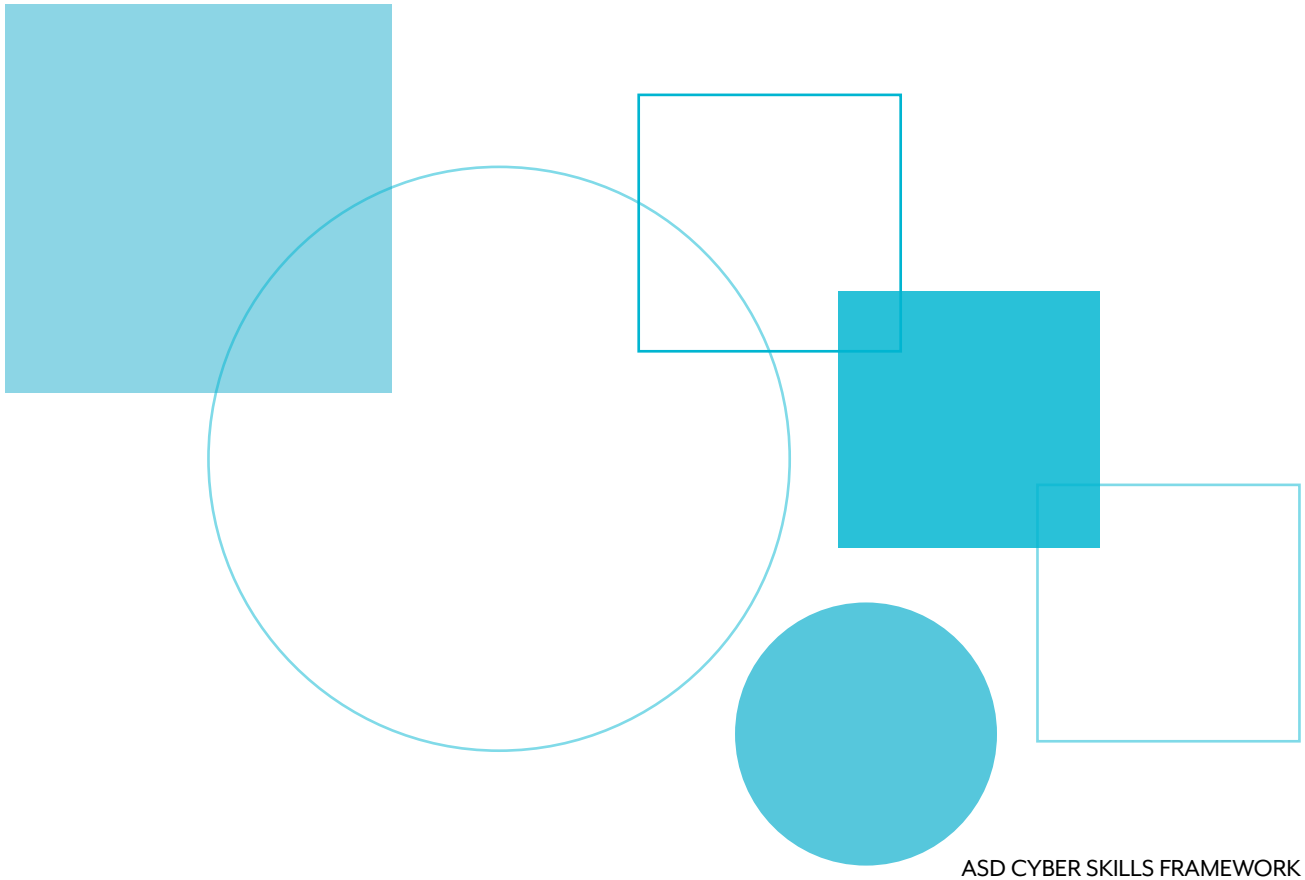
| Skills in detail | | |
|---|---|---|
| 1.1 Governance | 3.3 Software Design | 5.2 Secure Operations and Service Delivery |
| 1.2 Policy and Standards | 3.4 Programming/Software Development | 6.1 Intrusion Detection and Analysis |
| 1.3 Information Security Strategy | 4.1 Internal and Statutory Audit | 7.1 Research |
| 1.5 Legal & Regulatory Environment and Compliance | 4.3 Security Evaluation and Functionality Testing | 7.2 Applied Research |
| 2.3 Information Risk Management | 4.4 Penetration Testing & conducting Simulated Attack Exercises | 9.1 Specialist Advice |
| 3.1 Systems Development Management | 5.1 Secure Operations Management | |
| 3.2 Systems Design | | |

# LEARNING AND DEVELOPMENT PATHWAY

# INCIDENT RESPONSE LEARNING AND DEVELOPMENT PATHWAY

The Learning and Development Pathway is designed to support cyber practitioners' development of their professional and technical expertise and is an extension of the skills guidance provided in the ASD Cyber Skills Framework. The Learning and Development Pathway provides an understanding of the learning outcomes and objectives required to develop skills in different capabilities across proficiency levels, with indicative learning and development options.

The Incident Response Learning and Development Pathway identifies the key learning outcomes necessary for proficiency in the defined skill and level, which is complemented by suggested formal and experiential learning and development. This template can be used as a guide for developing Learning and Development Pathways for additional cyber roles.



INCIDENT RESPONDER CAREER DEVELOPMENT

| PROFICIENCY LEVEL | SKILLS | LEARNING OUTCOMES |
|---|---|---|
| **LEVEL 6**<br>**Expert Practitioner**<br>**(Initiate, Enable and Ensure)** | • Responsible to Senior Leadership regarding secure operations and service delivery for ASD.<br>• Experienced in handling major cyber security incidents, recognised as an authority across ASD and representing them for media comment.<br>• Responsible for deciding on and organising the appropriate corporate response to a cyber security incident.<br>• Sets policies, standards and guidelines about the way in which the organisation conducts digital forensic investigations. Authorises the release of formal forensics reports. | • How to communicate with clarity and technical expertise to non-technical audiences on behalf of ASD.<br>• How to evaluate cyber security incidents to assess risks and dependencies in order to make informed decisions when leading major investigations.<br>• How to guide and set the strategic mitigation strategies to prevent future incidents. |
| **LEVEL 5**<br>**Principal Practitioner**<br>**(Advise)** | • Manages intrusion and analysis teams. Responsible for taking decisions on appropriate response, escalating as necessary.<br>• Takes full responsibility for managing and investigating information security incidents.<br>• Ensures that the information security incident management processes are aligned with generic incident management and business continuity processes. Advises on corporate response to an incident.<br>• Conducts investigations to correctly gather, analyse and present the totality of findings, including digital evidence to business. Collates conclusions and recommendations and presents forensics findings to stakeholders. Contributes to the development of policies, standards and guidelines. Oversees all ASD incident response investigations and determines prioritisation of activity. | • How to summarise the incident recovery and post-incident response process.<br>• How to explain the relationship between frameworks, common policies, controls, and procedures.<br>• How to use data to recommend remediation of security issues related to identity and access management. |
| **LEVEL 4**<br>**Senior Practitioner**<br>**(Enable)** | • Develops or operates security management procedures and processes without close supervision.<br>• Operates as a member of an intrusion and analysis team without close supervision.<br>• Leads digital forensic investigations. Processes and analyses evidence in line with policy, standards and guidelines and supports production of forensics findings and reports. | • How to analyse threat data or behaviour to determine the impact of an incident.<br>• How to explain the importance of communication during the incident response process.<br>• How to analyse common symptoms to select the best course of action to support incident response. |
| **LEVEL 3**<br>**Practitioner**<br>**(Apply)** | • Develops or operates security management procedures and processes with some supervision. Operates as a member of an intrusion and analysis team under supervision.<br>• Contributes to information security incident management policy and/or incident management, investigation procedures and investigation processes under some supervision.<br>• Contributes to forensic activities with some supervision.<br>• Liaises with relevant threat intelligence partners. | • How to implement and maintain security controls.<br>• How to explain the purpose of practices used to secure a corporate environment.<br>• How to compare and contrast common vulnerabilities found within an organisation.<br>• How to prepare a toolkit and use appropriate forensics tools during an investigation. |
| **LEVEL 1 & 2**<br>**Learner / Novice**<br>**(Knowledge/Understand)** | • Can explain the basic principles involved in monitoring network and system activity for anomalous behaviour and how the results can be used.<br>• Can explain the basic principles of incident management, investigation and response.<br>• Can describe how incident management can operate effectively, benefiting whole of economy.<br>• Understands the need to preserve evidence to support any investigation and can explain the basic principles involved.<br>• Can explain the basic principles of digital forensics, including the principles and processes surrounding securing and analysing evidence. This might include experience of applying these principles in a training environment. | • How to compare and contrast the general purpose and reasons for using various security tools and technologies.<br>• How to support incident response activities.<br>• How to manage network security, including how to operate and configure network-based security devices.<br>• How analyse the output results from a vulnerability scan. |

INCIDENT RESPONDER CAREER DEVELOPMENT

| PROFICIENCY LEVEL | RECOMMENDED LEARNING AND DEVELOPMENT | SUGGESTED PROFESSIONAL DEVELOPMENT | EXPERIENTIAL LEARNING | RELATED CERTIFICATIONS |
|---|---|---|---|---|
| **LEVEL 6**<br>**Expert Practitioner**<br>**(Initiate, Enable and Ensure)** | • Router Incident Response<br>• JTAG<br>• Hardware Reversing | • Be an industry leader, internally and externally<br>• Make contributions to the industry, e.g. via professional bodies | | |
| **LEVEL 5**<br>**Principal Practitioner**<br>**(Advise)** | • REDHAT 300 Certified Engineer<br>• iOS Internals<br>• Android internals<br>• SANS SEC660: Advanced Pen Testing<br>• Pen Testing with Kali<br>• Windows Internal<br>• Cyber Ethics | • Coach and mentor junior staff<br>• Become a fellow of a professional industry body | • Quality Control Analysis<br>• Vulnerability Management | • CISSP – ISSMP<br>• CISSP<br>• CISM |
| **LEVEL 4**<br>**Senior Practitioner**<br>**(Enable)** | • Advanced C++ and Python<br>• SANS SEC560: Network Pen Testing<br>• Offensive PowerShell<br>• Introduction to Software Reverse Engineering<br>• REDHAT 200 Certified Systems Administrator | • Develop skills in area of interest to become a Subject Matter Expert<br>• Contribute to Learning & Development design and material<br>• Become a mentor | • Offensive PowerShell<br>• Penetration Testing<br>• Trends Analysis | • CREST: Certified Incident Manager<br>• SANS SEC560: Network Pen Testing |
| **LEVEL 3**<br>**Practitioner**<br>**(Apply)** | • Intermediate C++ and Python<br>• SANS SEC508: Advanced Intrusion Forensics<br>• Bash<br>• Microsoft Configuring Windows Servers<br>• Splunk<br>• Clouderra | • Volunteer for outreach activities | • PowerShell<br>• Malware Analysis<br>• Data/network Analysis<br>• Information Assurance | • SANS SEC508: Advanced Intrusion Forensics<br>• CISMP<br>• SSCP |
| **LEVEL 1 & 2**<br>**Learner / Novice**<br>**(Knowledge/Understand)** | • Introduction to C++ and Python<br>• SANS SEC408: Forensics basics<br>• SANS SEC504: Incident Handling | • Seek and engage a mentor<br>• Volunteer for outreach activities<br>• Actively pursue learning & development opportunities online via Cybrary.it and Open Universities | • Incident Handling<br>• Digital Forensics | • SANS SEC408: Forensics basics<br>• SANS SEC504: Incident Handling |

# COMPLEMENTARY FRAMEWORKS

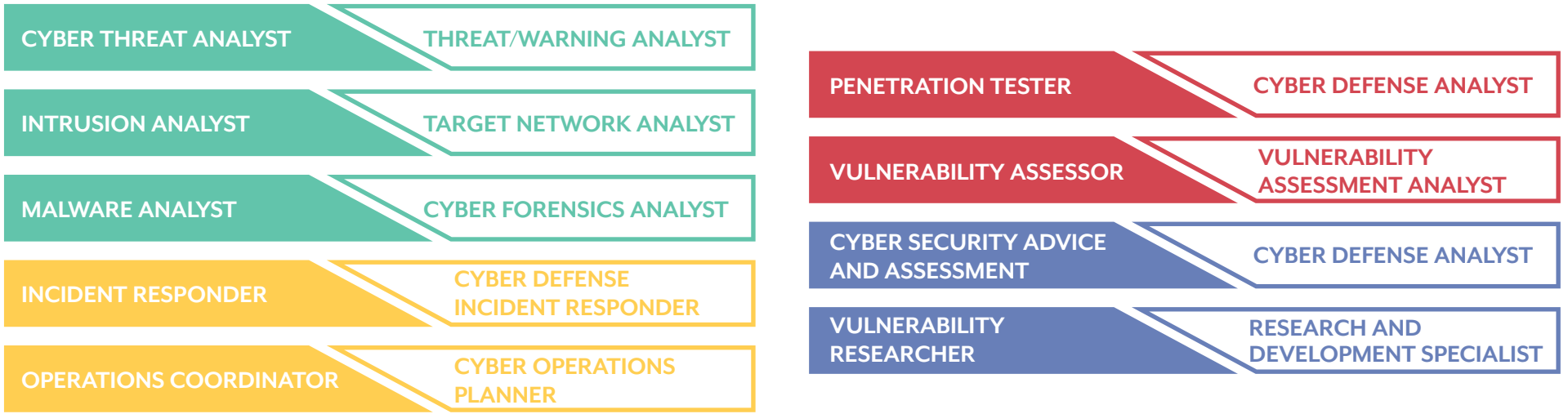
# ASD CYBER SECURITY ANALYSIS ROLES MAPPED TO NICE CYBERSECURITY WORKFORCE FRAMEWORK

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework was published in August 2017 by the National Institute of Standards and Technology, within the US Department of Commerce. The NICE Framework is used as a reference document that describes seven key categories of work roles which define speciality areas, and details the knowledge, skills and abilities (KSAs) of cyber security work roles.

The NICE Framework is recommended for use as a source to further develop and complement custom skills frameworks, where the cyber security workforce is extensive and has a requirement for comprehensive KSAs at defined proficiency levels.

The ASD Cyber Skills Framework and the NICE Framework are complementary and can be used to address cyber skills development, especially at the entry level. While the ASD Cyber Skills Framework defines the core capabilities and skills of nine cyber security roles, the NICE Framework defines entry level KSAs for 52 work roles relevant to the US cyber eco-system.

To enable Australian academic institutions, which are implementing the NICE Framework, to understand how NICE KSAs translate to entry level cyber security roles in Australian government, the following graphic demonstrates the best fit translation of ASD cyber roles to work roles identified in the NICE Framework, based on definition, duties, role expectations and KSAs.



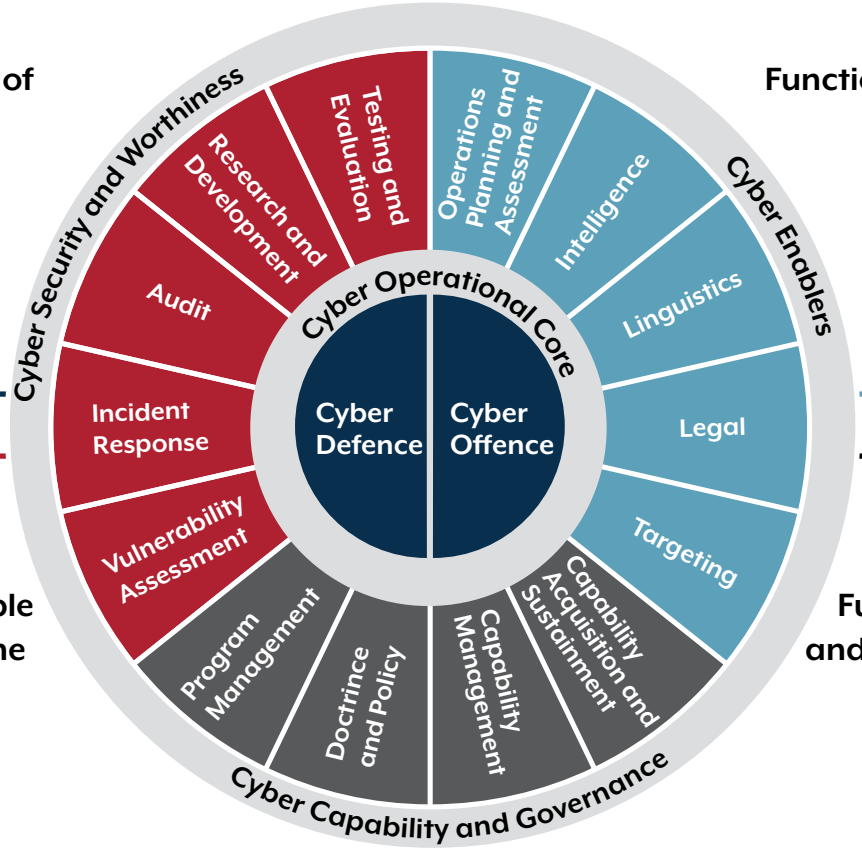
# ADF CYBERSPACE PROFESSIONAL FRAMEWORK

The Australian Defence Force (ADF) Cyberspace Professional Framework provides a common workforce definition for the ADF Cyberspace capability to better enable the collective maintenance of a sustainable, integrated and interoperable ADF cyberspace workforce. The ADF Cyberspace Professional Framework and the ASD Cyber Skills Framework have been developed using the same guiding principles: create a common taxonomy, support professional development, describe the cyber workforce and be fit for purpose for the intended audience.

ASD and the ADF are committed to working in partnership in support of Defence missions, including cyber operations. ASD and ADF Information Warfare Division share a strong partnership and are working together to address cyber skills now and in the future.

**CYBER OPERATIONAL CORE**
**Key functions for the execution of cyber operations.**

**CYBER ENABLERS**
**Functions to support the execution of cyber operations.**




**CYBER SECURITY AND WORTHINESS**
**Functions to establish favourable cyberspace environments for the conduct of operations.**

**CYBER CAPABILITY AND GOVERNANCE**
**Functions that provide guidance and oversight for cyber operations and capability generation.**

# ASD CYBER SKILLS FRAMEWORK REFERENCE PAGE

**Chartered Institute of Information Security (CIISec)**
www.ciisec.org

**Skills Framework for the Information Age (SFIA)**
www.sfia-online.org

**Australian Public Service Commission (APSC) Integrated Leadership System (ILS)**
https://www.apsc.gov.au/integrated-leadership-system-ils-0

**National Institute for Cybersecurity Education (NICE) Workforce Framework**
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

**Digital Career Pathways, Digital Transformation Agency (DTA)**
https://data.gov.au/data/dataset/aps-digital-career-pathways

**Digital Professional Stream**
https://www.apsc.gov.au/aps-digital-professional-stream

**Defence White Paper 2016**
https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf

ASD.GOV.AU