DE&S

Security Profession

Competency Framework

Introduction

The DE&S Security Profession Technical Competencies align closely with those within the skills detailed in the Government Security Profession and SFIA frameworks.

DE&S Skill Level Definitions
Awareness Applies knowledge and experience of the skill, including tools and techniques, adopting those most appropriate for the environment.
Supervised Practitioner * Applies knowledge and experience of the skill with others, including tools and techniques, adopting those most appropriate for the environment. *This level is known as 'Working' in the GSP framework
Practitioner Shares knowledge and experience of the skill with others, including tools and techniques, defining those most appropriate for the environment.
Expert Has knowledge and experience in the application of this skill. Is a recognised specialist and adviser in this skill including user needs, generation of ideas, methods, tools and leading or guiding others in best practice use.

Contents

Applied Personnel Security

Applied Personnel Security refers to the policies, practices and methodologies that seek to mitigate the risk of workers (insiders) exploiting legitimate access to an organisation's assets for unauthorised purposes.

Level	Descriptors
Awareness	• Describes concepts of Personnel Security, including the significance of the Personnel Security specialism, the relationship between all specialisms and how the specialisms relate to the security function across government • Promotes Personnel Security within the local working environment
Supervised Practitioner	• Applies concepts of Personnel Security within the context of the other specialisms/enablers. • Champions Personnel Security within the wider security function, providing advice to others.
Practitioner	• Develops and applies new concepts in Personnel Security, involving the other specialisms/enablers • Develops individuals and contributes to the development of the specialism • Promotes Personnel Security as a business enabler throughout the organisation • Engages with the UK security community
Expert	• Leads innovation in Personnel Security, taking into account other specialisms/enablers and business drivers • Promote the development of individuals against the career framework • Promote the use of Personnel Security as a business enabler at board or senior management level • Active member of the UK security community

Applied Physical Security

Applied Physical Security refers to the policies, practices and methodologies used to protect assets, including people, services, infrastructure, systems, places, equipment and networks.

Level	Descriptors
Awareness	• Describes concepts of Physical Security, including the significance of the Physical Security specialism, the relationship between all specialisms, and the how the specialisms relate to the security function across government • Promotes Physical Security within the local working environment.
Supervised Practitioner	• Applies concepts of Physical Security within the context of the other specialisms. • Promotes Physical Security as a business enabler within the security profession.
Practitioner	• Develops and applies new concepts in Physical Security, involving the other specialisms. • Promotes Physical Security as a business enabler throughout DE&S, providing advice to others.
Expert	• Leads innovation in Physical Security, taking into account other specialisms and business drivers. • Promotes Physical Security as a business enabler at senior manager and board level.

Applied Research

Applied research is the understanding and application of research methods to assure and maintain best practice within an organisation. The principles of applied research are vulnerability research and discovery. They lead to the development of exploits; reverse engineering and researching mitigation bypasses; cryptographic research leading to the assessment of existing algorithms; and the use of existing knowledge in experimental development to produce new or substantially improved devices, products and processes.

Level	Descriptors
Awareness	• Describes the basic principles of applied research and how it applies to security. • Conducts basic applied research under supervision.
Supervised Practitioner	• Explains the principal requirements of applied research and applies methods correctly. • Conducts basic applied research.
Practitioner	• Leads teams conducting applied research. • Advises colleagues on choice and application of research methods to assure best practice.
Expert	• Leads applied research activities for DE&S. • Undertakes advanced research. • Helps DE&S adopt a wide range of research methods. • Leads a community of practice to help DE&S continually assure, improve and innovate their research.

Applied Security Capability

Applied security capability is formed of a set of complementary security skills. Individual roles may have a requirement for a different profile across these skills. Applied security capability involves 4 elements: 1. Security requirement elicitation: gathering and deriving meaningful security requirements to support an identified need 2. Application of security capabilities: apply standardised or unique security capabilities to address security needs 3. Provision or assurance and confidence: provide confidence that business priorities are appropriately protected 4. Security and risk reporting: communicate security and risk effectively.

Level	Descriptor
Awareness	• Understands why security must support business needs and the importance of being able to demonstrate that relationship. • Aware of some key, well-understood, security principles and can demonstrate an awareness of some Cyber Security relevant technologies. • Understands why it is important to gain confidence in security measures and can describe some straightforward mechanisms such as pen-tests. • Understands and can describe basic security concepts.
Supervised Practitioner	• Aware of the need to provide traceability between business need and security requirements. • Gathers and derives simple or obvious security requirements for highly standardised use cases, using well-established guidance that is unlikely to be contentious. • Provides basic security advice to address standard security needs. Advice could be written or verbal. Knows the limitations and scope for what advice can be given and when to draw on others' expertise. • Is aware of and follows appropriate process such as quality control arrangements. • Understands and can apply a range of basic approaches to assurance and understands their applicability. • Meaningfully describes straightforward security concepts and their business applicability. • Ensures security recommendations and risk statements developed are reasonably and well contextualised to the business need under consideration.
Practitioner	• Elicits security requirements based on straightforward approaches such as threat/vulnerability/impact analysis. Security needs will include an understanding of the user as part of the overall system. • Helps organisations to derive and reason about their security needs, such as understanding and applying security principles to particular business scenarios. • Interprets and clarifies management or organisational intention with regards to security, such as described in risk appetite statements. This includes interpreting such statements into meaningful and appropriate security requirements.

	• Provides security advice to non-standard use cases, drawing on and using experts in specific topics or technologies. • Uses standardised control frameworks (such as 27001/2) appropriately, with awareness of their strengths and limitations. • Understands when security measures might impact on users or business needs and provides effective advice to help the business make an appropriate decision. • Applies a range of assurance approaches, with a clear understanding of the strengths and limitations of each approach. There is a clear ability to map the assurance options recommended directly to the security need to be addressed. • Assurance and confidence is not limited to a point in time but seeks to address confidence across the system/service life cycle. • Provides meaningful security and risk communication in a range of scenarios. • Understands and takes account of the limitations of various risk communication mechanisms such qualitative v quantitative approaches.
Expert	• Considers complicated, non-obvious security needs, e.g. where the connections between business need, the technology that supports that need and how it might be impacted are important to work out. • Works closely with those who 'own' business needs, deduces their tolerances with regard to things they care about and turns those into meaningful security statements that can be applied. This might be either complicated and specific, or simple scenarios with broad applicability. • Delivers security advice that is contextualised and appropriate for the strategic customer need. • Avoids providing 'point' solutions or advice that does not address the overall key need. Looks at the wider 'system' including sociotechnical considerations (e.g. the role the user plays in meeting the desired security outcomes) • Provides security advice that extends beyond particular technologies of which the candidate is familiar and draws upon and directs appropriate expertise to solve the bigger security problem. Ensures the overall technical coherence and quality of advice. • Together with assurance experts, develops and applies novel approaches to assurance of products/systems/services. • Understands and applies different approaches to product, implementation and operational assurance. Uses each appropriately to derive a genuine understanding of confidence that the overall business objective is protected. • Provides technical leadership for specific experts (be they pen-testers, product or behavioural assurance, for example) in the context of a specific technical assurance or confidence challenge. • Effectively communicates difficult risk and security concepts in accessible ways that can be clearly understood by business leaders. Contributes to and develops risk communication strategies.

Applied Technical Security

Applied Technical Security refers to the policies, practices, and methodologies used to protect sensitive information and technology from close acquisition or exploitation by hostile actors, as well as other forms of technical manipulation.

Level	Descriptor
Awareness	• Describes concepts of Technical Security, including the significance of the Technical Security specialism, the relationship between all specialisms, and how the specialisms relate to the security function across government. • Promotes Technical Security within the local working environment.
Supervised Practitioner	• Applies concepts of Technical Security within the context of the other specialisms/enablers • Champions Technical Security within the wider security function, providing advice to others.
Practitioner	• Develops and applies new concepts in Technical Security, involving the other specialisms/enablers. • Develops individuals and contributes to the development of the specialism. • Promotes Technical Security as a business enabler throughout the organisation. • Engages with the UK security community.
Expert	• Leads innovation in Technical Security, taking into account other specialisms/enablers and business drivers. • Promotes the development of individuals against the career framework. • Promotes the use of Technical Security as a business enabler at board or senior management level. • Active member of the UK security community

Business Continuity Management

Business continuity management helps mitigate risks to the disruption of an organisation or service, by identifying critical elements including information, assets and infrastructure, and then planning to ensure that the organisation or service can operate to the extent required in the event of a disruption.

Level	Descriptor
Awareness	• Describes the basic principles of business continuity management. • Follows documented business continuity management principles and guidelines.
Supervised Practitioner	• Explains the importance of business continuity management. • Follows documented principles and guidelines for business continuity management activities. • Assists with the design, development and implementation of business continuity management. • Assists with the implementation and execution of business continuity management.
Practitioner	• Leads business continuity management activities at team level. • Advises others on principles and guidelines for business continuity management activities. • Leads teams designing, developing and implementing business continuity management. • Promotes the sharing of business continuity management best practice.
Expert	• Leads business continuity management activities for DE&S. • Promotes business continuity management principles and guidelines. • Advises others on business continuity management processes providing thought leadership to the field. • Champions business continuity management best practice at senior manager and board level.

Cyber Security Operations

Cyber Security operations are the secure configuration and maintenance of information, controls 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. Security Information and Event Management (SIEM)). Principles include implementing security policy (e.g. patching policies) and security operating procedures in respect of system and/or network management, maintaining security records and documentation in accordance with security operating procedures, and monitoring processes for violations of relevant security policies (e.g. acceptable use, security).

Level	Descriptor
Awareness	• Recognises the need for information systems and services to be operated and monitored securely and can list some of the main policies and practices involved in achieving this. • Explains the main principles of secure configuration of role specific security components and devices, including firewalls and protective monitoring tools (e.g. SIEM)
Supervised Practitioner	• Demonstrates experience applying the principles of secure configuration of role-specific security components and devices in a training or academic environment, for example through participation in syndicate exercises, undertaking practical exercises, and/or passing a test or examination. • Supports the overall aims of a Cyber Security operations-related team, e.g. a monitoring team. • Applies routine security procedures appropriate to the role, such as patching, managing access rights, malware, protection or vulnerability testing under direction/supervision. • Develops and tests rules for detecting violations of security operating procedures under supervision.
Practitioner	• Develops security operating procedures for use across multiple information systems or maintains compliance with them. • Applies routine security procedures appropriate to the role, such as patching, managing access rights, malware protection or vulnerability testing with autonomy. • Develops and tests rules for detecting violations of security operating procedures with autonomy. • Leads small teams managing Cyber Security operations within an organisation.
Expert	• Leads teams managing Cyber Security operations within an organisation. • Identifies the need for, and implements, new security operating procedures and practices to meet changing requirements. • Is a subject matter expert in developing and operationalising techniques for Cyber Security operations, e.g. detecting anomalous activity, automating orchestration and configuration of IT.

Incident management, incident investigation and response management

Incident management, incident investigation and response refers to the set of processes, procedures and systems used to reduce the harm caused to victims of cyber incidents and deter future attacks. The principles of the skill include engagement with the overall organisation incident management process to ensure that information security incidents are handled appropriately, defining and implementing processes, procedures and configuring system policies for responding to and investigating information security incidents, establishing and maintaining a Computer Emergency Response Team (CERT) and systems to deal with information security incidents.

Level	Descriptor
Awareness	• Describes the basic principles of incident management, incident investigation and response. Implements processes, procedures and systems for responding to and investigating incidents. • Follows documented principles and guidelines for incident management, incident investigation and response activities with supervision.
Supervised Practitioner	• Contributes to incident management, incident investigation and response policy and/or incident management processes, procedures and systems. • Follows documented principles and guidelines for incident management, incident investigation and response activities with limited direction/supervision.
Practitioner	• Defines incident management, incident investigation and response policy and/or incident management and investigation processes, procedures and systems. • Follows documented principles and guidelines for incident management, incident investigation and response activities. • Advises others on incident management, incident investigation and response processes.
Expert	• Champions incident management, incident investigation and response policy and/or incident management and investigation processes, procedures and systems • Shapes incident management, system response, incident investigation and response principles and guidelines for incident management activities • Advises on corporate and systems response to an incident. • Promotes incident management, incident investigation and response best practice. • Monitors the effectiveness of reporting.

Information risk assessment and risk management

Information risk assessment and risk management identifies and evaluates security risks to information, systems, and processes owned by the organisation, and proactively provides appropriate advice, drawing on a wide variety of sources, to stakeholders across the organisation and at a variety of levels.

Level	Descriptor
Awareness	• Demonstrates knowledge of risk assessment and risk management theory and approaches • Understands how risk management supports business or organisational objectives. • Understands and can follow routine organisational governance processes for security and risk management.
Supervised Practitioner	• Supports security professionals in carrying out risk assessments and developing mitigation strategies for relatively common and well-understood scenarios. • Has an understanding of, and can apply, the fundamental principles of risk assessment, risk management processes and decision-making.
Practitioner	• Understands the organisation's business drivers and approach to managing risk to support delivery of balanced and cost-effective risk management decisions on situations with a relatively well-defined scope. Relates risk to corporate governance, organisational strategic direction and planning. • Delivers or reviews risk assessments using appropriate risk assessment methods for common scenarios such as enterprise IT systems. • Inspects and reports on the security characteristics of systems with straightforward scope. • Has a good understanding of how assessed risks are addressed as part of an approach to risk treatment
Expert	• Enables the organisation to deliver balanced and cost-effective risk management decisions on situations with complex scope or significant risk. Ensures that risk is embedded into corporate governance processes. • Integrates risk management processes into appropriate business activities such as system development, security architecture or procurement. • Develops approaches to effectively report risk (including through system life cycles) to management who are responsible for risk to a given system or capability. This includes the ability to interpret management risk direction to others (such as developers or other security professionals) • Delivers comprehensive risk assessments for complicated or novel scenarios, using methodologies appropriate to the situation. Understands in detail how the risk assessment output dovetails into the risk management process. • Determines and understands the security characteristics of complicated or novel systems.

Intrusion detection and analysis

Intrusion detection and analysis consists of network and system activities to identify potential intrusion or other anomalous behaviour. Processes, methods and procedures include information analysis, security analytics including outputs from intelligence analysis, predictive research, and root cause analysis, vulnerability report analysis, and the production of warning materials. Further principles of the skill include monitoring, collating and filtering external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes, and ensuring that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available.

Level	Descriptor
Awareness	• Describes the basic principles of intrusion detection and analysis including the difference between intrusion prevention and intrusion detection. • Follows documented principles and guidelines for intrusion detection and analysis activities. • Implements intrusion detection and analysis processes and procedures.
Supervised Practitioner	• Understands and explains the basic principles of monitoring network and system activity to identify potential intrusion or other anomalous behaviour. • Uses information provided from various sources to identify, analyse, and report events that occur or might occur within the network. Uses a range of methods and procedures to identify, acquire, and preserve artefacts by means of controlled and documented analytical and investigative techniques. • Understands the business context of the activities. • Educates others on policies, procedures and guidelines relating to monitoring and analysing network and system activity.
Practitioner	• Understands and explains advanced principles of monitoring network and system activity to identify potential intrusion or other anomalous behaviour and applies the results in investigations. • Collects information from a variety of sources (e.g. data from cyber defence tools, system logs) and uses it to identify, analyse, and report events that occur or might occur within the network. Uses a range of advanced methods and procedures (including intelligence analysis, predictive research, root cause analysis, vulnerability report analysis) to identify, acquire, analyse and preserve artefacts by means of controlled and documented analytical and investigative techniques. • Supervises and manages teams undertaking intrusion detection and analysis. • Creates policies, procedures and guidelines based on intrusion detection and analysis standards. • Advises others on intrusion detection and analysis. • Tailors and refines systems and processes to meet the organisation’s needs.

Expert	• Understands and explains advanced monitoring of network and system activity to identify potential intrusion or other anomalous behaviour and applies the results in complex investigations. • Collects or oversees collection of information from a variety of sources (e.g. data from cyber defence tools, system logs) and uses it to identify, analyse, and report events that occur or might occur within the network. Uses a range of advanced methods and procedures (including intelligence analysis, predictive research, root cause analysis, vulnerability report analysis), developing techniques and tools where necessary, to identify, acquire, analyse and preserve artefacts by means of specialist analytical and investigative techniques. • Leads and oversees intrusion detection and analysis function and activities for an organisation. • Shapes intrusion detection and analysis strategy, policy, procedures and guidelines within the organisation and influences developments in the field at a national level • Advises and influences senior management on intrusion detection and analysis matters. • Defines, articulates and communicates required capabilities and tools.

Legal and Regulatory Environment and Compliance

Legal and regulatory environment and compliance refers to an organisation's adherence to laws, regulations, guidelines and specifications relevant to its business processes. It consists of a blend of compliance requirements and assurance capabilities. Principles of the skill include understanding the legal and regulatory environment within which the business operates, ensuring that information security governance arrangements are appropriate, and ensuring that the organisation complies with legal and regulatory requirements.

Level	Descriptor
Awareness	• Describes the major legislative regulatory instruments relevant to security and regulation relevant to the role. • Maintains understanding of regulations that will impact the role. • Follows documented procedures for compliance or regulations.
Supervised Practitioner	• Explains the principal requirements of major legislative regulatory instruments relevant to security, and the legal and regulation relevant to the role. • Reviews and implements alterations to operating procedures in response to changes in regulations. • Reports residual non-compliance to management in accordance with DE&S procedures.
Practitioner	• Advises others on the principal requirements of major legislative regulatory instruments relevant to security, and the legal and regulation relevant to the role. • Provides oversight of the range of regulations that impact the security profession and the interactions between them. • Designs and leads implementation of business change, where required by regulation. • Reports residual non-compliance to senior management in accordance with DE&S procedures.
Expert	• Leads the application of major legislation and regulations relevant to security, to ensure security is a business enabler. • Champions opportunities that regulation and compliance can provide at senior manager and board level. • Promotes regulation and compliance within the security profession.

Protective Security

Protective security encompasses the combination and multi-layering of appropriate and proportionate Physical, Personnel and Cyber Security measures to help identify and respond to any attack. Security requirements will change accordingly with the locally identified threats and vulnerabilities.

.

Level	Descriptor
Awareness	• Maintains an up-to-date understanding of fundamentals of all areas of security (especially in the context of government), and appreciates the importance of making use of a combination and multi-layering of appropriate and proportionate Physical, Personnel and Cyber Security measures to protect assets • Identifies aspects from across the breadth of the security field • Promotes protective security, providing advice to others
Supervised Practitioner	• Applies concepts of protective security within the context of the other specialisms/enablers, and keeps knowledge up to date • Champions protective security within the wider security function, providing advice to other procedures.
Practitioner	• Develops and applies new concepts in protective security, involving the other specialisms, including the Corporate Enablers • Develops individuals and contributes to the development of protective security practices • Promotes protective security as a business enabler throughout the organisation • Engages with the UK security community
Expert	• Leads innovation in protective security, taking into account other specialisms/enablers and business drivers. • Promotes the development of individuals against the career framework. • Promotes the use of protective security as a business enabler at board or senior management level. • Is an active member of the UK security community. •

Risk Understanding & Mitigation

Risk understanding and mitigation identifies and evaluates security risks to information, systems and processes owned by the organisation, and proactively provides appropriate advice, drawing on a wide variety of sources, to stakeholders across the organisation and at a variety of levels. Principles of the skill include developing 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.

Level	Descriptor
Awareness	• Develops basic cost-effective risk management plans. • Supports risk assessment and mitigation plan development. • Follows documented principles and guidelines for risk understanding and mitigation. • Relates risk to corporate governance, organisational strategic direction and planning. • Develops basic cost-effective risk management plans. • Supports risk assessment and mitigation plan development. • Follows documented principles and guidelines for risk understanding and mitigation. • Relates risk to corporate governance, organisational strategic direction and planning.
Supervised Practitioner	• Interprets sources of threat information for the local environment and applies knowledge of the external environment. • Maintains understanding of local and strategic threat environments, and trends affecting the landscape, and can apply to inform and provide context. • Uses local and strategic threat information in decision-making and planning. • Communicates tailored threat information to relevant local stakeholders within the organisation.
Practitioner	• Develops complex and innovative risk management plans, enabling the organisation to deliver balanced and cost–effective risk management decisions based on advanced threat principles and concepts. • Leads risk assessment and mitigation plan development. • Ensures that risk is embedded into corporate governance processes and integrates risk management processes into appropriate business activities.
Expert	• Leads risk management within an organisation, enabling senior leadership to make effective risk-based business decisions. • Leads on the provision of top-end risk understanding and mitigation advice. • Integrates risk understanding and mitigation processes into appropriate business activities. • Develops approaches to effectively report risks and delivers comprehensive risk assessments.

Secure Operations Management

Secure operations management refers to the ongoing operation, management and continuous improvement of security capabilities throughout an organisation through policies, procedures and guidelines. Principles of the skill include creating and maintaining system understanding, including hardware and software inventories; establishing 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; assessing and responding to new technical, physical, personnel or procedural vulnerabilities; engaging with suppliers, penetration testers and the change management process to ensure that vulnerabilities are mediated; and managing the implementation of information security programmes, coordinating security activities across the organization.

Level	Descriptor
Awareness	• Describes the basic principles of secure operations management. • Follows documented principles and guidelines for secure operations management activities. • Implements secure operations management processes and procedures.
Supervised Practitioner	• Explains the main processes for secure operations management. • Understands the business context in which policies, procedures and guidelines sit. • Implements secure operations management processes and procedures.
Practitioner	• Applies standards into secure operations management. • Responds to challenges to policies, procedures and guidelines and implements continuous improvements. • Identifies and implements new management controls to reflect changes in factors such as threat levels and legislation.
Expert	• Shapes policies, procedures and guidelines within DE&S and wider MOD. • Implements business change as a result of policies, procedures and guidelines. • Champions the need for and the business benefits of management controls.

Secure Supply Chain Management

Secure supply chain management refers to the activities, processes and procedures related to protecting the operations across a logistics network regarding the moving of a product or service from supplier to customer and from concept to disposal. Secure supply chain management can be divided into 4 sections: (1) understand the risks; (2) establish control; (3) check your arrangements; and (4) continuous improvement.

Level	Descriptor
Awareness	• Implements secure supply chain management processes and procedures within their areas of responsibility. • Describes the basic principles of secure supply chain management. • Follows documented principles and guidelines for secure supply chain management activities.
Supervised Practitioner	• Implements secure supply chain management processes and procedures across DE&S. • Explains and can develop processes for secure supply chain management. • Understands the business context in which policies, procedures and guidelines sit, tailoring processes to suit business needs.
Practitioner	• Identifies and implements new secure supply chain management controls to reflect changes in factors such as threat levels and legislation. • Develops secure supply chain management processes to meet standards or changes to standards. • Responds to challenges to policies, procedures and guidelines and implements continuous improvements.
Expert	• Champions the need for and the business benefits of secure supply chain management controls. • Shapes policies, procedures and guidelines within DE&S and wider MOD. • Implements business change as a result of policies, procedures and guidelines.

Threat Understanding

Threat understanding encompasses evidence-based knowledge, including context, about an existing or emerging threat to assets that can be used to inform decisions.

Level	Descriptor
Awareness	• Describes specific threats and how they may manifest themselves in a local environment. • Maintains understanding of local threat environment and can apply to inform and provide context for wider activities. • Uses local threat information in decision-making and planning. • Demonstrates knowledge of current threats and trends affecting the landscape
Supervised Practitioner	• Interprets sources of threat information for the local environment and applies knowledge of the external environment. • Maintains understanding of local and strategic threat environments, and trends affecting the landscape, and can apply to inform and provide context. • Uses local and strategic threat information in decision-making and planning. • Communicates tailored threat information to relevant local stakeholders within the organisation.
Practitioner	• Proactively identifies, interprets and leverages a range of relevant sources of threat information, using a variety of techniques, to understand the threat environment (local and strategic), including its nature, capability, focuses of interest and other factors associated with relevant threats. • Uses lessons learned to maintain an understanding of the organisation's attack surface and uses local and strategic threat information in decision-making and planning. • Communicates tailored threat information to relevant senior stakeholders across multiple sites and/or business functions. • Combines external threat information, organisational context and situational awareness to provide a holistic threat understanding capability.
Expert	• . Uses a range of techniques and sources to develop, maintain and direct an understanding of the operating threat environment, including its nature, capability, focuses of interest and other factors associated with relevant threat sources/threat actors.

	• Combines external threat information, organisational context and situational awareness to provide a holistic threat understanding capability, including the use of threat models. • Communicates tailored threat information to relevant senior stakeholders at the board level across multiple sites and/or business functions. • Combines external threat information, organisational context and situational awareness to provide a holistic threat understanding capability to teams and organisations. • Implements business change as a result of policies, procedures and guidelines.

Threat intelligence and threat assessment

Threat intelligence and threat assessment encompasses evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging concern or risk that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Principles of the skill include assessing and validating 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 the organisation, including security analytics for big data; processing, collating and exploiting data, taking into account relevance and reliability to develop and maintain 'situational awareness'; predicting and prioritising threats to an organisation and their methods of attack; analysing the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities, predicting and prioritising threats to an organisation and their methods of attack; using human factor analysis in the assessment of threats; using threat intelligence to develop attack trees; and preparing and disseminating intelligence reports, providing threat indicators and warnings.

Level	Descriptor
Awareness	• Understands and utilises basic threat principles and concepts.
Supervised Practitioner	• Understands and can explain threat intelligence and threat assessment principles and concepts. • Uses prescribed tools and techniques to acquire, validate and analyse threat information from multiple sources. • Under direction enriches threat information by providing context, assessing possible implications and summarising the behaviour, capabilities and activities of threat actors. • Uses approved techniques to model routine threats, under supervision, to identify common enterprise attack vector, identify critical organisational functions, and protect organisational assets and goals. • Applies knowledge to prioritise remediation of identified vulnerabilities for a single asset or system.
Practitioner	• Has an advanced understanding of threat intelligence and threat assessment principles and concepts, and leads threat intelligence and assessment activities • Identifies sources of threat information and utilises a variety of techniques, without supervision, to acquire, validate and analyse threat information, enterprise attack vectors, and critical organisational functions from multiple sources. Synthesises and places intelligence in context. • Applies expertise and insight to enrich threat information, including understanding the behaviour, capabilities and activities of threat actors and assessing possible implications, prioritising remediation of identified vulnerabilities for multiple systems. • Disseminates enriched threat intelligence.

	• Applies threat intelligence to model threats and protects organisational assets and goals, including informing the selection of security controls, developing indicators of compromise, detecting illicit behaviour (including evidence of fraud and crime), providing context for undertaking investigations and responding to events. • Directs others in undertaking threat intelligence activities.
Expert	• Demonstrates a highly advanced understanding of threat principles and concepts. Identifies sources of threat information and selections and, where required, develops techniques to acquire, validate and analyse threat information from multiple sources. • Synthesises and places complex intelligence in context, understanding relevance in the context of organisational strategy. • Applies and directs others in application of expertise and insight to enrich threat information, including understanding the behaviour, capabilities and activities of threat actors and assessing possible implications. • Is responsible for disseminating enriched threat intelligence. • Directs and is responsible for the application of threat intelligence to model threats, including sophisticated and complex threats, to protect organisational assets and goals, including informing the selection of security controls, developing indicators of compromise, detecting illicit behaviour (including evidence of fraud and crime), and providing context for undertaking investigations and responding to events • Leads and oversees the threat intelligence function and activities for an organisation. • Is responsible for strategy, policy, procedures, guidelines and selection of relevant tools and techniques within the organisation. • Advises and influences senior management when required, and influences developments in the field at a national level.