24.2. Glossary of Terms

Glossary of Terms

24.2.1.

Term	Meaning
802.11	The Institute of Electrical and Electronics Engineers standard defining WLAN communications. Formally titled IEEE 82.11.
Access Gateway	An architectural construct that provides the system user access to multiple security domains from a single device, typically a workstation.
Access control	The process of granting or denying requests for access to systems, applications and information. It can also refer to the process of granting or denying requests for access to facilities.
Accountable	Required or expected to justify actions or decisions; being answerable and responsible for those actions & decisions.
Accountable Material	Accountable information, an accountable item or accountable material refers to the accountability controls applied to specified information, equipment or materials. Accountable information, items or materials are usually uniquely identifiable (usually a serial or identification number) and are tracked from acquisition or creation to final disposal. Safe custody is a fundamental and is achieved through: • is easily to compute; • will usually output a significantly different value, even for small changes made to the input; and • can detect many types of data corruptions. • allocation to a specific individual (issued or responsibility designated); • allocation or designation of responsibility may also require a specific briefing related to the handling, care and protection of particular types of classified information and COMSEC equipment; • the allocation, issue or designation being recorded; • strict controls over access and movement (special handling requirements); • maintenance of a register (manual or electronic); and • regular audits to ensure accountability conditions continue to be adhered to and any briefings are current. As a general rule, accountable information, items or materials are afforded physical security protection by specifying special handling and accountability conditions. Examples may include cryptographic or COMSEC equipment, other high value equipment, money, computers or information subject to privacy legislation and regulation. Cryptographic or COMSEC equipment and any information classified as CONFIDENTIAL, SECRET or TOP SECRET is accountable by definition.
Accountability	Most contemporary definitions include two key elements: • the conferring of responsibility and authority; and • the answering for the use of that authority. Accountability exists when the performance of tasks or functions by an individual or organisation, are subject to another's oversight, direction or request that they provide information or justification for their actions. Answering for the use of authority means reporting, explaining actions, assuming obligations, and submitting to outside or external judgement. Having responsibility means having the authority to act, the power to control and the freedom to decide. It also means that one must behave rationally, reliably and consistently in exercising judgement.
Accreditation	A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the operation of a system and issues a formal approval to operate the system.
Accreditation Authority	The authoritative body or individual responsible for systems accreditation.
Adaptive Authentication	This varies the level or degree of authentication required where unusual login requests occur. For example, out of normal hours, from an unusual geolocation, from an unknown device and so on. When an unusual authentication request is received, Adaptive Authentication may request additional credentials such as a one-time code provided to a known mobile phone number.
Agency	New Zealand Government departments, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the Public Service Act.
Agency Control	This description applies where an Agency has direct control of agency information systems and data. It follows that Non-Agency Control occurs where direct control is impaired or does not or cannot exist.
Agency Head	The government employee with ultimate responsibility for the secure operation of agency functions, whether performed inhouse or outsourced.
All-of-Government	Refers to the entire New Zealand state sector.
Allow list	A list that confirms items being analysed are acceptable. This is the opposite of a deny or block list.
Approved Cryptographic Algorithms	Approved cryptographic algorithms have been extensively scrutinised for vulnerabilities by government, industry and academic communities in a practical and theoretical setting. The approved cryptographic algorithms fall into three categories: asymmetric/public key algorithms, hashing algorithms, and symmetric encryption algorithms.

Approved Destruction Facility	The status of "approved facility" for the destruction of media and equipment, applies to a specific installation/site, and is granted by the Director-General GCSB under the NZISM. Approval depends upon the Director-General's satisfaction that the proposed facilities are capable of securely destroying IT equipment, devices and media to the standard required under the NZISM and related policies and that procedural security meets the required standards.
Asset	Anything of value to an agency, such as IT equipment and software, information, personnel, documentation, reputation and public confidence.
Attack Surface	The IT equipment and software used in a system. The greater the attack surface the greater the chances are of an attacker finding an exploitable vulnerability.
Attribute Based Access Control	An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.
Audit	A structured process of examination, review, assessment, testing and reporting against defined requirements or objectives. Auditors should be independent of any IT system, business process, agency, function, site, supplier or other subject area being audited.
Australian Information Security Evaluation Program	A program under which evaluations are performed by impartial companies against the Common Criteria. The results of these evaluations are then certified by ASD, which is responsible for the overall operation of the program.
Authentication	The process of identifying an individual, device or system before granting access to system resources or data. Usually based on a set of credentials such as an identifier (such as a user or device name) and an authenticator (such as a password or some other authentication factor). Authentication is distinct from Authorisation.
Authentication Header	Part of the protocol used for authentication within IPSec, it provides authentication, integrity and anti-replay for the entire packet (both the header and data payload).
Authorisation	Authorisation is the process of granting (or revoking) access privileges to an individual, device or system.
Baseline	Information and controls that are used as a minimum implementation or starting point to provide a consistent minimum standard of systems security and information assurance.
Brute Force Attack	A brute force attack is when an automated continuous attack is conducted against a system or file to decrypt or discover passwords and data. Often used as an entry point for privilege escalation.
Bug Bounty	A monetary reward to researchers for the discovery and reporting of software and other information system vulnerabilities.
Cascaded Connections	Links to other systems that occur when connected systems are themselves connected to other systems. This may result in multiple indirect (cascaded) connections to systems with differing security implementations, data, equipment and other aspects important for the security and assurance of systems.
Caveat	A marking that indicates that the information has special requirements in addition to those indicated by the classification and any prescribed endorsement. The term covers codewords, source codewords, releasability indicators and special-handling caveats. See also Endorsements.
Certification	The process by which the controls and management of an information system is formally evaluated against any specific risks identified and the requirements of the NZISM. A key output is a formal assurance statement that the system conforms to the requirements of the NZISM.
Certification Authority	An official with the authority to assert that a system complies with prescribed controls within a standard.
Certification Report	A report generated by a certification body of a Common Criteria scheme that provides a summary of the findings of an evaluation.
Characterisation	In the NZISM "characterisation" is a synonym for "unique identifier". This is typically applied to an operating system, programme, library or other programmatic element in the form of a checksum which can be calculated from a "known good" component and stored for comparison should there be any concern that components have been damaged or compromised. Forensic methods may also provide characterisation indicators but are likely to require additional levels of expertise. See also Checksum and Hash.

Checksum	A checksum verifies or **checks** the integrity of data. A good checksum algorithm: • is easily to compute; • will usually output a significantly different value, even for small changes made to the input; and • can detect many types of data corruptions. Checksums are often used to verify the integrity of operating system, programme, library or other programmatic elements, images and firmware updates. Checksums typically range in length from one to 64-bits, depending on the intended usage and algorithm used to determine the checksum. Checksums are related to hash functions, fingerprints, randomisation functions, and cryptographic hash functions. Note, however, each of those concepts are distinct, have different applications and therefore different design goals. Check digits and parity bits are special uses of checksums. It is important to recognise that, although related, a hash is not a checksum. See also Hash.
Chief Information Security Officer	A senior executive with overall responsibility for the governance and management of information risks within an agency. This may include coordination between security, ICT and business functions to ensure risks are properly identified and managed.
Classified Information	Government information that requires protection from unauthorised disclosure.
Classified Systems	Systems that process, store or communicate classified information.
Cloud deployment model	The term deployment model refers to the type of access and the fundamental nature of the support infrastructure but is not specific as to the type of service consumed. Typically this includes: • private cloud, • public cloud, • hybrid cloud, and • multi-cloud.
Cloud service model	The term cloud service model refers to the type of service used. These cloud service offerings are provided and maintained by the cloud service provider. Typical service offerings include: • Infrastructure-as-a-Service, • Software-as-a-Service, and • Platform-as-a-Service.
Cloud service provider	An external company that provides a platform, infrastructure, applications, and/or storage services for its clients.
Codewords	A short (usually a single word) descriptions of a project, operation or activity, typically assigned used for reasons of reliability, clarity, brevity, or secrecy. Each code word is assembled in accordance with the specific rules of the code and assigned a unique meaning. Synonymous with *Codename*.
Coercivity	A measure of the resistance of a magnetic material to changes in magnetisation, equivalent to the field intensity necessary to demagnetise any magnetised material. The amount of coercive force required to reduce any residual magnetic induction to zero. Normally used in describing the characteristics of degaussing magnetic media (see Degausser).
Common Criteria	A formal, internationally-recognised scheme, defined in the ISO 15408 standard. This standard describes process to specify, design, develop, test, evaluate and certify as secure IT systems, where 'secure' is explicitly and formally defined.
Common Criteria Recognition Arrangement	An international agreement which facilitates the mutual recognition of Common Criteria evaluations by certificate producing schemes, including the Australian and New Zealand certification scheme.
Communications Security	Controls applied taken to deny unauthorised access to information derived from information and communication systems and to ensure the authenticity of related communications and data.
Conduit	A tube, duct or pipe used to protect cables.
Connection Forwarding	The use of network address translation to allow a port on a network node inside a local area network to be accessed from outside the network. Alternatively, using a Secure Shell server to forward a Transmission Control Protocol connection to an arbitrary port on the local host.
ConOp	Concept of Operations, a document describing the characteristics of an information systems and its intended use. It is used to communicate the intent and system characteristics to all stakeholders
Consumer Guide	Product specific advice concerning evaluated products can consist of findings from mutually recognised information security evaluations. This may include the Common Criteria, findings from GCSB internal evaluations, any recommendations for use and references to relevant policy and other standards.
Content Filtering	The process of monitoring communications, including email and web pages, analysing them for any suspicious or unwanted content, and preventing the delivery of suspicious or unwanted content.

Contract	Contract means an agreement between two or more persons or entities, which is intended to be enforceable at law and includes a contract made by deed or in writing,
Cross-Domain Solution	A Cross-Domain Solution (CDS) is a controlled interface that enables secure manual and/or automatic access and/or information transfer between different security domains while protecting the confidentiality, integrity and availability of each domain. There are several types of CDS including access, multi-level and transfer gateways.
Cryptographic Hash	An algorithm (the hash function) which takes as input a string of any length (the message), and generates a fixed length string (the message digest or fingerprint) as output. The algorithm is designed to make it computationally infeasible to find any input which maps to a given digest, or to find two different messages that map to the same digest.
Cryptography	Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
Cryptoperiod	The useful life of the cryptographic key.
Cryptographic Protocol	Specified cryptographic algorithms, parameters (such as key length) and processes for managing, establishing and using encrypted communications.
Cryptographic System	A related set of hardware or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates.
Cryptographic System Material	Material that includes, cryptographic key, equipment, devices, documents, firmware or software that contains or describes cryptographic logic.
Data At Rest	Information residing on media storage facility or a system that is not in use.
Data Diode	A device that allows data to flow in only one direction.
Data In Transit	Information that is being conveyed across a communication medium.
Data In Use	Information that has been decrypted for processing by a system.
Data Remanence	Residual information remaining on a device or storage media after clearing or sanitising the device or media. Sometimes described as data persistence.
Data Spill	An information security incident that occurs when information is transferred between two security domains by an unauthorised means. This can include from a classified network to a less classified network or between two areas with different need-to-know requirements.
Declassification	A process whereby information is reduced to an unclassified state. Subsequently an administrative decision can be made to formally authorise its release into the public domain.
Degausser	An electrical device or permanent magnet assembly which generates a coercive magnetic force to destroy magnetic storage patterns in order to sanitise magnetic media.
Delegate	A person or group of personnel who may authorise noncompliance with requirements in this manual on the specific authority of the agency head.
Demilitarised Zone	A small network with one or more servers that is kept separate from an agency's core network, either on the outside of the agency's firewall, or as a separate network protected by the agency's firewall. Demilitarised zones usually provide public domain information to less trusted networks, such as the Internet.
Deny list	A set of items to be excluded, blocked or prevented from execution. A deny list can also be known as a Block List. It is the opposite of an allow list which confirms that items are acceptable.
Department	Term used to describe Public Service Departments and Non-Public Service Departments within the state sector. Refer State Services Commission list of Central Government Agencies – Central government organisations - Te Kawa Mataaho Public Service Commission
Device Access Control Software	Software that can be installed to restrict access to communications ports such as USB, Serial HDMI and Ethernet Ports. Device access control software can either block all access to a communications port or allow access using an allow listing approach based on device types, manufacturer's identification, or even unique device identifiers.

DevOps	DevOps is a set of practices that combines software development (Dev) and IT operations (Ops). It aims to shorten the systems development life cycle and provide continuous delivery with high software quality.
Diffie-Hellman Groups	A method used for specifying the modulus size used in the hashed message authentication code algorithms. Each DH group represents a specific modulus size. For example, group 2 represents a modulus size of 1024 bits.
Direct Control	In relation to the NZISM, Direct Control is the immediate and continuous physical and logical control, responsibility for, and operation of agency information systems and data. See also Indirect Control.
Domain-based Message Authentication, Reporting, and Conformance	Domain-based Message Authentication, Reporting, and Conformance is a scalable mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting, that a mail-receiving organization can use to improve mail handling.
DomainKeys Identified Mail	DomainKeys Identified Mail defines a mechanism by which email messages can be cryptographically signed, permitting a signing domain to claim responsibility for the introduction of a message into the mail stream. Message recipients can verify the signature by querying the signer's domain directly to retrieve the appropriate public key, and thereby confirm that the message was attested to by a party in possession of the private key for the signing domain.
Dual-Stack Device	A product that implements both IP version 4 and 6 protocol stacks.
Emanation Security	The counter-measures, techniques and processes employed to reduce classified emanations from a facility and its systems to an acceptable level. Emanations can be in the form of RF energy, sound waves or optical signals.
Emergency Access	The process of a system user accessing a system that they do not hold appropriate security clearances for due to an immediate and critical emergency requirement.
Emergency Situation	A situation requiring the evacuation of a site. Examples include fires and bomb threats.
Encapsulating Security Payload	A protocol used for encryption and authentication within IPSec.
Encryption	The transformation of data from plaintext (recognisable/readable data) to ciphertext (encrypted and not readable) using a cryptographic key. Data is encrypted using an encryption key to produce ciphertext and decrypted to plaintext using a decryption key. These keys may be the same (symmetric encryption) or two different keys (asymmetric encryption). Encryption alone does not prevent interference or unauthorised access but denies the intelligible content to unauthorised individuals, organisations or other would-be interceptors.
Endorsement	Certain information may bear an endorsement marking in addition to a security classification. Endorsement markings are not security classifications in their own right and must not appear without a security classification. Endorsement markings are warnings that the information has special requirements in addition to those indicated by the security classification and should only be used when there is a clear need for special care. Endorsement markings may indicate: • the specific nature of information; • temporary sensitivities; • limitations on availability; or • how recipients should handle or disclose information.
Escort	An individual who supervises visitors to secure areas to ensure uncleared visitors are not exposed to classified information, conversations equipment and other classified materials. Such visitors may include maintenance staff, IT contractors and building inspectors.
Evaluation Assurance Level	A numeric representation of the security functionality of a product gained from undertaking a Common Criteria evaluation. Each EAL comprises a number of assurance components, covering aspects of a product's design, development and operation. The range covers EAL0 (lowest) to EAL7 (highest).
Exception	The formal acknowledgement that a requirement of the NZISM cannot be met and that a dispensation from the particular compliance requirement is granted by the Accreditation Authority. This exception is valid for the term of the Accreditation Certificate or some lesser time as determined by the Accreditation Authority.
Exceptions and Waivers	An exception is NOT the same as a waiver. An exception means that the requirement need not be followed. A waiver means that some alternative controls or conditions are implemented.
Facility	An area that facilitates government business. For example, a facility can be a building, a floor of a building or a designated area on the floor of a building.
Filter	A device that manages or restricts the flow of data in accordance with a security policy.

Finder	An individual or organisation that reports a vulnerability under an agency's VDP.
Firewall	A network protection device that filters incoming and outgoing network data, based on a series of rules.
Firmware	Software embedded in a hardware device.
Flash Memory Media	A specific type of EEPROM.
Fly Lead	A cable that connects IT equipment to the fixed infrastructure of the facility. For example, the cable that connects a workstation to a network wall socket.
Foreign National	A person who is not a New Zealand citizen.
Foreign System	A system that is not owned and operated by the New Zealand Government.
Functional Segregation	Segregation based on the device function or intended function.
Gateway	Connections between two or more systems from different security domains to allow access to or transfer of information according to defined security policies. Some gateways can be automated through a combination of physical or software mechanisms. Gateways are typically grouped into three categories: access gateways, multilevel gateways and transfer gateways.
General User	A system user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass system security.
Government Chief Information Officer	Government Chief Information Officer (GCIO) is a role undertaken by the Chief Executive of the Department of Internal Affairs in order to provide leadership on ICT matters within the NZ Government.
Hardware	A generic term for any physical component of information and communication technology, including peripheral equipment and media used to process information.
Hardware Security Module	Hardware Security Modules (HSMs) are a device, card or appliance usually installed inside of a PC or server to provide cryptographic functions. HSM's are usually physically and electronically hardened to reduce the possibility of tampering or other interference.
Hash	A hash is the result of a one-way, cryptographic function that converts a data string of any length into a unique fixed-length bit string. Typically applied to passwords and messages to protect against loss and/or add resistance to attacks. Hashing algorithms or functions are often are designed as a one-way cryptographic transformation so that it's impossible to reverse the hash process and reconstitute the original string. The values returned by a hash function are variously described as hash values, hash codes, digests, or simply hashes. One common use of a hash is a data structure called a hash table, widely used in computer software for indexing and rapid retrieval of database elements. Note that a hash is not the same as data encryption although it does utilise cryptographic functions. See also Checksum.
Hash Value	See Hash. Also known as "message digest".
Hashed Message Authentication Code Algorithms	In cryptography, a keyed-hash message authentication code (HMAC) is a specific type of message authentication code (MAC) using a cryptographic hash function and a cryptographic key.
High Assurance	High Assurance is a generic term encompassing Common Criteria Evaluation Assurance Levels (EAL) 5, 6 and 7. Alternatively refers to the independent (unrelated) ASD High Assurance Evaluation Scheme.
High Assurance Cryptography	The U.S. ranks cryptographic products and algorithms through a certification programme and categorising the products and algorithms into product types. Product types are defined in the US National Information Assurance Glossary (CNSSI No. 4009) which defines Type 1 and 2 products, and Type 3 and 4 algorithms. Type 1 products are used to protect systems requiring the most stringent protection mechanisms.
High Assurance Cryptographic Equipment (HACE)	The equivalent to United States Type 1 cryptographic products & equipment. Previously described as High Grade Cryptographic Products & Equipment, the term HACE includes classified CCI, and other GCSB-Specific devices.
Hybrid Hard Drives	Non-volatile magnetic media that use a cache to increase read and write speeds and reduce boot time. The cache is normally flash memory media or battery backed RAM.
Incident Response Plan	A plan for responding to information security incidents as defined by the individual agency.

Identity and Access Management	Identity and Access Management (IAM) is a framework of business processes, policies and technologies that enable and support the management of electronic or digital identities, authorisation, privileges and access to organisational resources. Identity management deals with attributes related to a user (including people, machines, devices and systems). Access Management applies organisation processes, policies and security to enable and manage access. The two aspects are highly interdependent and are most effectively managed conjointly. An IAM framework is a key element in Privileged Access Management (PAM) and Zero Trust architectures.
Image persistence / Image retention	LCD/LED/OLED and plasma technologies can be susceptible to persistence or retention of an image or "ghost" image on the screen. This can also led to screen burn-in, as can occur in traditional CRT monitors.
Indirect Agency Control	In relation to the NZISM, Indirect agency control is when information, services or operations are not under the direct control of the agency. This may be through outsourcing of, ICT management or services, use of third party facilities such as data centre co-locations, or consumption of cloud services. See also Direct Control.
Information	Any communication or representation of knowledge such as facts, data, and opinions in any medium or form, electronic as well as physical. Information includes any text, numerical, graphic, cartographic, narrative, or any audio or visual representation.
Information Asset	Information asset is any information or related equipment has value to an organisation. This includes equipment, facilities, patents, intellectual property, software and hardware. Information Assets also include services, information, and people, and characteristics such as reputation, brand, image, skills, capability and knowledge
Information and Communications Technology (ICT)	Information and Communications Technology (ICT) includes: • Information management; • Technology infrastructure; and • Technology-enabled business processes and services
Information Security	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or any other means.
Information Security Incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it or by any other process or system and processes.
Information Security Policy	A high-level document that describes how an agency protects its information. The CSP is normally developed to cover all systems and can exist as a single document or as a set of related documents.
Information Technology Security Manager	ITSMs are executives within an agency that act as a conduit between the strategic directions provided by the CISO and the technical efforts of systems administrators. The main responsibility of ITSMs is the administrative controls relating to information security within the agency.
Infrared Device	A device such as a mouse, keyboard, pointing device, laptop and smart phone that have an infrared communications capability.
Infrastructure-as-a-Service	Infrastructure-as-a-Service is where the cloud service provider offers access to a variety of capabilities and technologies on demand. Service is provided either over the public Internet or through dedicated connections.
Internet Key Exchange Extended Authentication	Used to provide an additional level of authentication by allowing IPSec gateways to request additional authentication information from remote users. As a result, users are forced to respond with credentials before being allowed access to the connection.
Intrusion Detection System	An automated system used to identify an infringement of security policy from an internal or external source.
Intrusion Prevention System	A security device, resident on a specific host, which monitors system activities for malicious or unwanted behaviour and can react in real-time to block or prevent those activities.
Inverse split tunnelling	A particular configuration of split tunnelling where only specifically authorised and trusted systems are able to be simultaneously communicated with via the external network connection.
IP Security	A suite of protocols for secure IP communications through authentication or encryption of IP packets including protocols for cryptographic key establishment.
IP Telephony	The management and transport of voice communications over IP networks. Also described as Voice Over IP (VOIP).

IP Version 6	A protocol used for communicating over a packet switched network. Version 6 is the successor to version 4 which is widely used on the Internet. The main change introduced in version 6 is a greater address space available for identifying network devices, workstations and servers.
ISAKMP Aggressive Mode	An IPSec protocol that uses a reduced Exchange to establish an IPSec connection. Connection negotiation is quicker but potentially less secure.
ISAKMP Main Mode	An IPSec protocol that offers improved security using additional negotiation to establish an IPSec connection.
ISAKMP Quick Mode	An IPSec protocol that is used for refreshing security association information. Similar to aggressive mode
Isolation	Includes disconnection from other systems and any external connections. In some cases system isolation may not be possible for architectural or operational reasons. Isolation may also include the quarantine of suspected or known malware and unwanted content.
IT Equipment	Any equipment to support the acquisition, processing and storage of information. This may include servers, routers, switches, switch panels, UPSs, PCs, laptops printers, MFDs etc.
Key Management	The management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.
Key Management Plan	Describes how cryptographic services are securely deployed within an agency. It documents critical key management controls to protect keys and associated material during their life cycle, along with other controls to provide confidentiality, integrity and availability of keys.
Key Stretching	A defence against brute force and similar system attacks by increasing the time required to complete hashing and making an attack more time-consuming.
Limited Higher Access	The process of granting a system user access to a system that they do not hold appropriate security clearances for, for a limited period of time.
Lockable Commercial Cabinet	A cabinet that is commercially available, of robust construction and is fitted with a commercial lock.
Logging Facility	A facility that includes the software component which records system events and associated details, the transmission (if necessary) of these records (logs) and how they are stored and secured.
Malicious Code	Any software that attempts to subvert the confidentiality, integrity or availability of a system. Types of malicious code include logic bombs, trapdoors, Trojans, viruses and worms. More usually as Malware
Malicious Code Infection	An information security incident that occurs when malicious code is used to infect a system. Examples of malicious code infection viruses, worms and Trojans.
Malware	Malicious Software or Malicious Code.
Management Traffic	Communications generated by system administrators and processes over a network in order to manage and control a device.
Mandatory Controls	Controls within this manual with either a 'MUST' or a 'MUST NOT' compliance requirement.
Media	A generic term for any type of hardware or material that is capable of storing or retaining data. The following examples, while not a definitive list, includes any type of "floppy disk", tapes, all types of optical disks, HDD, SSD, USB, RAM, Flash, ROM, EPROM, printer cartridges, printer drums and so on.
Media Destruction	The process of physically damaging the media with the objective of making the data stored on it inaccessible. To destroy media effectively, only the actual material in which the data is stored needs to be destroyed.
Media Disposal	The process of relinquishing control of media, or disposing of when no longer required, in a secure manner that ensures that no data can be recovered from the media
Media Sanitisation	The process of securely erasing or overwriting data stored on media.
Multi-Factor Authentication	Multi-Factor Authentication (MFA) is a security system that verifies a user's identity by requiring multiple credentials, which may be of the same factor or type. Initial authentication normally requires a username and password. MFA requires other—additional—credentials, for example as a code from the user's smartphone, the answer to a security question, a fingerprint, or facial recognition.

Multifunction Devices	The class of devices that combines printing, scanning, copying, faxing or voice messaging functionality within the one piece of equipment. These are often designed to connect to computer and communications networks simultaneously.
Multilevel Gateway	A gateway that enables access, based on authorisation, to data at many classification and releasability levels where each data unit is individually marked according to its domain.
Need-To-Know	The principle of telling a person only the information that they require to fulfil their role.
Network Access Control	Policies and processes used to control access to a network and actions on a network, including authentication checks and authorisation controls.
Network Device	Any device designed to facilitate the communication of information destined for multiple system users. For example: cryptographic devices, firewalls, routers, switches and hubs.
Network Infrastructure	The infrastructure used to carry information between workstations and servers or other network devices. For example: cabling, junction boxes, patch panels, fibre distribution panels and structured wiring enclosures.
Network Protection Device	A category of network device used specifically to protect a network. For example, a firewall, session border controller etc.
NZ Eyes Only	A caveat indicating that the information is not to be passed to or accessed by foreign nationals.
NZ Government Information Security Manual	National security policy that aims to provide a common approach to ensure that the implementation of information security reduces both agency specific, and whole of government, information security risks to an acceptable level.
NZ Government Protective Security Manual	The PSM was superseded by the Protective Security Requirements (PSR) in December 2014.
No-Lone-Zone	An area in which personnel are not permitted to be left alone such that all actions are witnessed by at least one other person.
Non-Agency Control	This description applies where an Agency does NOT have direct control of elements of agency information systems and data. This may occur, for example, where data centre operations are outsourced.
Non-Volatile Media	A type of media which retains its information when power is removed.
Off-Hook Audio Protection	A method of mitigating the possibility of an active, but temporarily unattended handset inadvertently allowing discussions being undertaken in the vicinity of the handset to be heard by the remote party. This could be achieved through the use of a hold feature, mute feature, push-to-talk handset or equivalent. May not be effective on smart phones / cell phones.
Official Information	Any information held by a government department or agency. See the Official Information Act 1982 (as amended).
OpenPGP	An open-source implementation of Pretty Good Privacy (PGP), a widely available cryptographic toolkit.
Oversight	The term is used in this document in the following ways: 1. In the context of governance where the term is used to describe the responsibility and requirement to manage, govern, inspect or direct activities to ensure particular outcomes, e.g. the oversight of supply contracts. 2. In the physical security context to describe the ability to observe activity (surveillance) and/or read materials which should be protected and shared only under strict guidelines. It enables the systematic observation of places and people by visual, audio, electronic, photographic or other means. Typically this is caused by poor placing of computer screens and desks and proximity to windows, doors, corridors or other means of physical access and overview or oversight. Other physical factors may contribute.
Patch Cable	A metallic (usually copper) or fibre optic cable used for routing signals between two components in an enclosed container or rack or between adjacent containers or racks.
Patch Panel	A group of sockets or connectors that allow manual configuration changes, generally by means of connecting cables to the appropriate connector. Cables could be metallic (copper) or fibre optic.
Perfect Forward Security	Additional security for security associations in that if one security association is compromised subsequent security associations will not be compromised.
Peripheral Switch	A device used to share a set of peripherals between a number of computers.

Platform-as-a-Service	Platform-as-a-Service provides application developers access to all necessary hardware, software, and infrastructure to allow applications to be built, run, and managed. The PaaS infrastructure is typically managed by the cloud service provider
Post-quantum cryptography	Post-quantum cryptography (sometimes described as quantum-resistant) refers to cryptographic algorithms that are considered to be secure against a cryptanalytic attack by a quantum computer.
Principles of Separation and Segregation	Systems architecture and design incorporating separation and segregation in order to establish trust zones, define security domains and enforce boundaries.
Privacy Marking	Privacy markings are used to indicate that official information has a special handling requirement or a distribution that is restricted to a particular audience.
Private Network	A private network is a network and infrastructure owned, managed and controlled by a single entity for its exclusive use. This term includes networks used by private organisations, nongovernment organisations, state owned enterprises, or government department, agencies and ministries. If any part of the transmission path utilises **any** element of a public network, such as telecommunications or data services from a service provider that utilise any component of local, regional or national infrastructure, then the network is defined as a public network
Privileged Access Management (PAM)	Privileged Access Management (PAM) – sometimes also described as Privileged Account Management, refers to a set of processes and tools for granting, controlling, monitoring, and auditing privileged access.
Privileged Account	A Privileged Account is a user account with high levels of access to systems, devices and data. Privileged accounts may, for example, be able to install or remove software, upgrade operating systems, or modify system or application configurations. They may also have access to data that is not normally accessible to standard users.
Privileged User	A system user who can alter or circumvent system security protections. This can also apply to system users who could have only limited privileges, such as software developers, who can still bypass security precautions. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.
Protective Marking	A marking that is applied to unclassified or classified information to indicate the security measures and handling requirements that are to be applied to the information to ensure that it is appropriately protected.
Protective Security Requirements	The Protective Security Requirements (PSR) outlines the Government's expectations for managing personnel, physical and information security.
Protective Security Requirements Framework	The Protective Security Requirements Framework (PSRF) is a four-tier hierarchical approach to protective security. Strategic Security Directive (tier one); Core policies, strategic security objectives and the mandatory requirements (tier two); Protocols, standards and good practice requirements (tier three); Agency-specific policies and procedures (tier four).
Public Domain Information	Official information authorised for unlimited public access or circulation, such as agency publications and websites.
Public Key Infrastructure	The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover and revoke public key certificates. SOURCE: CNSSI-4009
Public Network	A public network contains components that are outside the control of the user organisation. These components may include telecommunications or data services from a service provider that utilise any component of local, regional or national infrastructure.
Public Switched Telephone Network	An historic term describing a public network where voice is communicated using analogue communications. Today almost all communication networks are substantially or entirely digital networks.
Push-To-Talk	Handsets that have a button which must be pressed by the user before audio can be communicated, thus improving off-hook audio protection.
Quality Of Service	A process to prioritise network traffic based on availability requirements.
Radio Frequency Device	Devices including mobile phones, wireless enabled personal devices and laptops.
Reaccreditation	A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the continued operation of a system.

Reclassification	A change to the security measures afforded to information based on a reassessment of the potential impact of its unauthorised disclosure. The lowering of the security measures for media containing classified information often requires sanitisation or destruction processes to be undertaken prior to a formal decision to lower the security measures protecting the information.
Remote Access	Access to a system from a location not within the physical control of the system owner.
Removable Media	Storage media that can be easily removed from a system and is designed for removal.
Residual Risk	The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk (Institute of Internal Auditors). Also sometimes referred to as "net risk" or "controlled risk".
Rogue Wireless Access Point	An unauthorised Wireless Access Point operating outside of the control of an agency.
Role-Based Access Control	The Role-Based Access Control model employs pre-defined roles that carry a specific set of privileges associated with them and to which subjects are assigned.
Salt	Salts are a random data string added to the start or the end of a hash to strengthen its resistance to attack. Typically used in the generation of a password hash or checksums.
Seconded Foreign National	A representative of a foreign government on exchange or long-term posting to an agency.
Secure Area	An area that has been certified to physical security requirements as either a Secure Area; a Partially Secure Area; or an Intruder Resistant Area to allow for the processing of classified information. Refer to the PSR for more detail on Physical Security.
Secure Multipurpose Internet Mail Extension	A protocol which allows the encryption and signing of Multipurpose Internet Mail Extension-encoded email messages.
Secure Shell	A network protocol that can be used to securely log into a remote server or workstation, executing commands on a remote system and securely transfer file(s).
Security Association	A collection of connection-specific parameters containing information about a one-way connection within IPSec that is required for each protocol used.
Security Association Lifetimes	The duration for which security association information is valid.
Security Domains	A system or collection of systems operating under a security policy that defines the classification and releasability of the information processed within the domain. It can be defined by a classification, a community of interest or releasability within a certain classification. This term is NOT synonymous with *Trust Zone*.
Security Domain (Cloud)	A security domain in public cloud can be categorised as a group of trust zones operating under a common set of security requirements and policies.
Security Domain Owner	The individual responsible for the secure configuration of the security domain throughout its life-cycle, including all connections to/from the domain.
Security Risk Management Plan	A plan that identifies the risks and appropriate risk treatments including controls needed to meet agency policy.
Security Target	An artefact of Common Criteria evaluations. It contains the information security requirements of an identified target of evaluation and specifies the functional and assurance security measures offered by that target of evaluation to meet the stated requirements.
Segmentation	Segmentation is a logical grouping of the separate components of a network or system for design, control, installation, security and management purposes. This may occur where similarities of function, control and management exist or will be of advantage.
Segregation	Segregation includes the development, enforcement and monitoring of rules in order to control access to systems and information and to manage or restrict the communication between network components, devices, hosts and service. Segregation is essential in all networks but particularly in entirely virtual networks, such as cloud-hosted networks.
Separation	Separation includes partitioning and physically dividing systems and networks into smaller components. Separation should be applied as a design and control principle to networks where agencies have physical control over devices and components, such as in-office Wi-Fi systems, MFD's, desktops, laptops and other system or user devices.

Separation, segmentation and segregation	Separation, segmentation and segregation are architectural, design and management strategies to limit the effect and impact of network intrusions and system attacks and exploits. They will improve the ability to detect, and also improve the speed and effectiveness of any response to such events.
Server	A computer used to run programs that provide services to multiple users. For example, a file server, email server or database server.
Session Border Controller (SBC)	A device (physical or virtual) used in IP networks to control and manage the signalling and media streams of real-time UC and VoIP connections. It includes establishing, controlling, and terminating calls, interactive media communications or other VoIP connections. SBCs enable VoIP traffic to navigate gateways and firewalls and ensure interoperability between different SIP implementations. Careful selection of SBCs will provide such functionality as prevention of toll fraud, resistance to denial of service attacks and resistance to eavesdropping.
Shared Responsibility Model	The responsibility for the selection, implementation, management and maintenance of controls in public cloud services is shared between provider and consumer. Where the responsibilities lie depends on the provider, and the service and deployment models.
Softphone	A software application that allows a workstation to act as a VoIP phone, using either a built-in or an externally connected microphone and speaker.
Software Component	An element of a system, including but not limited to, a database, operating system, network or Web application.
Solid State Drives	Non-volatile media that uses flash memory media to retain its information when power is removed.
Split Tunnelling	The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices, and simultaneously, access uncontrolled networks.
SSH-Agent	A programme storing private keys used for public key authentication thus enabling an automated or script-based Secure Shell session.
Standard Operating Environment	A standardised build of an operating system and associated software that is deployed on multiple devices. An SOE can be applied to servers, workstations, laptops and mobile devices.
Standard Operating Procedures	Procedures for the operation of system and complying with security requirements.
System	A related set of IT equipment and software used for the processing, storage or communication of information and the governance framework in which it operates.
System Classification	The highest classification of information for which the system is approved to store or process.
System for Cross-domain Identity Management	The SCIM protocol is an application-level protocol for provisioning and managing identity data specified through SCIM schemas. A SCIM server provides a set of resources, the allowable contents of which are defined by a set of schema URIs and a resource type. SCIM's schema is not a document-centric one. Instead, SCIM's support of schema is attribute based, where each attribute may have different type, mutability, cardinality, or returnability.
System Owner	The person responsible for the information resource.
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System User	A general user or a privileged user of a system.
Target Of Evaluation	The functions of a product subject to evaluation under the Common Criteria.
Technical Surveillance Counter-Measures	The process of surveying facilitates to detect the presence of technical surveillance devices and to identify technical security weaknesses that could aid in the conduct of a technical penetration of the surveyed facility.
Telephone	A device that converts between sound waves and electronic signals that can be communicated over a distance.
Telephone System	A system designed primarily for the transmission of voice traffic.
TEMPEST	A short name referring to investigations and studies of compromising emanations.

TEMPEST Rated IT Equipment	IT equipment that has been specifically designed to minimise TEMPEST emanations.
The Principle of Least Privilege	The minimisation of access rights and permissions for users, accounts, applications, systems, devices and computing processes to the absolute minimum necessary in order to perform routine, authorised activities and maintain the safe and secure operation of agency or organisational systems.
TOP SECRET Area	Any area certified to operate at TOP SECRET, containing TOP SECRET servers, workstations or associated network infrastructure.
Traffic Flow Filter	A device that has been configured to automatically filter and control the form of network data.
Transfer Gateway	Facilitates the secure transfer of information, in one or multiple directions (i.e. low to high or high to low), between different security domains.
Transport Mode	An IPSec mode that provides a secure connection between two endpoints by encapsulating an IP payload.
Trust Boundary	The interface between two or more Trust Zones.
Trust Zone	A logical construct encompassing an area with a high degree of trust between the data, users, providers and the systems. It may include a number of capabilities such as secure boot, codesigning, trusted execution and Digital Rights Management (DRM). This term is NOT synonymous with *Security Domain*.
Trust Zone (Cloud)	In the public cloud environment, trust zones represent combinations of public cloud services (made up of user, system and data object combinations) that are authorised to interact with each other and are protected by a common set of security capabilities.
Trusted Source	A person or system formally identified as being capable of reliably producing information meeting defined parameters, such as a maximum data classification and reliably reviewing information produced by others to confirm compliance with defined parameters.
Tunnel Mode	An IPSec mode that provides a secure connection between two endpoints by encapsulating an entire IP packet. The entire packet is encrypted and authenticated.
UNCLASSIFIED Information	Information that is assessed as not requiring a classification.
UNCLASSIFIED Systems	Systems that process, store or communicate information produced by the New Zealand Government that does not require a classification.
Unified Communications	The integration of real-time and near real time communication and interaction services in an organisation or agency. Unified Communications (UC) may integrate several communication systems including unified messaging, collaboration, and interaction systems; real-time and near real-time communications; and transactional applications.
Unsecure Area	An area that has not been certified to meet physical security requirements to allow for the processing of classified information.
Virtual Private Network	The tunnelling of a network's traffic through another network, separating the VPN traffic from the underlying network. A VPN can encrypt traffic if necessary.
Virtual Private Network Split Tunnelling	Functionality that allows personnel to access both a public network and a VPN connection at the same time, such as an agency system and the Internet.
Virtualisation	The software simulation of the components of an information system and may include the simulation of hardware, operating systems, applications, infrastructure and storage.
Volatile Media	A type of media, such as RAM, which gradually loses its information when power is removed.
Waiver	The formal acknowledgement that a particular compliance requirement of the NZISM cannot currently be met and that a waiver is granted by the Accreditation Authority on the basis that full compliance with the NZISM is achieved or compensating controls are implemented within a time specified by the Accreditation Authority. Waivers are valid in the short term only and full accreditation cannot be granted until all conditions of the waiver have been met.
Waivers and Exceptions	A waiver means that some alternative controls or conditions are implemented. An exception means that the requirement need not be followed. An exception is NOT the same as a waiver.

Wear Levelling	A technique used in flash memory that is used to prolong the life of the media. Data can be written to and erased from an address on flash memory a finite number of times. The wear levelling algorithm helps to distribute writes evenly across each memory block, thereby decreasing the wear on the media and increasing its lifetime. The algorithm ensures that updated or new data is written to the first available free block with the least number of writes. This creates free blocks that previously contained data.
WEEE	Electrical and electronic equipment contains a complex mix of materials, components and substances, many which can be poisonous, carcinogenic or toxic in particulate or dust form. This is known as Waste from Electrical and electronic equipment (WEEE). Destruction and disposal of WEEE needs to be managed carefully to avoid the potential of serious health risk or environmental hazard.
Wi-Fi Protected Access	Protocols designed to replace WEP. They refer to components of the 802.11i security standard.
Wired Equivalent Privacy	Wired Equivalent Privacy (WEP), a deprecated 802.11 security standard.
Wireless Access Point	Typically also the device which connects the wireless local area network to the wired local area network. Also known as AP
Wireless Communications	The transmission of data over a communications path using electromagnetic waves rather than a wired medium.
Wireless Local Area Network	A network based upon the 802.11 set of standards. Such networks are often referred to as wireless networks.
Workstation	A stand-alone or networked single-user computer.
X11 Forwarding	X11, also known as the X Window System, is a basic method of video display used in a variety of operating systems. X11 forwarding allows the video display from one network node to be shown on another node.
Zero Trust	Zero Trust is a security concept based around the idea that systems and users should not be given access to any information without verification, even when they are connected to internal networks.