MINIMUM CYBER SECURITY STANDARDS

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre

Contents

Introduction

A more directive approach through standards and system insights

The introduction of the Standards allows us to take a more directive stance and drive sector-wide uplift against foundational cyber security practices. This work contributes to our authoritative voice for mandated agencies and responds to feedback asking for us provide clearer advice to support cyber security uplift.

We will continue to build greater visibility of the system through consolidating insights across the Protective Security Requirements (PSR), the Standards, the Vulnerability Insights Programme, and the Cyber Security Framework. We will use the insights, along with other data, to refine, update, and more effectively deploy our products and services for GCISO-mandated agencies.

Minimum Cyber Security Standards and insights uplift

We have developed the Minimum Cyber Security Standards (the Standards) in line with the GCISO mandate. A key consideration when developing the Standards was ensuring alignment with the PSR framework. The PSR framework provides the assurance mechanism for the NCSC to assess agency compliance with the Standards.

The Standards:

a. establish clear expectations about the basics – the Standards map to both the Cyber Security Framework and the NZISM;
b. help agencies to understand, benchmark and improve their practices – the Standards sit against a maturity model;
c. generate system insights through agency reporting. These insights will help build our dashboard of agency performance, which in turn will inform the development and renewal of products and services.

We are consulting on the Standards in collaboration with PSR

We are coordinating closely with PSR and have aligned our consultation and publication timeframes. Consultation on the Standards with GCISO-mandated agencies and industry partners commenced on 16 June 2025 and will continue until 4 July 2025. To support this consultation, the Standards will be published on the NCSC website. We are coordinating across NCSC and GCSB to support communication and engagement activities.

Feedback from the consultation will help us evaluate whether we have set the Standards at the right level. The final Standards are planned for publication in October 2025 with agencies directed to report back on implementation as part of the PSR assurance reporting process in April 2026.

The Standards

Organisations must actively identify, assess, and manage risks across the business as part of their day-to-day operations, including cyber security risks. The 10 Standards are designed to assist organisations in identifying, planning, and responding to security risks within their bespoke environments.

The 10 Standards drafted as part of this release are listed in the table below:

Security Awareness	Risk Management
Assets and their Importance	Secure Software Configuration
Patching	Multi-factor Authentication
Detect Unusual Behaviour	Least Privilege
Data Recovery	Response Planning

How the Standards are structured

Each Standard has been designed to provide sufficient detail to enable agencies to implement them and further enhance the security maturity level for that Standard. Each Standard has been designed to help organisations understand the what, why, and how aspects. The Standards have a maturity model built in, which will assist in standardising how cyber risks can be tracked and measured over time.

Each Standard is comprised of the following elements:

SECTION	DESCRIPTION/EXPLANATION
Standard Statement	A summary statement provides an overview of what the Standard is.
Maturity Level	We have established criteria within a maturity model to provide clarity, including the expected minimum implementation level. The requirements are intended to meet and comply with each respective level of maturity. The levels provide a pathway that can be used by agencies to assess themselves against, with a view to improving maturity over time. Each maturity builds on the requirement from the preceding level.
Focus Area	The areas the Standard is applicable to. Provided as a guide and not an exhaustive list, each agency is best-placed to identify areas of relevance.

SECTION	DESCRIPTION/EXPLANATION
Intent of the Standard	What the Standard is trying to achieve, including the security risks it is addressing.
Suggested Actions	Suggested actions that could be taken to achieve the Standard, aligned to the Measurable Outcomes section.
Key Dependencies	To implement the Standard, there are likely to be requisite measures or technologies in place. A number of dependencies apply to multiple Standards. In general, these dependencies are less technology-specific and relate to business processes.
Measurable Outcomes	To establish whether the Standard is being implemented, the outcomes are one tool an organisation may wish (or already have in place) to measure to help make this determination. The outcomes have been designed to align with the requirements contained in the maturity level.
NZISM Controls	Relevant controls that provide additional detail to assist in implementing the Standard and meeting New Zealand Government compliance requirements.

Capability Maturity Model

To provide greater clarity, the Standards have a maturity model built in. We have developed the standards so that CMM2 is the minimum.

A description of each level is provided below:

CMM 5 Optimising	Security capability adapts to a dynamic, high-risk operating environment. Practices are generally recognised as world-leading and have near real-time measurement and response mechanisms.
CMM 4 Quantitatively controlled	Security capability and performance is measured, monitored, and objectively and quantitively controlled. Security measures are hardened in response to performance alerts. Security is a strategic focus for the organisation.
CMM 3 Standardised	Security capability is standardised, integrated, understood, and followed consistently across the enterprise. Security is well-governed and managed at an enterprise level
CMM 2 Planned & tracked	Security capability is well-formed in designated business units. The security policies, capabilities, controls, and practices are in place and repeatable. They are designed to meet the organisation's core security requirements.
CMM 1 Informal	Security capability may be ad-hoc, unmanaged, or unpredictable. Success may rely on individuals rather than institutional capability.

Each maturity level has a number of specific requirements. This approach was intentionally chosen, rather than an overall or overarching statement, which often tends to be aspirational in nature or open to varying interpretations.

Key to the development of these Standards is the ability to measure progress and maturity through a set of measures. The measures are also intended to help organisations plan for maintaining and improving their cyber resilience, as well as assisting in identifying areas for potential future investment.

Security Awareness

Standard Statement

Security awareness training provided is in-line with the organisation's risk posture and is relevant to staff. All security awareness training is continually developed to reflect changes in business, technology, and the threat landscape.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	Security policies and guidelines are regularly reviewed, updated, and communicated to all staff.
	Security awareness training is conducted at induction and throughout the year through several approaches, including: • Training on any new systems, policies, or threats • Prompts and warnings • Memorandums and emails • Ongoing campaigns aligned with broader industry initiatives
	Staff are given focused security training for the roles they hold within the organisation.
CMM 3 Standardised	Security policies are kept up to date, published, and are accessible to all staff.
	Staff are given security awareness training regularly throughout their employment, often aligned with broader industry initiatives and aligned with the organisation's specific threat landscape.
	Access to systems is secured through successful completion of training by integrated and automated methods.
	Security requirements are embedded throughout organisational business-as-usual activities and included in employees' job descriptions.
CMM 2 Planned & Tracked	Staff are given dedicated security awareness training during onboarding, including: • Approved systems and usage • Password management • Security risks and threats • Locations of security policies and guidelines
	Security awareness updates are reported at the appropriate organisational level.
CMM 1 Informal	Security awareness training is provided on an ad-hoc basis. Security awareness training material is reviewed and updated sporadically.

Focus areas

All organisational staff.

Intent of the Standard

People can be both the biggest asset and biggest liability when it comes to cyber security risks. This Standard seeks to ensure staff have the appropriate context, understanding, and awareness of cyber security to undertake their day-to-day jobs in a safe manner.

Through security awareness, an organisation can foster an environment where security is a primary consideration, in the same way that financial, operational, health and safety, and technical considerations are today.

Organisations will provide the necessary training and guidance to enable safe usage of the approved systems and applications. Any such training needs to be maintained, so that security awareness remains relevant.

Suggested actions

The following list is not meant to be exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Develop both onboarding and ongoing security awareness training for staff at all levels of the organisation.
- Guidance and training for staff on the safe usage of information systems is provided and routinely reviewed to ensure it aligns with the organisation's security posture.
- Ensuring acceptable use or other cyber policies contain clear expectations on allowable vs. prohibited usage.
- Compliance with associated policies is undertaken and the results are reported.
- Develop and deploy role-based training programmes for staff in specialised roles.

Key dependencies

- Threats and risks are identified.
- Acceptable tool inventory, policy, standards, and procedures exist.
- Support and endorsement for security awareness training has been obtained from management.
- Guidelines for staff when seeking guidance on cyber security issues are in place.

Measurable outcomes

- Cyber security awareness training programmes and guidance are included throughout staff employment lifecycles.
- Regular communication occurs, reinforcing expected and prohibited cyber security activities from all staff.
- Staff demonstrate an understanding of expected behaviours.
- Staff demonstrate an understanding of prohibited activities.
- Staff are empowered and encouraged to highlight security risks, issues, suspected compromises, or anomalies.
- Communication channels exist to facilitate communication to and from management and staff.
- Security awareness programmes are in place.
- Online courses, modules, education days, compliance requirements.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
3.3.8.C.03.	ITSMs SHOULD select and coordinate the implementation of controls to support and enforce information security policies.
3.3.8.C.04.	ITSMs SHOULD provide leadership and direction for the integration of information security strategies and architecture with agency business and ICT strategies and architecture.
3.3.10.C.02.	ITSMs SHOULD monitor and report on compliance with information security policies, as well as the enforcement of information security policies within the agency.
3.3.13.C.01.	ITSMs SHOULD provide or arrange for the provision of information security awareness and training for all agency personnel.
3.3.13.C.01.	ITSMs SHOULD provide or arrange for the provision of information security awareness and training for all agency personnel.
3.3.13.C.02.	ITSMs SHOULD develop technical information materials and workshops on information security trends, threats, good practices and control mechanisms as appropriate.

Risk Management

Standard Statement

Organisations have considered and assessed all risks and threats, including those for cyber security, and have in place adequate measures that meet acceptable risk levels.

Organisations use a defined and documented risk-based approach to identify and control any new and evolving risks and threats, and to assist in the identification of potential areas for investment.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	Assessments are automated and dynamically adjusted in conjunction with changes in risk appetite, including external independent assessments.
	Emerging threats and vulnerabilities are mapped for relevance back to an organisation's risk profile.
	Identification and communication of risks occurs organisation wide.
	Risks are regularly reviewed for changes in risk profile and corresponding controls for effectiveness.
CMM 3 Standardised	Assessments are undertaken regularly, results are reported, and areas for improvement are actioned.
	Risks and associated mitigations have clearly identified individual owners.
	Cyber security risks are assessed from all areas of the business as part of the wider risk process.
	Risk tolerance is clearly defined, allowing for prioritisation and focused risk mitigation.
	Identification and communication of risks occurs two-way.
CMM 2 Planned & Tracked	A risk framework is adopted across the business, with cyber security risks bundled with other organisational areas.
	Risks and associated mitigations may have non-specific or departmental owners.
	Awareness of changes to the threat landscape is ad-hoc and inconsistently evaluated.
	Risk tolerance is defined and applied, addressing only critical business functions.
	Identification and communication of risks is top-down.

CMM 1 Informal	Some risk processes exist, but do not conform to a Standard and/or only include traditional business and financial risks.
	Risk owners are unclear and inconsistent.
	Risk tolerance is not clearly defined, resulting in inconsistent prioritisation and criticality of any remedial work.

Focus areas

Business-critical systems.

Intent of the Standard

Organisations must actively identify, assess, and manage risks across the business as part of their day-to-day operations, including cyber security risks. The primary purpose of a defined risk management approach is to allow for a common understanding of risks and threats, their impact, and to take the appropriate measures to reduce impacts, in case they eventuate, to an accepted level.

By implementing this Standard, organisations will be able to ensure identified risks have adequate measures in place to mitigate those risks to pre-agreed levels. In particular:

- Have clearly defined acceptable residual risk levels to help inform mitigation and investment decisions.
- Ensuring risks are identified and managed beyond the traditional business and financial risks.
- Have cyber security risk handled as part of organisation’s risk management, rather than separately.
- Continually tracking mitigated risks and management of any residual risk.
- Organisations can obtain assurance that their current and planned mitigations are adequately designed to meet the changing threat landscape.
- Security assurance activities effectively identify emerging threats and trends that may have an adverse impact.
- Accountability, responsibility, and ownership of risks is clearly assigned.

Implementing these activities will assist organisations to protect data and ensure availability, enabling operational activities to continue unimpeded.

Suggested actions

The following list is not exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Adopt an industry-standard risk management approach for the organisation.
- Develop risk tolerance levels with executive and governance to help inform the organisation's risk mitigation strategies.
- Define accountabilities and ownership within the organisation for risk, including those for cyber security risk.
- Risk remediation is prioritised and undertaken according to a combined likelihood and impact assessment, and the organisation’s defined risk appetite.
- Cyber security risk profiles are regularly reviewed and updated to reflect an organisation’s risk exposure.

- Cyber security policies and procedures are developed and implemented to assist organisations to meet business outcomes.

Key dependencies

- A digital asset inventory exists and is kept up to date.
- Channels for identifying, assessing, and reporting threats and risks exist.
- Organisations have identified their critical information and digital assets.

Measurable outcomes

- An industry-standard risk management approach is used by the organisation.
- Risk assessments are undertaken regularly, the results reported, and areas for improvement are actioned.
- Risk and associated mitigations are prioritised, reflecting the organisation's risk appetite and risk evaluation.
- Risks have clearly defined owners and regular review dates.
- An organisation can demonstrate a coordinated approach to identifying new and emerging threats across the cyber landscape.
- Supply chain risks are identified, assessed, and managed as part of the wider risk management program.
- Cyber security risks are handled as part of the organisation’s broader risk management process. These broadly cover physical security, personnel security, personnel security, and information security.
- Emerging threats and vulnerabilities are mapped for relevance back to an organisation’s cyber risk profile.
- Existence of formalised risk acceptance through certification and accreditation policy and procedures.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
3.2.12.C.03.	The CISO SHOULD work with business teams to facilitate security risk analysis and security risk management processes, including the identification of acceptable levels of risk consistently across the agency.
5.3.6.C.01.	Agencies SHOULD determine agency and system specific security risks that could warrant additional controls to those specified in this manual.
5.3.7.C.01.	Agencies SHOULD incorporate their SRMP into their wider agency risk management plan.
6.1.7.C.01.	Agencies SHOULD undertake and document information security reviews of their systems at least annually.
6.2.6.C.01.	Agencies SHOULD analyse and treat all vulnerabilities and subsequent security risks to their systems identified during a vulnerability assessment.
6.2.4.C.01.	Agencies SHOULD implement a vulnerability analysis strategy by: • monitoring public domain information about new vulnerabilities in operating systems and application software, • considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner, • running manual checks against system configurations to ensure that only allowed services are active and that disallowed services are prevented, • using security checklists for operating systems and common applications, and • examining any significant incidents on the agency's systems.

Assets and their Importance

Standard Statement

Organisations have a framework and process that enables asset identification and importance.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	The organisation has a continuous monitoring regime in place for tracking and recording any changes in assets.
	Risks are identified and managed through formalised processes.
CMM 3 Standardised	The organisation has a comprehensive inventory of assets, including hardware, software, and data (including cloud).
	Business owners are assigned for assets based on criticality, sensitivity, and importance to the organisation.
	Assets are classified based on their criticality, sensitivity, and importance to the organisation.
	The organisation's procurement policies require the security teams' endorsement prior to asset acquisitions being confirmed or completed.
	All assets must have a business owner that conforms with the organisation's policy, to help manage shadow IT.
CMM 2 Planned & Tracked	The organisation has a basic inventory of assets, including hardware, software, and data (including cloud).
	The organisation has an asset management policy in place that includes end-of-life or end-of-support processes.
	An agreed policy on asset classification exists and is applied to critical systems and assets.
	Security requirements are included within the assets and service acquisitioning process.
CMM 1 Informal	The organisation does not have a clear understanding of which assets they have, their importance, or where they are located.
	Assets are classified by individuals, inconsistently marked and based on an educated guess by the user.
	The organisation does not have a clear understanding of what assets they have, their importance, or where they are located.

Focus areas

- Corporate network systems.
- Cloud services (private, semi-public, public), as-a-service delivery, internal-facing systems.
- External-facing/internet-facing systems.

Intent of Standard

Organisations need to protect their assets. There are many asset types including intellectual property and customer data, IT and OT assets (hardware and software), and people and their skills. This Standard focuses on identifying assets in a cyber security context and understanding their importance so that the appropriate controls to achieve security objectives can be applied. This includes third-party managed services that process and protect organisational assets.

Implementing this Standard will help to identify and prioritise assets that provide and support critical functions to an organisation using a risk-based approach. This Standard intends to address:

- **Identification of Assets:** Understanding which assets are critical to the organisation is the first step before identifying and implementing controls to manage the confidentiality, integrity, and availability of these assets. Organisations must also understand which dependencies exist between assets located either on-site or externally.
- **Establishing an asset life cycle management process:** Having a good asset management process will help in the deliberate and active management of an asset throughout its life while accounting for its total cost of ownership. This may include legacy assets and as-a-service (aaS) offerings. An organisation must ensure assets nearing the end of their supportable life are replaced before they are no longer supportable.
- **Risk Management:** Organisations will be able to apply appropriate controls once levels of risk have been identified. Implementing this Standard will require organisations to undertake a risk assessment.

Identifying and understanding assets and their importance in your organisation will enable the application of appropriate security controls, which may include but is not limited to: monitoring, patch management (see Patching Standard), and hardening. It may also identify opportunities for procedural changes in processes for incident management, data recovery, and response planning (See Data Recovery and Response Planning standards).

Suggested actions

The following list is not exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Establishing an asset lifecycle management policy and procedure.
- Identifying and maintaining a current asset inventory - for hardware and software - that has the appropriate minimum configuration items listed, such as:
  - Application name
  - Business owner
  - Licensing model
  - Server/instance names
  - IP address & URL (if web-based)
  - Vital dependencies (i.e. other systems, networks, etc.)

    - Other supporting information such as C&A artefacts and privacy impact assessments.
- Establishing business owners for mission-critical systems, software, and applications, and ensure they fully understand their role and responsibility as an owner.
- Ensuring procurement policies satisfy security requirements prior to asset acquisitions.
- Procurement of assets is not allowed via corporate credit cards or, where this is permitted, ensure asset invoices are reconciled to procurement tools.
- Continuous monitoring is in place to detect, manage, and track the movement and usage of assets, including oversight around the supply chain.
- Identifying key personnel involved in the management of assets and systems to enable the identification of single points of failure.

Key dependencies

- An asset management tool exists, including resourcing to operate the tool.
- A risk management strategy that includes a defined acceptable risk level exists.
- A defined governance process (e.g. business impact analysis) for rating applications or systems as critical.
- Sufficient capacity and capability to risk-assess critical assets for vulnerabilities and weaknesses.
- A procurement process involves asset management.
- Asset identification methodology is in place.
- Asset governance model that accounts for procurement, onboarding, deployment, recovery, and disposition of assets.

Measurable outcomes

- An asset registry is kept current and regularly reviewed against risks.
- Critical assets, and all dependencies to operate these, have been identified and regularly reviewed.
- Organisations have a current asset inventory (e.g. hardware, software, licences, versions numbers).
- Organisations embed asset management processes and procedures into their procurement/sourcing process.
- Organisations have asset life cycle management policies and procedures, ensuring that all assets are always supportable.
- Business owners are assigned for critical software and applications, and they are also responsible for documenting and communicating any changes in the asset to all relevant support units or key stakeholders.
- Demonstrate an understanding of the total cost of ownership (TCO) of assets for future years.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
3.4.10.C.01.	Each system MUST have a system owner who is responsible for the operation and maintenance of the system.
3.4.10.C.02.	System owners SHOULD be a member of the Senior Executive Team or an equivalent management position, for large or critical agency systems.
5.1.9.C.01.	Agencies MUST ensure that every system is covered by a Security Risk Management Plan, which includes identification of risk owners.
5.3.8.C.01.	Agencies SHOULD incorporate their SRMP into their wider agency risk management plan.
8.4.8.C.01.	Agencies MUST account for all IT equipment containing media
12.1.30.C.03.	Agencies SHOULD select products in the following order of preference: • a protection profile (PP) evaluated product, • products having completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement (CCRA), • products in evaluation in the AISEP, • products in evaluation in a scheme where the outcome will be recognised by the GCSB when the evaluation is complete, or • If products do not fall within any of these categories, normal selection criteria (such as functionality and security) will apply.
12.7.14.C.03.	Agencies SHOULD follow the Government Rules of Procurement.
13.1.9.C.01.	When the Information System reaches the end of its service life in an organisation, policy and procedures SHOULD be in place to ensure secure decommissioning and transfer or disposal, in order to satisfy corporate, legal and statutory requirements.
13.1.13.C.01.	The Agency's Accreditation Authority SHOULD confirm IA compliance on decommissioning and disposal
13.1.13.C.03.	The Agency's Accreditation Authority SHOULD confirm asset register updates.

22.2.15.C.07. Agencies SHOULD implement security and operational management and monitoring tools which include the following minimum capabilities:

- Identify VMs when initiated,
- Validate integrity of files prior to installation,
- Scan new VMs for vulnerabilities and misconfigurations,
- Load only minimum operating system components and services,
- Set resource usage limits,
- Establish connections to peripherals only as required,
- Ensure host and guest time synchronisation,
- Detect snapshot rollbacks and scans after restores,
- Track asset migration, and
- Monitor the security posture of migrated assets.

Secure Configuration of Software

Standard Statement

Organisations shall adopt a secure by design approach when implementing new software within their environments.

Organisations shall consider industry best-practice and vendor guidance on secure configuration of software and not rely on software defaults.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	Configurations are locked and proactively and continuously monitored for deviations from approved templates.
	Changes or updates to baseline configuration triggers alerts across all applicable systems.
CMM 3 Standardised	Baseline configuration guides are regularly updated and reviewed to include any new options, features, or capabilities enabled through updates.
	Regular configuration audits across critical systems and platforms are undertaken and reported on.
	Legacy platforms are reviewed against baseline configuration.
CMM 2 Planned & Tracked	Baseline configuration guides are developed, incorporating vendor and best-practice publications.
	Updates to software are reviewed for configuration changes prior to deployment.
	All new systems adhere to the baseline configuration.
CMM 1 Informal	Baseline configuration guides do not exist, and best-practice adherence is ad-hoc.
	Systems are likely to be inconsistently configured, with the risk of insecure defaults being enabled.

Focus areas

- Corporate network
- Cloud services
- Operating systems and deployed software
- Internal-facing systems
- External/internet-facing systems
- System and software developers and application support teams
- Third-party vendors who provide and are responsible for software.

Intent of the Standard

Default configurations on software and applications can leave organisations insecure and vulnerable to exploitation by malicious actors. This Standard aims to focus efforts on the reviewing and updating of configurations on new and existing software, and to adopt secure implementation practices.

Implementation of this Standard will reduce security vulnerabilities in an organisation's environment and introduce processes for the secure implementation of software. Some of the concerns this Standard aims to address include:

- Use of default credentials (admin) on software and applications.
- Use of default, insecure configuration settings.
- Use of insecure services and protocols.
- Lack of awareness of enabled services and interfaces.
- Lack of awareness in the changes in environment post-software changes/updates.

The guidance provided within this Standard proposes that organisations commit to adopting best practices and application-hardening recommendations during implementation, as well as conducting regular audits to confirm compliance. The degree of hardening will vary depending on the risk appetite acceptable to an organisation. This includes but is not limited to:

- Referring to vendor guidelines for software/application hardening.
- Following organisational processes and procedures for change management.
- Adhering to best practices for securing and updating software/applications.
- Undertaking periodic audits of compliance to the approved configuration.

Undertaking periodic updates of the configuration guidelines.

Organisations with a software development function should adopt a Secure Software Development Life Cycle approach to integrating security practices and considerations at every phase of the software development life cycle (SDLC). This enables organisations to identify security issues early in the software development phase and address them.

Suggested actions

The following list is not exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Allocating business owners for mission-critical systems, software, and applications.
- Developing a baseline requirement for secure software or application configuration from vendor recommendations and best practice. For example, disabling unnecessary services, insecure ports, and

protocols. Enabling encryption for data at rest and in transit.
- Implementing a process to include a technical review of any security changes for software and applications.
- Implementing a process to audit configurations regularly, ensuring adherence to the agreed baseline.
- Implementing a process to regularly update the baselines to capture any configuration option changes through the life of the software or platform.
- Including vendor contract clauses noting the requirements for maintaining secure development practices for services provided.

Key dependencies

- Change management process exists.
- Sufficient resourcing and capacity available to assess technical risks.
- A risk management strategy and defined acceptable risk level.
- Asset inventory that is regularly updated.
- Patch evaluation or testing process is in place.
- Patch compliance monitoring is undertaken.
- Understanding corporate data and corresponding information flows.

Measurable outcomes

- Organisations have identified mission-critical systems and applications.
- Organisations embed security requirements, including secure by design/secure by default development practices, into their procurement or sourcing process.
- Organisations have change management processes to review, test, and approve patches prior to being deployed into production.
- Organisations have a test environment to test new software and updates.
- Organisations have contractual commitments from vendors ensuring secure development practices including secure by default/secure by design are undertaken.
- Organisations adopt a secure by design policy and establish a baseline requirement for secure configuration.
- An ongoing programme of configuration review against approved configuration templates.
- An ongoing programme that reviews configuration templates to address changes over time of the configuration options available.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
3.3.6.C.03.	ITSMs SHOULD consult with ICT project personnel to ensure that information security is included in the evaluation, selection, installation, configuration and operation of IT equipment and software.
3.3.6.C.05.	ITSMs SHOULD be included in the agency's change management and change control processes to ensure that risks are properly identified, and controls are properly applied to manage those risks.
5.4.5.C.02.	Agencies SHOULD use the latest baseline of this manual when developing, and updating, their SSPs as part of the certification, accreditation and reaccreditation of their systems.
6.1.9.C.01.	Agencies SHOULD review the components detailed in the table below. Agencies SHOULD also ensure that any adjustments and changes as a result of any vulnerability analysis are consistent with the vulnerability disclosure policy.
14.1.9.C.01.	Agencies MUST ensure that for all servers and workstations: • a technical specification is agreed for each platform with specified controls. • a standard configuration created and updated for each operating system type and version. • system users do not have the ability to install or disable software without approval, and • installed software and operating system patching is up to date.
14.2.7.C.02.	Agencies SHOULD ensure that application allow listing is used in addition to a strong access control list model and the use of limited privilege accounts.

Patching

Standard Statement

Organisations have processes to identify, implement, and oversee security patches for their systems and applications, including levels around patch compliance.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	A formal patching policy and process exists that includes requirements around patch prioritisation in the context of the organisation.
	Adequate separation of duties is embedded throughout the patching process.
	Systems are retired, upgraded, or replaced at least 12 months before their end of support date or in accordance with the organisation's asset management policy.
	Audit of patches are undertaken that reconciles OS changes through to change requests.
CMM 3 Standardised	Criteria to prioritise patches is clearly defined and applied in line with the organisation's risk management processes.
	A method to proactively identify applicable patch releases is in place.
	A formal process to approve patches, including rollback procedures, exists in line with the organisation's change and risk management processes.
	Systems are retired, upgraded, or replaced at least 6 months before their end of support date or in accordance with the organisation's asset management policy.
	Criteria to prioritise patches is clearly defined and applied in line with the organisation's risk management processes.
CMM 2 Planned & Tracked	Patch severity prioritisation criteria are in place.
	An approval process is in place to source and review patches.
	Rollback procedures are in place if a patch deployment is unsuccessful.
	System replacement or upgrading for business-critical systems occurs at the end of support dates, occurs on an ad-hoc basis, or relies on extended support offerings to keep systems running.

CMM 1 Informal	Patching is undertaken on a reactive and ad-hoc basis and is only managed for vulnerabilities that are rated as severe or critical severity.
	Awareness of vulnerabilities is driven through the media and/or releases from relevant organisations, and word of mouth.
	System replacement or upgrading at end of support dates occurs only after the date has passed.

Focus areas

- External-facing/internet-facing systems.
- Cloud services.
- System and software support.
- Vulnerability scanning and identification.
- Third-party vendors who are responsible for an organisation's patching.
- Any other system required to conduct core business.
- Any other system required to connect with any other organisations (foreign or domestic) and/or the New Zealand public.

Intent of the Standard

Organisations must strive to protect information assets from attacks that may result in information being stolen or compromised. The primary purpose of patching to is to remediate security vulnerabilities in operating systems, applications, and other digitally connected environments.

By implementing this Standard, organisations will be able to better understand their attack surface and manage and prioritise their patching requirements to reduce the likelihood of vulnerabilities being exploited either internally or externally to the organisation. In particular:

- Reducing the opportunity for known vulnerabilities to be exploited and gain a foothold in your system.
- Reducing the opportunity for launching from that foothold to move laterally around your computer systems and compromise them.
- Maintaining an accurate inventory of all systems and applications, so you can swiftly deploy any patches or alternative mitigations that may be required.
- Reducing the likelihood of legacy vulnerabilities being the cause of compromises.

Addressing these key risks will assist organisations to protect data and ensure availability, enabling operational activities to continue unimpeded.

The guidance provided in this Standard is intended to allow organisations to embed patching as part of their IT and business service delivery processes. This includes mechanisms to monitor sources for vulnerabilities, a process to oversee patching (including adequate separation of duties between individuals throughout the distribution process), and to regularly report on compliance levels so they meet acceptable risk standards defined by the organisation.

Suggested actions

The following list is not exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Development of a patch management policy including responsibilities, patch severity thresholds, and alternate mitigation processes in the event a vulnerability goes unpatched.
- Development and maintenance of a current asset inventory.
- Patch detection mechanisms are in place to regularly identify relevant patches.
- Application of all critical-rated security patches within two days (whether working days or not) of the release of the patch, or update on external-facing systems or where working exploits exist, and within two weeks on internal systems.
- Patch versions are registered and linked to the asset registry to provide oversight.
- Patches and upgrades come from reliable sources only.
- Planning for funding of upgrades and retirement of systems and software that no longer has vendor support for patching, well prior to the end of support date.

Key dependencies

- A risk management strategy and defined acceptable risk level exists.
- An asset inventory exists and is kept up to date.
- Capability exists that enable identification of relevant patches.
- Patch evaluation or testing process exists.
- Rollback capacity/capabilities (if required).
- Regime to monitor patch compliance monitoring exists.
- Contract SLAs include requirements around patching requirements.

Measurable outcomes

- Organisations have a current asset inventory (e.g. hardware/software, licences, versions numbers).
- Existence of and investment in patch management software, services, or other tools.
- Employees have mandated responsibility for patching as part of their job duties.
- Organisations have a patch management policy, including requirements around patch severity, risk levels, and patching timeliness.
- Organisations have a test environment or select pilot users to trial patches on.
- Organisations show an ongoing programme of work where end-of-support systems are identified, tracked, upgraded, retired, or replaced well before the operational and security lifecycle ends (and extended support offerings are only used while the replacement of these systems is taking place).
- Change-control process is in place to review, test, and approve patches being installed into production.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
12.4.3.C.01.	Agencies SHOULD monitor relevant sources for information about new vulnerabilities and security patches for software and IT equipment used by the agency.
12.4.4.C.02.	Agencies MUST implement a patch management strategy, including an evaluation or testing process.
12.4.4.C.01.	Agencies SHOULD apply all critical security patches as soon as possible and preferably within two (2) days of the release of the patch or update.
12.4.4.C.05.	Agencies SHOULD apply all non-critical security patches as soon as possible.
12.4.4.C.06.	Agencies SHOULD ensure that security patches are applied through a vendor recommended patch or upgrade process.
13.1.9.C.01.	When the Information System reaches the end of its service life in an organisation, policy and procedures SHOULD be in place to ensure secure decommissioning and transfer or disposal, in order to satisfy corporate, legal and statutory requirements.

Multi-factor Authentication

Standard Statement

Multi-factor Authentication (MFA) is adopted by organisations to assist in protecting business-critical and external-facing systems from unauthorised access, misuse, or compromise.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	MFA is required for all entities and applied across all systems.
	All successful and unsuccessful MFA authentication logs are retained and reviewed.
CMM 3 Standardised	MFA is used when users authenticate to externally facing systems, business-critical systems, and for core network access.
	MFA is required to be used by privileged users and cannot be bypassed unless within a managed 'break glass' scenario.
CMM 2 Planned & Tracked	MFA is used when users authenticate to business-critical systems, both internally and externally facing.
	MFA is used by an organisation when authenticating to third-party services.
	Privileged users are required to have MFA, and all unsuccessful MFA authentication logs are retained and reviewed.
CMM 1 Informal	MFA is available on some systems and users are required to enable any MFA themselves.
	No oversight or auditing exists for use of MFA.

Focus areas

- External-facing/internet-facing systems
- Cloud services
- Remote access
- Standard user accounts
- Privileged user accounts
- Core network access

Intent of the Standard

Organisations have a duty of care to ensure their critical and sensitive information is adequately protected and that requests to access, modify, transmit, or delete information are to authorised personnel only.

It is important that organisations have put in place appropriate multi-layered

preventive and protective measures, beyond conventional username and password authentication requirements. This will further bolster resilience levels, should the first level of authentication be compromised.

Authentication factors can be broadly defined as having the following attributes and characteristics:

- Knowledge factor
- Possession factor
- Inherence factor

MFA verifies a user's identity using multiple credentials, which may be of the same factor or type.

Suggested actions

The following list is not exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Organisations undertake an asset classification exercise to identify their business-critical and sensitive systems.
- Organisations decide on an MFA delivery option, including costings.
- Where possible, include MFA within the Identity Provider (IdP) platform using Single Sign-On (SSO).
- Training, documentation, support, and user acceptance procedures are developed and delivered.

Key dependencies

- An up-to-date understanding of critical business and internet-facing systems and roles.
- Availability of hardware (e.g. organisation issued key fobs, YubiKey).
- Availability of authenticators (e.g. tokens, smart cards).
- Software (e.g. Google or Microsoft Authenticator).
- Biometrics (e.g. thumbprint, facial recognition).
- Monitoring, logging, and alerting functionality/capability exists.
- User acceptance of user agreements is in place.
- Development and ongoing delivery of user awareness/training material has been created.

Measurable outcomes

- MFA is implemented for business-critical and internet-facing systems, and for privileged accounts.
- Funding for MFA monitoring, alerting, and operational management is included in budgets.
- Monitoring/logging to track operational performance, or for security-related events, is in place.
- Inventory or asset listing of MFA hardware.
- Evidence of security testing and/or other forms of assurance that the MFA system is secure.
- A lifecycle management process for MFA tokens, including resetting of privileged user tokens, has been developed.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
16.4.37.C.02.	Agencies MUST use two-factor or Multi-Factor Authentication to allow access to privileged accounts.
16.7.41.C.01.	Agencies MUST undertake a risk analysis before designing and implementing MFA.
16.7.42.C.01.	Where an agency has external facing systems, cloud-based services, or is authenticating to third-party services, they MUST: • require MFA for all user accounts, and • implement a secure, multi-factor process to allow entities to reset their standard user credentials.
16.7.42.C.02.	Where an agency has implemented MFA they MUST: • require MFA for administrative or other high privileged users, and • implement a secure, multi-factor process to allow entities to reset their standard user credentials.
16.7.42.C.03.	Agencies MUST implement MFA on all user accounts with remote access to organisational resources.
16.7.42.C.04.	Agencies SHOULD implement MFA on all user accounts with access to organisational resources.
16.7.42.C.07.	The design of an agency's MFA SHOULD include consideration of: • Risk identification. • Level of security and access control appropriate for each aspect of an organisation's information systems (data, devices, equipment, storage, cloud, etc.) • A formal authorisation process for user system access and entitlements. • Logging, monitoring and reporting of activity, • Review of logs for orphaned accounts and inappropriate user access including unsuccessful authentication, • Identification of error and anomalies which may indicate inappropriate or malicious activity, • Incident response, • Remediation of errors, • Suspension and/or revocation of access rights where policy violations occur, • Capacity planning.

16.7.43.C.01.	The design of an organisations MFA system SHOULD be integrated with the agency's Information Security Policy, the agency's Privileged Access Management (PAM) Policy, and any additional agency password policies.
16.7.44.C.01.	When agencies' implement MFA they MUST ensure users have an understanding of the risks and include appropriate usage and safeguards for MFA in the organisation's user training and awareness programmes.

Detect Unusual Behaviour

Standard Statement

Organisations have implemented a process to detect abnormal activity within their environments, including actions to enable timely and effective mitigations.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	Implement advanced baselining and detection techniques, including artificial intelligence/machine learning (AI/ML) analysis of all logs.
	Auto-mitigations are implemented on systems.
	Network and infrastructure monitoring is elevated to include per-application identification and trend reporting to identify unusual traffic.
	Use of the network, systems, and tools are tied to a user's identity.
CMM 3 Standardised	All environments including cloud are centrally monitored, correlated, and analysed for indicators of unusual behaviour and compromise.
	Monitoring and alerting of infrastructure utilisation, including user activity, server, compute, and network is maintained to identify exceptions in behaviour.
	Ongoing updating of baseline activity is undertaken to aid in the identification of exceptions.
	Ongoing tuning of indicators is undertaken to reduce the level of false positives.
	Introduce automatic mitigation of known bad scenarios, e.g. 'impossible travel'.
	Sufficient resources and capabilities exist to act on alerts as they arise.
CMM 2 Planned & Tracked	Logs for critical systems are stored centrally and analysed.
	Use of—and changes to—privileged accounts or protected system files are alerted.
	A series of indicators is developed and manually applied to the logs for review, including repeated authentication failures and login attempts from unexpected or impossible locations.
CMM 1 Informal	Logs are typically not centrally managed and/or contained within individual applications only.
	Logs that are centrally managed are done so on an ad-hoc/best effort basis.
	Logs are available to be reviewed but are not proactively monitored.

Focus areas

- Corporate network
- Cloud services
- Software as a service
- Bring-your-own-device access
- Internal systems
- Externally facing systems

Intent of the Standard

To minimise the time to detect breaches and compromises, organisations need to be able to proactively monitor for any anomalous or unintended changes or activity within their environment. Early detection will assist in limiting the impact of any breach or compromise and enables organisations to activate steps that facilitate their containment and incident response processes.

For this to be successful, an understanding of the baseline operating environment and behaviour will aid in the early detection and identification of unusual or unexpected behaviour. Establishing and maintaining a baseline of an operating environment, which, in conjunction with regular reviews, will effectively reduce false-positive detection rates.

The area of anomalous behaviour detection is broad, and this Standard seeks to provide guidance on initial deployments. This Standard addresses the areas of successful and unsuccessful user authentication, privilege escalation, and infrastructure utilisation.

Suggested actions

The following list is not exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Development of a baseline of utilisation for infrastructure.
- Monitoring failed login attempts, privileged operations, failed attempts to elevate privileges.
- Defining a tiered response plan (based on incident categorisation) to activate if unusual behaviour has been identified.
- Where possible, automatic responses such as lockout on pre-determined repeated authentication failures are implemented.
- Allocating of resources to oversee and administer monitoring, detection and reporting.

Key dependencies

- Centralised logging with adequate log retention function.
- Monitoring of infrastructure utilisation including compute and network occurs.
- Assets have been identified and their criticality evaluated.
- Threat intelligence capability to provide indictors of compromise exists.

Measurable outcomes

- An ongoing trend/baseline of utilisation of infrastructure, including network telemetry, is maintained and reviewed against.
- Maintaining a predefined tiered response plan to identified unusual behaviour exists and is regularly tested and updated when required.
- Centralised immutable logging capability exists.
- Proactive monitoring and response to unusual behaviour such as:
  - Security-related system alerts and failures

- Modifications to permissions, or protected systems files
- Repeated login failures
- Authentication from unexpected or ‘impossible travel’ countries
- Activities outside of regular business hours
- Unexpected or unusual network and compute utilisation.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
6.2.5.C.01.	Agencies SHOULD conduct vulnerability assessments in order to establish a baseline. This SHOULD be done: • before a system is first used, • after any significant incident, • after a significant change to the system, • after changes to standards, policies and guidelines, • when specified by an ITSM or system owner.
16.6.10.C.01.	Agencies SHOULD log the events listed in the table below for specific software components. (Please see NZISM Chapter 16 for complete table)
16.6.10.C.02.	Agencies SHOULD log, at minimum, the following events for all software components: • Any login activity or attempts, all privileged operations, • failed attempts to elevate privileges, • security related system alerts and failures, • all software updates and/or patching, • system user and group additions, deletions and modification to permissions, and • unauthorised or failed access attempts to systems and files identified as critical to the organisation
23.5.12.C.01.	Agencies MUST ensure that cloud service provider logs are incorporated into overall enterprise logging and alerting systems or procedures in a timely manner to detect information security incidents.
23.5.12.C.02.	Agencies SHOULD ensure that tools and procedures used to detect potential information security incidents account for the public cloud services being consumed by the agency.

Least Privilege

Standard Statement

Organisational requirements incorporate the principle of least privilege when designing and authorising access to their systems.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	Formal oversight is in place and assurance is obtained that third parties also implement least privileged access for its users and administrators on their platforms.
	Temporary accounts for administrative access is the preferred option.
CMM 3 Standardised	A formal process to grant, review, and remove access is in place and regularly monitored for compliance. Instances of non-compliance are resolved within agreed timeframes.
	Temporary access is actively encouraged and supported across the organisation.
	Logging and monitoring for privileged user roles is independently reviewed and stored centrally.
	A central register of all accounts is maintained.
	Local admin rights on workstations are by exception only.
	Just-in-time (JIT) access is actively encouraged and required where user separation cannot be achieved.
CMM 2 Planned & Tracked	Systems and applications where least privileges are to be applied are identified.
	A formal process to grant, review, and remove user access is in place and largely complied with.
	Logging and monitoring for privileged user roles is in place and regularly reviewed.
	Separate accounts are used for standard user and privileged user activity where possible.
	Local admin rights on workstations are limited where possible.

CMM 1 Informal	Default user role settings are applied.
	User account management is initiated manually via changes.
	User roles are categorised by function, if at all.
	Ad-hoc and irregular reviews of user permissions may be undertaken.
	Ad-hoc and irregular logging and monitoring of privileged users is implemented.

Focus areas

- User accounts
- Privileged accounts
- Shared accounts
- Service accounts
- Legacy systems
- Cloud services
- Critical business systems
- Third party/vendor systems (such as SaaS environments)
- User access policy and procedures

Intent of the Standard

The principle of least privilege can be defined as an approach requiring users, applications, or processes to only have access to the minimum number of network and system permissions required to perform pre-approved functions.

Organisations that have legacy systems will especially find this Standard helpful. A number of legacy systems require access to a broad range of IP address, port ranges, and protocols to use modern applications. This provides the opportunity for vulnerabilities to be exploited.

The privileges a user requires to perform their role changes over their time with an organisation, and often privileges are given but never revoked. This unintentional over-provisioning increases the impact of any compromise of an account.

This Standard is intended to reduce the impact of attacks using existing access (through insider threat or account compromise) that could otherwise cause major impacts to an organisation.

Implementing this Standard will help organisations mitigate against the following risks:

- Damage caused by a malicious actor (including insider threat) is contained to areas that they have permission in. For example, the spread of malware is limited to pre-approved locations.
- Attack surface areas are minimised.
- Risk of human error (e.g. reconfiguration) is largely mitigated by reducing the opportunities for lateral movement.

Suggested actions

The following list is not exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Separate user credentials are allocated for standard user and privileged user accounts.
- A formal process of review and approval for granting privileged user access.
- Systems or applications where least privilege is to be applied are identified and approved.
- Roles and user groups defined with permissions relevant to that role.
- Accounts are allocated into roles and user groups.
- Time and location-based restrictions are applied as appropriate for the role or system.
- System-hardening processes include changing all default passwords and disabling default accounts and services not being used.
- Regular audits are undertaken for usage, privileged users, and change to an account's password and permissions.
- Just-in-time (JIT) access control is implemented.
- Role-based access control (RBAC) is used to best reflect an individual user's privileges.
- Logging for privileged user access is monitored and stored in a central location.
- Ensure third parties are aware of and comply with an organisation's requirements around least privilege.

Key dependencies

- User permissions for roles have been defined.
- All systems have been identified.
- Privileged user lists are accurate and current to enable account permission settings and align individual users to accounts.
- Logging functionality is available.
- Management support and expectations around user access.
- Policies lay out the expectations of what the default access level should be

Measurable outcomes

- Privileged user roles are defined based on the organisation's role settings.
- A management or directive exists that lays out expectations around least privilege as a default.
- An account register is maintained.
- Evidence of privileged user audits.
- All accounts have permissions relevant to their roles.
- Regular review of assigned users and account privileges.
- Least privilege user permissions for roles are documented and reviewed on a regular basis.
- Evidence of review and monitoring of privileged user activity.
- Just-in-time (JIT) access is used to temporarily grant and revoke access.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
16.4.37.C.01.	Agencies MUST apply the Principle of Least Privilege when developing and implementing a Privileged Access Management (PAM) policy.
16.4.38.C.01.	As part of a Privileged Access Management (PAM) policy, agencies MUST establish and implement a strong approval and authorisation process before any privileged access credentials are issued.
16.4.38.C.02.	Privileged Access credentials MUST NOT be issued until approval has been formally granted.
16.4.41.C.02.	Privileged account monitoring systems MUST monitor and record: • individual user activity, including exceptions such as out of hours access • activity from unauthorised sources • any unusual use patterns, and • any creation of unauthorised privileged access
16.4.41.C.03.	Agencies MUST protect and limit access to activity and audit logs and records.
23.4.10.C.01.	Agencies MUST apply the principle of least privilege and configure service endpoints to restrict access to authorised parties.

Data Recovery

Standard Statement

Data recovery capabilities are adopted by organisations to assist in protecting business-critical and external-facing systems from risks surrounding data loss.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	Organisations have identified and regularly review and update their data recovery requirements.
	Data recovery testing or auditing is undertaken on a regular basis and the results are communicated to management or applicable data owners, and any necessary remediations are undertaken accordingly.
	Investment and/or funding to support data backup and recovery solutions is incorporated into business-as-usual.
	Roles and responsibilities for carrying out recovery activities are mapped to individual roles and tested during Disaster Recovery Plan/Business Continuity Plan (DRP/BCP) testing.
CMM 3 Standardised	Organisations have identified their data recovery requirements.
	Data recovery testing and auditing is undertaken on a regular basis and the results are communicated to management or applicable data owners.
	Backups are taken of all systems, in line with the data recovery requirements.
	Roles and responsibilities for carrying out recovery activities are mapped to individual roles.
CMM 2 Planned & Tracked	Organisations have identified their data recovery requirements for critical systems.
	Organisations have in place relevant documentation to support data recovery.
	Data recovery testing is undertaken on an ad-hoc basis.
	Roles and responsibilities for carrying out recovery activities are defined but may be team-based.
	Backups of critical systems are taken.

CMM 1 Informal	No data recovery or backup requirements or procedures are in place.
	Reliance is placed solely on high availability and does not include disaster recovery.
	Backups are taken based on individual discretion and on an ad-hoc basis.
	Backups and data recovery testing is not generally undertaken.

Focus areas

- External-facing/internet-facing systems
- Cloud services
- Remote access
- Critical business systems
- Business continuity/disaster recovery
- Third party/vendor systems (such as SaaS environments)

Intent of the Standard

Data recovery relates to the process of retrieving deleted, inaccessible, lost, corrupted, or damaged digital information.

In the context of data-loss implications, data recovery is an essential tool in risk mitigation and in maintaining business continuity. With more people working from home, the risks increase as many employees use their own devices or work on shared computers. Data recovery protects an organisation by maintaining uptime and minimising impacts on productivity.

Data recovery in the context of this Standard refers to:

- Logical data recovery: addresses issues like file corruption, formatting, and accidental deletion.
- Physical data recovery: involves repairing hardware issues like damaged drives or broken components.
- Remote data recovery: the process of recovering data from a location and device remotely.

Suggested actions

The following list is not exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Organisations undertake an asset classification exercise to identify their business-critical and sensitive systems. This could be incorporated into a business impact analysis assessment.
- Data retention requirements are identified and agreed on.
- Recovery point and recovery time objectives are defined.
- Organisations assess and choose data recovery methods appropriate for their situation.
- A data recovery policy is developed.
- Staff training is developed and delivered.
- Data recovery procedures are tested based on likely scenarios including loss of location/sites.

Key dependencies

- An up-to-date understanding of critical business and public-facing systems and roles.

- Executive management buy-in and commitment to business continuity and disaster recovery.
- Data backup and recovery requirements based on a business continuity objective, including:
  - Budget and cost
  - resourcing requirements
  - backup schedule
  - recovery time
  - security backup requirements
  - and the resilience of the overall recovery solution are defined.
- Procurement process provides appropriate assurance that vendors are aware of an organisation's data recovery requirements and can meet them.

Measurable outcomes

- A data recovery policy is in place, including the date of approval.
- Defined recovery point and recovery time objectives (RPO/RTO).
- Approved training plans.
- Data recovery plan is in place.
- Data recovery audits are regularly undertaken.
- Periodic testing and auditing of recovery plans (incorporating both simulated and real-world recovery).
- Roles and responsibilities for the different types of recovery have been defined.
- Data recovery procedures are in place and regularly tested.
- Evidence of investment/line items for data recovery.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
3.4.10.C.01.	Each system MUST have a system owner who is responsible for the operation and maintenance of the system.
6.4.5.C.01.	Agencies MUST determine availability and recovery requirements for their systems and implement measures consistent with the agency's SRMP to support them.
6.4.6.C.01.	Agencies SHOULD: • Identify vital records, • backup all vital records, • store copies of critical information, with associated documented recovery procedures, offsite and secured in accordance with the requirements for the highest classification of the information, and • test backup and restoration processes regularly to confirm their effectiveness.
6.4.7.C.01.	Agencies SHOULD develop and document a business continuity plan.
6.4.8.C.01.	Agencies SHOULD develop and document a disaster recovery plan.

Response Planning

Standard Statement

Organisations have in place a process to develop and test cyber-incident management plans to ensure business continuity in the event of system or service failure.

Minimum Maturity Level: CMM 2

CMM 4 Quantitatively Controlled	Response plans are tested and updated regularly, aligning to business requirements.
	Adequate oversight and monitoring for response activities undertaken by third parties/vendors.
	Response planning aligns to likelihood, impact, and overall risk management, to keep pace with emerging threats.
CMM 3 Standardised	Response plans are tested and are updated regularly.
	Management is supportive of response planning initiatives and allocates investment and resourcing to response activities.
	Roles and responsibilities for response planning are allocated to job positions and reviewed regularly.
CMM 2 Planned & Tracked	Response plans exist and are updated post-incident.
	Management is supportive of response-planning initiatives.
	Response planning is aligned to likelihood or impact and overall risk management.
	Roles and responsibilities for response-planning are allocated to employees rather than job positions.
CMM 1 Informal	Minimal response-planning procedures are in place.
	No formal testing occurs.
	Roles and responsibilities are undefined or poorly defined.

Focus areas

- Critical business systems
- External-facing systems
- Cloud services

Intent of the Standard

By implementing this Standard, organisations will be better prepared to respond to potential threats and security incidents. In the event of incident realisation, having a response plan will assist in minimising impact and restoring operations.

It is not feasible to have response plans to address all potential incidents. The objective of this Standard is for organisations to put in place response plans to address threats that have the greatest combined impact and likelihood. These plans should align to organisations' risk appetite.

The likely benefits of having a response plan include:

- **An organised approach,** including an agreed understanding across the business of what and how incidents are to be responded to. Security incidents are nearly impossible to predict in advance.
- **Strengthening of overall security** through the inclusion of additional resiliency measures.
- **Trust and confidence** are increased and/or maintained through as a result of knowing an organisation is better equipped to handle incidents.
- **Compliance requirements** are considered and, where appropriate, included within the response plan.

As there are cost and reputational considerations to developing response plans, it is vital that management:

- understands which financial, time, effort, and resourcing requirements are needed to stand-up the plan, and
- allocates adequate resources to support and maintain the organisation's environmental posture.

Suggested actions

The following list is not exhaustive. Organisations should identify which actions are appropriate to implement the Standard based on their current maturity level. However, the following actions follow good-practice guidelines:

- Organisations define which events are to be categorised as incidents factoring in criticality of data, systems under threat, and the level of response for each tier of system.
- Funding and resourcing requirements are identified and allocated.
- Organisations assign personnel to oversee, create, and implement response plans.
- Response planning documentation and artefacts are developed.
- The response plan is communicated to impacted parties.
- Response plans are tested, lessons learned are incorporated into incident response procedures, and results are communicated to appropriate levels within the organisation.
- Threat identification and risk likelihood analysis is undertaken regularly and assigned to an organisation's risk appetite.

Key dependencies

- Critical business systems
- External-facing systems
- Cloud services

Measurable outcomes

- Approved budget/investment for response planning activities.
- Defined system recovery objectives (e.g. Recovery Time Objective/Recovery Point Objective/Acceptable Interruption Window).
- Incident response plans are updated.
- Ongoing testing and development of incident response plans and playbooks.
- Current listing of systems and scenarios that will require response: this could also include evidence of regular review and testing.
- Clearly defined roles and responsibilities.
- An organisational threat identification and analysis assessment.
- Incident communication plan (internally and to stakeholders).
- Security logging, alerting, and monitoring functionality for incident and threat identifiers.

Applicable NZISM Controls

CONTROL REF	CONTROL DESCRIPTION
5.1.12.C.01.	Agencies MUST develop an Incident Response Plan and supporting procedures.
5.1.12.C.02.	Agency personnel MUST be trained in and periodically exercise the Incident Response Plan.
18.3.18.C.01.	Agencies SHOULD develop a Denial-of-Service response plan including: • how to identify the precursors and other signs of DoS, • how to diagnose the incident or attack type and attack method, • how to diagnose the source of the DoS, • what actions can be taken to clear the DoS, • how communications can be maintained during a DoS, and • report the incident.
23.5.10.C.01.	Agencies MUST understand the range of logging capabilities provided by their cloud service providers and determine whether they are sufficient for agency needs.
23.2.18.C.01.	Agencies SHOULD obtain regular assurance checks on cloud service providers, ensuring they have been undertaken by a suitably qualified assessor.

Questions and Answers

Why have the Standards been developed?

The Standards have been developed as part of the NCSC's work supporting the Director-General of the GCSB in their role as Government Chief Information Security Officer (GCISO)

The GCISO is responsible for strengthening government decision-making around cyber security and driving public sector system-wide uplift in cyber security practice. Part of this function is to set minimum cyber security standards for government agencies. Setting standards and guidance falls under the System Lead function for the GCISO as stated in Section 57 of the Public Services Act 2020.

Why are the Standards being published now?

A key driver for publishing the Standards now is to assist agencies in identifying their current levels of maturity against the minimum requirements. This work aligns with wider consultation being undertaken by the Protective Security Requirements team to develop self-assessment questions for agencies to use in accessing their current level of security maturity.

We also recognise that while the Standards will be mandatory for core government agencies, there is widespread interest in the Standards by other organisations and suppliers to government. We are making the Standards available in their current draft form to provide an opportunity for others to understand the Standards and to provide feedback. Previously, government cyber security standards were set primarily through the New Zealand Information Security Manual (NZISM), which remains our comprehensive technical controls catalogue for mandated agencies. The introduction of Minimum Standards allows the GCISO to take a more proactive approach to driving sector-wide uplift against foundational cyber security practices.

How does the Minimum Standards align with other guidance?

We have developed and aligned the Standards to take account of current international good practice. If agencies have adopted equivalent standards, they should be able to see how these are reflected in our Minimum Standards.

Who do the Standards apply to?

The Standards apply to GCISO-mandated agencies. We encourage non-mandated agencies to adopt the Standards as well, to help ensure an uplift in their resiliency levels.

What do the Standards apply to?

The Standards apply to mandated agencies' business-critical and external-facing systems. We have developed Minimum Standards to address risks associated with the highest-value assets and those that present the largest surface attack areas.

How do organisations assess themselves against the Minimum Standards?

Each Standard has a maturity model included. We have aligned the maturity levels of the Standards to the Protective Security Requirements (PSR) Capability Maturity Model, which has five levels. Each level has requirements set in place for organisations to meet.

The minimum level has been set at *CMM2 Planned & Tracked*. We have attempted to make the requirements as objective as possible to enable agencies to make this assessment. The PSR assessment tool has a built-in analysis capability, which will analyse the results inputted and provide a consolidated view of an organisation's maturity based on the self-reporting data inputted.

How can you give NCSC feedback on the Minimum Standards?

Feedback can be provided via email to: gciso@gcsb.govt.nz

How will agencies receive the consultation questions?

The questions will be sent to agencies on Monday 16 June 2025 from the Protective Security Requirements (PSR) team. The questions will be included within the consultation documents.

There are a total of six questions we are seeking feedback on.

Will the Minimum Standards replace the Critical Controls?

No. Minimum Standards are targeted at public sector agencies and include a minimum level of maturity for each Standard that agencies will need to meet. The Critical Controls are designed for a smaller and broader range of organisations companies and are not mandated.

How will you assess compliance with the Minimum Cyber Security Standards?

Compliance will be measured based on how well agencies are meeting the CMM2 maturity level. Going forward, we plan to assess compliance at both the organisational and system-wide level to ensure maturity settings and self–reporting requirements are adequately positioned, and this will be the next phase in the programme of work.

What will the GCISO use compliance information obtained from agencies' self-assessments for?

The information will allow us to measure and track performance across the public sector. It will help us identify areas for improvement and show where we need to focus our efforts to assist organisations to lift their cyber security maturity, either through the NZISM or other forms of guidance and support.

How will you minimise the burden on agencies?

The Minimum Standards are designed in a way that is easier for agencies to engage with and adopt. We have done this by integrating the reporting with the PSR and are being selective in its scope. Additionally, the Minimum Standards mirror the uplift that is required under the NZISM, as agencies are already expected to meet them. The new approach should make it easier for agencies to accurately assess whether their cyber efforts adequately address their risk landscape. These preventative measures should help minimise the likelihood of cyber incidents occurring.

Te Tira Tiaki
Government Communications
Security Bureau

National Cyber
Security Centre