icare | Insurance for NSW

TMF Agency - TMF Declaration 2025/2026 - Cyber Declaration Form

Cyber Risk Management - Cyber Risk Management

Policy Detail
Policy Number: *MFXXXXX*
Line of Business: *PL*

In the last few years, the emerging risk known generally as Cyber has become an issue for all organisations worldwide, TMF has responded by confirming to agencies that their insurable risk arising from Cyber exposures is supported within the TMF Statement of Cover. To understand risk factors and account for resulting exposures, we need to ask questions surrounding this relatively new TMF contribution assessment factor.
The question set should reduce in future years as our partners gain a greater understanding of agency cyber security controls.

Cyber Training Resources : Click here to download the Useful Tips Quick Reference Guide (QRG). Please refer to the Maturity descriptor table below for guidance.

Security Organisation - Roles and Responsibilities

Does the agency have a documented information/cybersecurity structure?

○ *Yes* ○ *No*

Cyber Security Standards/ Frameworks

Are the following cybersecurity standards, strategy, frameworks, or best practices implemented and maintained by the agency. (Please select all that apply)
NIST Cybersecurity Framework (NIST CSF), ASD Essential 8 (E8), PCI-DSS

Is the agency's cyber security program documented in the Enterprise Risk Management Framework and Risk Appetite Statement?

○ *Yes* ○ *No*

The agency's Information/Cybersecurity organisation is: (please select one).

○ *Centralised (e.g. There is a centralised information/ cybersecurity function which oversees all business units).*
○ *Decentralised (e.g. Business units are individually responsible for information/ cybersecurity functions.*
○ *Federated/Hybrid (e.g. Business units have day-to-day management control, but there are centralised information/ cybersecurity policies and standards).*

CISO

Does the agency have a Chief Information Security Officer (CISO), Chief Cyber Security Officer (CCSO) including a senior executive band officer with authority for Industrial Automation and Control Systems (IACS), if applicable or functional equivalent?

○ *Yes* ○ *No*

Privacy Officer

Does the agency have a Chief Privacy Officer (CPO) or a functional equivalent?

○ *Yes* ○ *No*

Incident Containment and Mitigation activities

Does the agency have a formal process or strategy that defines the activities necessary to contain/mitigate different types of incidents or other steps to prevent the expansion of an adverse event?

○ *Yes* ○ *No*

Does the agency have an active contract with incident response service providers to accomplish incident containment, and eradication (e.g. eliminate malware and return systems to normal operations), and orchestrate recovery? If yes, please provide the details.

○ *Yes* ○ *No*

Please provide the details
DRAGOS

Security Awareness Program

Does the agency's cybersecurity awareness program materials train users to avoid common cyber-risks and threats, such as social engineering and phishing?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

In the agency, are annual cybersecurity awareness training and communications mandatory for employees?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Information Security Policies

Does the agency have a documented enterprise or company-wide Information Security Policy?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privacy Policy

Does the agency have documented enterprise or company-wide Privacy Policies?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Physical Security Program

Has the agency implemented a physical security program with risk-based protections (e.g. CCTV, visitor access controls, badge access, and alarms for the perimeter) to secure offices and data centre facilities?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Screening Program

Does the agency's screening and background check require background verification checks including criminal records, credit history, education and reference checks, and employment history as permitted by law?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Third Party Risk Management Oversight

Does the agency conduct security assessments and periodic re-assessments on third-party partners and other service providers with access to information assets?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does the agency review independent audit reports (e.g. SOC 2) from third-party partners and other service providers with access to information assets at least annually?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does the agency require vendors to maintain insurance or any other means of indemnification for losses caused by the provider, including from a privacy breach?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Independent Audits and/or Assessments

Does the agency engage with an independent service provider to:
a) conduct an assessment of its information/cybersecurity program and associated controls?
b) prepare and deliver a report that documents the results of the assessment and recommendations for improvement?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does the agency's internal audit department conduct risk-based audits or assessments of the information/cybersecurity program and associated controls on an annual or more frequent basis?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Incident or Breach Response Plan(s)

Is the agency's incident response or breach response plan formally documented and it is aligned with the NSW Cyber Security Incident Emergency Sub Plan and applicable statutes or regulations?

○ *Yes* *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does the agency's incident response plans include icare NSW, IDSupport NSW, AFP, NSW Police, and Cyber NSW notification?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does your agency have a documented and regularly tested Ransomware Action Plan (RAP)?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Business Continuity/Disaster Recovery Plan

Does the agency maintain a business continuity/disaster recovery plan, and is the plan tested regularly?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does the agency have a Recovery Time Objective (RTO), defined as the maximum target period IT functionality may be lost due to an incident, for critical systems?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does the agency maintain an alternate backup IT facility?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does the agency have the capability for immediate failover to redundant or standby information systems?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

icare™ | Insurance for NSW

TMF Agency - TMF Declaration 2025/2026 - Cyber Declaration Form

Cyber Liability Section - Cyber Liability Section

In the last few years, the emerging risk known generally as Cyber has become an issue for all organisations worldwide, TMF has responded by confirming to agencies that their insurable risk arising from Cyber exposures is supported within the TMF Statement of Cover. To understand risk factors and account for resulting exposures, we need to ask questions surrounding this relatively new TMF contribution assessment factor.
The question set should reduce in future years as our partners gain a greater understanding of agency cyber security controls.

Firewall

Does the agency configure firewalls to prevent unauthorised access, and are the firewall configurations reviewed at least annually?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

In addition to the capabilities above, is the agency's formal firewall policy set up to deny-all by default, permit-by-exception to ensure only explicitly approved incoming/outgoing traffic is permitted?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Network Segmentation

Is the agency's network segmented based on the classification level of the information stored on the servers?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does the agency use a risk-based methodology (e.g. information classification and business criticality) to segment network domains; for domains with high risk/criticality ratings the agency's security appliances deny unexpected or inappropriate flows across network boundaries and has implemented a more rigorous network monitoring?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

In addition to the capabilities above, to mitigate risks/threats and increase the agency's operational resilience, has the agency implemented enhanced security controls/protections, such as, but not limited to:
a) Inbound and outbound traffic filtering at the perimeter
b) Intra-Zone Traffic and Inter-Zone Traffic Monitoring

c) Limiting unnecessary lateral communications (e.g. unfiltered workstation-to-workstation communication)
d) Configuring network device security in conformance with vendor and industry recognised hardening techniques (e.g. Cyber NSW, Center for Internet Security (CIS) Security Configuration Benchmarks or NIST security configuration checklists, etc.)

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Encryption
Does the agency utilise mandatory encryption to protect critical information and other sensitive information (e.g. PII, PHI, etc.) as defined by information classification and protection policies for: ?

Data at Rest

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Data in Transit

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Corporate laptops and desktops

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Data on Removable media

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Mobile Devices (e.g. Mobile phones and tablets)

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Backups

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Software and Hardware Inventory Tools

Are the agency's software and hardware inventory maintained to track operating systems and application versions?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Does the agency use an automated software and hardware inventory tool that provides visibility to information systems across the enterprise?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Are the agency's software inventory system and hardware asset inventory system integrated to track hardware and associated software in a unified register/portfolio?

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

ASD Essential Eight (E8) Mandatory Requirements

Application Control (E8.1) - Please confirm if:

Application control is implemented on workstations and servers.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft's 'recommended block rules' are implemented.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft's 'recommended driver block rules' are implemented.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Application control rulesets are validated on an annual or more frequent basis.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Allowed and blocked execution events on workstations and servers are centrally logged.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Event logs are protected from unauthorised modification and deletion.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

User Application Hardening (E8.2) - Please confirm if:

Web browsers do not process Java from the internet.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Web browsers do not process web advertisements from the internet.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Internet Explorer 11 is disabled or removed.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Web browser security settings cannot be changed by users.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office is blocked from creating child processes.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* *Fully aligned*

Microsoft Office is blocked from creating executable content.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office is blocked from injecting code into other processes.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office is configured to prevent activation of OLE packages.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office security settings cannot be changed by users.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

PDF software is blocked from creating child processes.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

PDF software security settings cannot be changed by users.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Windows PowerShell 2.0 is disabled or removed.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

PowerShell is configured to use Constrained Language Mode.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Blocked PowerShell script execution events are centrally logged.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Event logs are protected from unauthorised modification and deletion.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Restrict Administrative Privileges (E8.3) - Please confirm if:

Requests for privileged access to systems and applications are validated when first requested.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged access to systems and applications is automatically disabled after 45 days of inactivity.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged accounts are prevented from accessing the internet, email and web services.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged users use separate privileged and unprivileged operating environments.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged operating environments are not virtualised within unprivileged operating environments.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Unprivileged accounts cannot logon to privileged operating environments.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Just-in-time administration is used for administering systems and applications.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Administrative activities are conducted through jump servers.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged access events are centrally logged.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged account and group management events are centrally logged.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* *Fully aligned*

Event logs are protected from unauthorised modification and deletion.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Multi-Factor Authentication (E8.4) - Please confirm if:

Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.

○ *Yes* ○ *No (Not Aligned)*

Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.

○ *Yes* ○ *No (Not Aligned)*

Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.

○ *Yes* ○ *No (Not Aligned)*

Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Multi-factor authentication is used to authenticate privileged users of systems.

○ *Yes* ○ *No (Not Aligned)*

Multi-factor authentication is used to authenticate users accessing important data repositories.

○ *Yes* ○ *No (Not Aligned)*

Multi-factor authentication is phishing-resistant and uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

○ *Yes* ○ *No (Not Aligned)*

Successful and unsuccessful multi-factor authentication events are centrally logged.

○ *Yes* ○ *No (Not Aligned)*

Event logs are protected from unauthorised modification and deletion.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Configure Microsoft Office Macro Settings (E8.5) Please confirm if:

Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office macros in files originating from the internet are blocked.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office macro antivirus scanning is enabled.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office macros are blocked from making Win32 API calls.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Microsoft Office macro security settings cannot be changed by users.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Allowed and blocked Microsoft Office macro execution events are centrally logged.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Event logs are protected from unauthorised modification and deletion.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Patch Applications (E8.6) - Please confirm if:

An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, or within 48 hours if an exploit exists.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Applications that are no longer supported by vendors are removed.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Patching Operating Systems (E8.7) - Please confirm if:

A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, or within 48 hours if an exploit exists.

○ *Yes* *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

The latest release, or the previous release, of operating systems are used.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Operating systems that are no longer supported by vendors are replaced.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Regular Backups (E8.8) - Please confirm if:

Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Backups of important data, software and configuration settings are retained in a secure and resilient manner.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Unprivileged accounts cannot access backups belonging to other accounts, nor their own accounts.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts, nor their own accounts.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* *Mostly aligned* ○ *Fully aligned*

Unprivileged accounts are prevented from modifying and deleting backups.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

Privileged accounts (including backup administrator accounts) are prevented from modifying and deleting backups during their retention period.

○ *Yes* ○ *No (Not Aligned)*

Maturity Level

○ *Partly aligned* ○ *Mostly aligned* ○ *Fully aligned*

TMF Agency - TMF Declaration 2025/2026 - Cyber Declaration Form

Cyber Personal Records - Cyber Personal Records

Personal record means any item, collection, or grouping of information about an individual that is maintained by an agency. It includes, but is not limited to, the individual's education, financial, medical, or employment history, or items that contain or make reference to the individual's name, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
A personal health record (PHR) refers to the collection of an individual's medical documentation. This includes details such as but is not limited to:

- **Personally Identifiable Information (PII)** means any information about an individual (data subject) maintained by an agency, including:

Any information that can be used to distinguish or trace an individual's identity, such as name, Tax File Number, date and place of birth, mother's maiden name, or biometric records; and

Any other information that is linked or linkable to an individual, such as medical (Medicare), educational, financial, and employment information.

We consider HR databases to be personal records.

- **Payment Card Industry (PCI)** refers to a debit, credit, or prepaid card "primary account number" (PAN), which is the 16-digit number on the card, the CVV or CVV2 (card security codes), and the individual's PIN, the card expiration date, and the individual cardholder's name.

- **Protected Health Information (PHI)** refers to any information, whether oral or recorded in any form or medium, that:

- Is created or received by a health provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

- Relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

PHI may include details such as but is not limited to:

- The patient's medical history
- Applicable diagnoses
- Historical and ongoing medications, including over-the-counter and alternative treatments
- Past medical and surgical interventions
- Immunisation status
- Allergies and other relevant medical conditions that can impact the delivery of emergency care
- Blood type
- Whom to contact in the event of an emergency
- Insurance information
- Contact information for the patient's regular health providers

Given the increase in cyber-attacks on NSW Government agencies in recent times, a hacker could access any of the databases and the personal records held. We need to understand the potential reach of parties affected if the Agency's system or systems were breached and information leaked or stolen, and the number of persons that could make a claim.
The important thing is not number of records but number of persons affected. E.g. Number of patient records held by each hospital etc. this includes current and historic (1 patient = 1 record), number of employee records held by each Agency (1 employee = 1 record).
We are not after absolutely accurate numbers, but the best estimate that the Agency can provide.

Cyber Personal Records - Cyber Personal Records

Please indicate the type of records held

Approximate number of public sector records processed/held by your agency.

○ *Yes* ○ *No*

Approximate number of records held (Public Sector)

Approximate number of PII (Personally Identifiable Information) records processed/held by your agency.

○ *Yes* ○ *No*

Approximate number of records held (PII)

Approximate number of PHI (Protected Health Information) records processed/held by your agency.

○ *Yes* ○ *No*

Approximate number of records held (PHI)

Approximate number of PCI (Payment Card Industry) related records processed/held by your agency.

○ *Yes* ○ *No*

Approximate number of Hardcopy (vital records) processed/held by your agency.

○ *Yes* ○ *No*

Total Approximate number of records held (value is auto-calculated)

Does your agency have satellite offices/facilities in other geography(ies) or overseas?

○ *Yes* ○ *No*

How many Locations do you have?