ASIC Cyber Pulse Survey

The Australian Securities and Investments Commission, in partnership with Deloitte Touche Tohmatsu (Deloitte), has developed the Cyber Pulse Survey to help your organisation better understand its cyber resilience capability. The survey asks about your organisation's ability to:

- **govern** and **manage** organisational-wide **cyber risks**.
- **identify** and **protect** information assets that support critical business services.
- **detect, respond** to and **recover** from cyber security incidents.

The survey will also allow ASIC to assess the market's cyber maturity on an anonymous basis, and work together with industry to uplift cyber resilience.

Who should complete the survey?

The multiple-choice survey is suitable for ASIC-regulated organisations of all sizes and sectors. Avoiding cyber 'jargon', questions are easy to understand and tailored to the size and scale of your organisation.

Where your organisation is part of a group of companies, the survey should be completed once for the entire group. Responses for the group should be based on the company with the lowest maturity.

If your organisation is small, you will likely be able to answer the questions yourself or with help from your IT support. Larger organisations may require input from their Chief Risk Officer, Chief Information Security Officer and an executive officer or member of the board.

Each section is intended to be completed without needing to refer to other sections. Depending on the nature and size of the organisation, sections may be completed by internal personnel or external service providers.

How do I complete the survey?

To complete the survey, organisations access the Cyber Pulse Survey link hosted on Qualtrics platform via the ASIC regulatory portal. If your organisation is entering the survey for the first time, you will be given the option to complete the survey in one go or receive a unique code allowing you to resume the survey later. The unique code can be shared with others in your organisation whose input may be required to complete the survey. Please do not delete the communication containing the unique code.

When accessing the survey for the first time, your organisation can opt in to receive an individual report following the close of the survey period. The report will provide insight into how you have assessed your organisation's cyber maturity compared to your industry peers.

If your organisation has previously accessed the survey, please enter the unique code to resume the survey. You should only answer questions relevant to your function/s. Please make sure all questions are completed and an 'owner' is assigned to submit the survey on behalf of your organisation.

Who do I contact for help?

cyberpulse@asic.gov.au

Privacy statement

If you opt in to receive a unique code or an individual report for your organisation, Deloitte will collect an email address for your organisation. This email address will only be used by Deloitte for the distribution of the unique code and/or individualised reports back to your organisation. Deloitte will de-identify the survey data before sharing with ASIC and will not share any personal information with ASIC. This means ASIC will not collect, use or disclose any personal information provided by survey participants for ASIC's regulatory or enforcement action. Please refer to ASIC's privacy policy, and Deloitte's privacy statement, for information about how each entity handles your personal information, your rights to seek access to and correct personal information, and how to complain about breaches of your privacy.

About your organisation

What function(s) best describe the role of person or people that completed this survey?	IT Function Management Leadership Other	[Multiple Selection]
Number of employees	Small (1-25 persons employed) [1] Medium (26-199 persons employed) Large (200 or more persons employed)	[Single Selection]
Which type of company best describes your organisation?	Unlisted public company Listed public company Proprietary Company Other (Sole Trader/ Trust / Partnership)	[Single Selection]
What type of ASIC licence does your organisation hold? Please select all that apply.	Australian financial services licence (AFSL) Australian credit licence (ACL) Benchmark administrator licence Clearing and settlement facility licence Derivative trade repository licence Market operator licence The organisation does not hold any of the ASIC licences above.	[Multiple Selection]
What sector best describes your organisation's activity?	Auditors or liquidators' sector Deposit-taking, payments and credit sector Investment management Superannuation sector Market infrastructure sector Market intermediaries' sector Financial advice sector Insurance sector The organisation does not operate in the above sectors	[Single Selection]
What activity/s (subsector) best describe your organisation? You can make more than 1 selection if required.	Auditors or liquidators' sector (a) Company auditor (b) SMSF auditor	[Single Selection]

[1] Small organisations are presented with survey questions in green.

(b) Registered Liquidator

Deposit-taking, payments and credit sector

- (a) Credit Provider[2]
- (b) Credit Intermediaries
- (c) Deposit Product Providers[2]
- (d) Payment Product providers[2]
- (e) Margin Lenders

Investment management

- (a) Responsible Entities[2]
- (b) Wholesale Trustees
- (c) Custodian[2]
- (d) Investor Directed Portfolio Services Operators
- (e) Managed discretionary account (MDA) providers
- (f) Traditional trustee company service providers

Superannuation sector

- (a) Superannuation Trustees[2]

Market infrastructure sector

- (a) Domestic market operators[2]
- (b) Overseas market operators[2]
- (c) Clearing and settlement facility operators[2]
- (d) Other market participants, including derivative trade repository operators[2]
- (e) Credit Rating agencies[2]

Market intermediaries' sector

- (a) Securities exchange participants[2]
- (b) Futures exchange participants[2]
- (c) Securities Dealers[2]
- (d) Corporate Advisors
- (e) Over-the-counter (OTC) traders
- (f) Retail OTC derivative issuers[2]
- (g) Wholesale electricity dealers

Financial advice sector

- (a) Licensee providing financial advice
- (b) Licensee providing general advice
- (c) Licensee providing wholesale advice

[2] Organisations are presented with all survey questions regardless of size.

	(d) Licensee providing advice on products that are not relevant financial products Insurance sector (a) Insurance product providers[2] (b) Insurance product distributors[2] (c) Risk management product providers (d) Claims handling and settling services providers	
What is the most senior role accountable for overseeing the management of cyber security in your organisation?	Board member or other leadership role Senior management Internal IT function External IT function Unknown Other [Free text]	[Single Selection]
Which is the most senior role, group or function responsible for the day-to-day management cyber security for your organisation?	Board member or other leadership role Senior management Internal IT function External IT function Unknown Other [Free text]	[Single Selection]
Does your organisation handle (e.g., store, use and/or transmit) confidential information?	[Y/N]	[Y/N]
How many cyber security incidents did your organisation experience, directly or indirectly, in past two financial years?	10+ 5– 10 2 – 5 less than 2 zero Unknown	[Single Selection]
In the past 24 months, has your organisation had difficulty recruiting and retaining staff (or external expertise) with sufficient cyber security expertise?	Yes Partially No Have not recruited	[Single Selection]
What does your organisation consider are the top three cyber security threats (ranked in order) to the continued operation of your organisation?	Threats in the supply chain Threats to cloud Software threats Insider threats Weak passwords/ credentials Phishing	[Multiple Selection; mandatory selection of 3, ranked]

	Social engineering Business email compromise Ransomware Other [Free text; <50 characters]	
List your organisation's top three technology providers that support the organisation's critical business services, that could cause a major disruption, if any are unable to render their services.	[Free text; 3 fields]	[Free text; 3 fields, <50 characters per field, mandatory]
Which of the following frameworks does your organisation implement or benchmark against?	ACSC Essential Eight Maturity Model American Institute of Certified Public Accountants (SOC2) Australian Government Information Security Manual (ISM) Centre for Internet Security (CIS) Control Objectives for Information and Related Technologies (COBIT) Custom Organisational Internal Standards Cybersecurity Maturity Model Certification (CMMC) Federal Financial Institutions Examination Council (FFIEC) ISO/IEC 27001: Information security management MITRE Privacy Maturity Model National Institute of Standards and Technology (NIST) Cybersecurity Framework NIST SP 800-53: Security and Privacy Controls for IS and Organizations Unknown No standard Other [Free text; mandatory]	[Multiple Selection; mandatory – minimum one selection required]

GOVERNANCE: This section assesses the role of the organisation's leadership in setting strategy and overseeing the management of organisational cyber risk to help ensure the organisation remains cyber resilient.

	A	**B**	**C**	**D**	**E**
Does the organisation understand its cyber risk landscape?	The organisations' leaders do not generally consider the cyber risk landscape the organisation operates in.	The organisations' leaders occasionally consider cyber risk if and when they are reported by the organisation.	The organisations' leaders monitor vulnerabilities in, and threats to, the organisations' information assets that may impact the organisation's critical business services and prevent it from achieving its strategic objectives and priorities.	**In addition to C:** The organisations' leaders monitor cyber risk arising from the organisation's role in the broader industry sector, supply chain and, where applicable, as part of critical infrastructure.	**In addition to D:** Cyber risk is part of a recurring agenda item for the organisations' leaders and metrics are regularly reviewed.
Does the organisation have a cyber security strategy?	The organisation does not have a documented cyber security strategy.	An IT function is responsible for setting a cyber security strategy or policy as and when required.	The organisations' leadership set and periodically review the organisations medium to long term cyber security strategy, which is communicated to all personnel.	**In addition to C:** The cyber security strategy supports the organisations' other strategic objectives and priorities and aligns with the organisations' risk appetite.	**In addition to D:** Additional reviews are triggered if there are material changes in the organisations' cyber risk landscape or risk appetite.
Does the organisation have a framework to support the cyber security strategy?	The organisation does not have a documented framework to deliver its cyber security strategy.	An IT function is responsible for implementing a framework to deliver the organisations' cyber security strategy or policy.	The organisations' leaders have approved a documented framework that supports the organisations' cyber security strategy.	**In addition to C:** The framework is informed by or aligns to a measurable and recognised standard.	**In addition to D:** The organisations' leadership oversights the implementation of the framework to ensure it remains effective in an evolving cyber risk landscape.
Who is empowered to implement the cyber security strategy and framework?	No one person or function is responsible for implementing the framework.	An internal function is responsible for implementing some aspects of the cyber security strategy or policy and framework.	The organisation has identified and documented personnel accountable for the delivery of the cyber security strategy and framework and empowers them to make decisions in line with their level of responsibility.	**In addition to C:** The identified personnel report directly to, or have an open dialogue, with the organisation's leadership.	
Does the organisation consider cyber security capability?	The organisation does not generally consider its cyber security capability.	The organisation considers some aspects of its internal cyber security capability.	The organisations' leadership periodically assess cyber security capability of the organisation.	**In addition to C:** Assessment informs periodic reviews of the internal security capability against the objectives of the cyber security strategy.	**In addition to D:** Assessment informs investment in the organisations' cyber capability build.

Does the organisation have defined cyber security roles and responsibilities?	Cyber security roles and responsibilities are generally not defined or documented.	Some cyber security roles and responsibilities are defined and documented.	Internal cyber security roles, including for the organisations' leaders and IT function, are defined, documented, and communicated to all personnel.	**In addition to C:** External cyber security roles and responsibilities are defined, documented, and communicated to all personnel.	**In addition to D:** Internal and external cyber security roles align with and support the organisations' cyber security strategy.
Does your organisation consider its risk appetite for how much cyber risk it is willing to accept?	The organisation does not have a defined risk appetite related to cyber risk.	The organisation's risk appetite makes general reference to technology.	The organisations' leadership have approved a risk appetite statement that articulates the level and type of cyber risk the organisation is willing to accept.	**In addition to C:** The risk appetite statement includes metrics that enable the organisations' leaders to monitor and measure how the organisation is operating against its risk appetite.	**In addition to D:** Cyber risk that exceeds the organisations' risk appetite are reported to the organisations' leadership.
Are cyber risk managed in accordance with the organisations' risk management framework?	The organisation generally does not have a documented framework to manage cyber risk.	Cyber risk is managed outside of the organisations' risk management framework.	Cyber risk is managed in a framework that aligns to the organisations' risk management framework.	Cyber risk is integrated into, and managed in accordance with, the organisations' risk management framework.	**In addition to D:** Cyber risk is considered in strategic and operational decisions at all levels of the organisation.
Does the organisation comply with cyber security regulatory requirements?	The organisation does not generally identify or document regulatory requirements that relate to the organisations' cyber security.	The organisation manages some compliance with regulatory requirements that relate to the organisations' cyber security.	Regulatory compliance obligations that relate to the organisations' cyber security are managed, identified, documented, and communicated to all personnel.	**In addition to C:** The organisation's leaders monitor the organisations' compliance with regulatory obligations that relate directly or indirectly to the organisations' cyber security.	**In addition to D:** The organisation has established procedures to meet regulatory reporting timeframes that relate to cyber security.
Does the organisation have appropriate cyber risk controls in place?	The organisation does not generally consider cyber risk controls.	The organisation has implemented some cyber risk controls.	The organisation's cyber risk controls are proportionate to the nature, scale and complexity of the business and its information assets.	**In addition to C:** The organisation periodically reviews cyber risk controls.	**In addition to D:** The organisation's leadership evaluates the performance of the cyber risk controls.
Does the organisation test if it is cyber risk controls are effective?	The organisation does not generally test the effectiveness of its cyber risk controls.	The organisations' occasionally test whether some of the organisations' cyber risk controls are effective.	The organisations' periodically test whether the cyber risk controls are effective through internal assurance activities.	The organisations' periodically test whether the cyber risk controls are effective through internal and external assurance activities.	**In addition to D:** The organisations' leadership periodically evaluates the testing of the organisations' cyber risk controls
Do the organisations' leaders know what their role is in the event of a cyber security incident?	The organisations' leadership do not have a defined role in the organisations' response to a cyber security incident.	The organisations' leadership only become involved in the organisations' response to a	The organisations' leadership has a defined role in the organisations' response to a cyber security incident.	The organisations' leadership has a defined role that is documented in the	**In addition to D:** The organisations' leadership participate in the incident response testing.

		cyber security incident if an incident occurs.		organisation's cyber security incident response plan.	

VULNERABILITIES AND THREATS: This section assesses how the organisation identifies, assess and monitors vulnerabilities and corresponding threats to its information assets.

	A	B	C	D	E
Does your organisation identify and prioritise vulnerabilities to information assets?	The organisation does not generally have a process in place to identify and prioritise vulnerabilities to information assets.	The organisation performs vulnerability scanning of some information assets connected to the network.	The organisation consistently uses vulnerability scanning to identify and prioritise vulnerabilities in all information assets.	**In addition to C:** Appropriately qualified personnel identify and prioritises vulnerabilities in accordance with a documented vulnerability management plan	**In addition to D:** Management prioritises the treatment of vulnerabilities and continuous improvement of the vulnerability management plan.
Does your organisation identify and assess threats to information assets?	The organisation does not generally identify and assess threats to information assets.	The organisation does not consistently identify and assesses the criticality of vulnerabilities and threats.	The organisation identifies threats based on their ability to exploit known vulnerabilities and appropriately qualified personnel periodically performs penetration testing to determine the criticality of the threat in accordance with a documented process.	**In addition to C:** The organisation has established a repeatable and continuous improving threat hunting capability to search for search for threats that evades the organisations existing controls.	**In addition to D:** The organisation improves its threat intelligence capability, including through formal and informal information-sharing activities. Critical threats that cannot be remediated are reported to leadership in a clearly understandable way.
How does your organisation monitor physical vulnerabilities and threats to information assets?	The organisation does not generally monitor physical access to information assets.	The organisation some controls to monitor access to the physical environment.	The organisation has controls in place to monitor access to its physical environment, including controls that address insider threats.	**In addition to C:** Physical access to critical information assets is restricted, logged, and monitored to detect potential unauthorised access.	**In addition to D:** The organisation investigates unauthorised access to its physical environment.
How does your organisation assess cyber risk?	The organisation does not generally assess cyber risk.	The organisation assesses some cyber risk, but assessments are not aligned to or integrated with the organisations risk management framework.	The organisation consistently assesses prioritises cyber risks in accordance or alignment with the organisations risk management framework.	**In addition to C:** Appropriately qualified personnel assess emerging cyber risks, including those stemming from new, and material changes to, products, services, and relationships.	**In addition to D:** Assessment aligns to a recognised standard and informs reporting metrics to leadership.

SUPPLY CHAIN RISK MANAGEMENT: This section assesses how the organisation identifies, assesses, and manages risks in its supply chain.

	A	B	C	D	E
Does your organisation manage cyber risk in its supply chain?	The organisation does not generally consider cyber risk in its supply chain.	The organisation assesses some cyber risk in its supply chain, such as assessing cyber risks prior to procurement or new goods or services.	The organisation has a documented policy or process in place to identify and assess cyber risk in its supply chain in line with the organisations’ risk appetite.	**In addition to C:** Where practical, the organisation uses appropriate contractual controls to manage cyber risk in its supply chain.	**In addition to D:** The organisation has agreed on responsibilities with suppliers in the case of a cyber security incident
Does your organisation test its cyber security incident response with critical suppliers?	The organisation does not generally test its cyber security incident response with critical suppliers.	The organisation undertakes testing of a documented cyber security incident response plan with some critical suppliers.	Critical suppliers are identified, and current contact details referenced in the organisations’ cyber security incident response plan. The organisation tests its response to cyber security incidents with its most critical suppliers.	**In addition to C:** Cyber security incident response testing includes tabletop exercises.	**In addition to D.** Cyber security incident response testing includes checklists, walk-throughs or tabletop exercises, and simulations (parallel or full interrupt).

INFORMATION ASSET MANAGEMENT: This section assesses how the organisation identifies, prioritises, and manages information assets essential to its critical business services.

	A	B	C	D	E
Does your organisation identify its critical business services, and their dependencies?	The organisation does not generally identify critical business services and dependencies.	The organisation has identified some critical business services and dependencies.	The organisation has a documented process to identify all critical business services with their dependencies.	**In addition to C:** The organisation reviews critical business services and dependencies when there is material change to or within the organisation.	**In addition to D:** Changes to the organisations’ critical business services, that are approved by leadership, are communicated throughout the organisation.
Does your organisation identify and prioritise its information assets?	The organisation does not generally identify or prioritise information assets.	Some information assets are identified and prioritised.	The organisation identifies all information assets and their owners using a central inventory. Prioritisation of information assets is based on defined prioritisation criteria, including the relative importance of those assets to critical business services.	**In addition to C:** Management periodically reviews and verifies the prioritisation criteria.	**In addition to D:** The relative prioritisation of the information asset informs investment in its protection.

Does your organisation map information flow between its information assets?	The organisation does not generally map information flow.	The organisation maps some information flow between its information assets.	The organisation has a documented process to consistently map all information flow between information assets, including those provided or managed by suppliers and other third parties.	**In addition to C:** Information flow maps include network and data flow diagrams identifying all internal and external connections which are frequently updated in accordance with established change management processes.	**In addition to D:** A central inventory of information asset contains comprehensive diagrams depicting data repositories, information flow, infrastructure, and connectivity.

IDENTITY AND ACCESS MANAGEMENT: This section assesses how the organisation manages access to its information assets.

	A	B	C	D	E
Does your organisation manage user privileges? *	The organisation does not generally have controls in place to manage privileges.	The organisation has some controls in place to manage privileges.	The organisation has controls in place to manage privileges, in accordance with an established process. The organisation regularly reviews and revalidate privileges.	**In addition to C:** All users have uniquely identifiable accounts. Users only have access to the specific information assets that they need for their roles. Unnecessary or outdated privileges are regularly removed.	**In addition to D:** The organisation has a process in place to identify access violations. Administrative privileges are subject to an established approval process. Privileges are validated each time a user access an information asset.
Does the organisation manage administrative privileges?	All users have administrative privileges.	Users are assigned administrative privileges on an ad-hoc basis.	Administrator privileges are limited to a tightly controlled group, monitored, and subject to elevated authentication controls. (i.e., multifactor authentication). The organisation regularly reviews and revalidate administrative privileges. Users with administrative privileges are required to complete advanced cyber security awareness training.	**In addition to C:** The organisation tracks and monitors users with administrative privileges.	**In addition to D:** Information assets are configured using the principles of least functionality. The organisation uses the principles of separation of duties, segregating administrative privileges from other privileges. The organisation uses different accounts for administrative and normal tasks.

Does your organisation manage internal and external consumer access to information assets?	The organisation does not generally have consumers that has access to information assets.	Consumers access information assets using usernames and passwords.	Consumer access to information assets is controlled with password complexity requirements and is blocked when the organisation detects suspicious activity.	**In addition to C:** The organisation uses advanced methods to determine that consumer access is legitimate, i.e., detecting familiar devices, geolocation.	**In addition to D:** The organisation requires consumers to use multifactor authentication to access information assets.
Does your organisation use multifactor authentication? *	The organisation uses single-factor authentication.	The organisation's users can opt into multi-factor authentication.	The organisation uses multi-factor authentication, with no ability for users to opt out.	**In addition to C:** Multifactor authentication is resistant to impersonation. Multifactor authentication attempts are monitored for indicators of attack.	**In addition to D:** The organisation has baselined personnel actions to detect suspicious activity that are assessed in a central security incident and event logging system. The organisation uniquely identifies and authenticates devices before establishing a connection.
Does your organisation configure information assets to provide only essential functionality?	The organisation does not generally limit functionality of information assets.	The organisation limits functionality of some information assets.	The organisation disables any functionality of an information assets that is unnecessary or insecure. The organisation configures information assets to provide only essential functionality and specifically prohibit or restrict functionality that are not required.	**In addition to C:** The organisation frequently identifies and removes unnecessary functionality.	**In addition to D:** The organisation has controls in place to prevent or limits unnecessary changes to functionality.

CYBER SECURITY AWARENESS TRAINING: This section assesses what level of cyber security training the organisation provides its personnel and others.

	A	B	C	D	E
Does your organisation provide cyber security awareness training to personnel?	The organisation does not generally provide cyber security awareness training to personnel.	Cyber security awareness training is provided to some personnel.	Mandatory cyber security awareness training is periodically provided to all personnel.	**In addition to C.** Tailored cyber security awareness training is provided to personnel relative to their seniority, role, privileges, and responsibilities. The organisation evaluates personnel completion rates	**In addition to D.** Where applicable, the organisation seeks to enhance consumer cyber security awareness, updating the content regularly.

				and tests cyber security awareness, including by performing simulation exercises.	
DATA SECURITY: These questions assess to what extent the organisation protects the confidential information it holds.					
	A	**B**	**C**	**D**	**E**
Does your organisation encrypt confidential information?	Confidential information is generally not encrypted.	The organisation encrypts some confidential information.	The organisation identifies and assesses confidential information to determine if encryption is appropriate in accordance with established criteria and process. Controls are in place to prevent unauthorised access and disclosure of cryptographic keys used for encryption.	**In addition to C:** The organisation has implemented cryptographic mechanisms, consistent with recognised standards.	**In addition to D:** The organisation uses full-device or container-based encryption for all device types including mobile devices. The organisation stores cryptographic keys in a hardware-protected key store
Does your organisation prevent unauthorised transmission of confidential information?	The organisation does not generally have controls to detect the unauthorised transmission of confidential information.	The organisation has some controls to detect the unauthorised transmission of confidential information.	The organisation has implemented controls (i.e.., data loss prevention) to detect and prevent unauthorised transmissions of confidential information.	**In addition to C:** The organisation scans outgoing emails and data transfers to detect and prevent unauthorised transmission of confidential information.	**In addition to D:** The organisation frequently monitors internet sites for evidence of unauthorised disclosure of confidential information.
Does your organisation manage data destruction?	The organisation does not have a data destruction policy.	The organisation has a data destruction policy.	The organisation destroys data in accordance with its data destruction policy, which is periodically reviewed. Data that is no longer required to be retained are securely disposed of within expected time frames.	**In addition to C:** The organisation tests its data destruction mechanisms to ensure that data is not recoverable by any forensic means.	**In addition to D:** Data destruction mechanisms are proportionate to the nature or type of data being destroyed.
PROTECTION OF INFORMATION ASSETS: This section assesses how the organisation protects its information assets.					
	A	**B**	**C**	**D**	**E**

Does the organisation harden the configuration of its information assets? *	The organisation does not generally harden the configuration of its information assets.	The organisation uses some recognised standards or guidelines to harden the configuration of its information assets.	The organisation follows recognised standards for hardening its information assets configurations. The organisation uses baseline configurations from reputable organisations (i.e., ACSC and vendors).	**In addition to C:** The organisation configures all information assets to enable only essential functionality and specifically prohibit or restrict functionality that is not required.	**In addition to D:** The organisation uses advanced cyber security principles, to harden the configuration of its information assets including secure by default, secure by design.
Does your organisation ensure adequate access to information assets?	The organisation does generally consider backup, recovery, and contingency plans.	An IT function maintains and tests a backup, recovery, and contingency plan for some information assets.	A documented backup, recovery, and contingency plan exist for all information assets. Plans are periodically tested to determine whether controls are effective, including those in place to address disruptive cyber attacks	**In addition to C:** The organisation has established alternative processes and information assets to resume critical business services within a reasonable period.	**In addition to D:** The organisation has determined the level of backup required (i.e., personnel, configuration, documentation) and backup protection requirements. Regular failover testing is consistent with the organisation's recovery time target.
Does your organisation protect its network?	The organisation does not have a defined approach to protect its network.	The organisation uses a security model in which everyone inside the network is trusted by default.	The organisation uses a defence-in-depth approach to network security, with multiple layers to protect the organisation from external cyber attacks.	**In addition to C:** Controls are in place to ensure network segments are established and operating appropriately.	**In addition to D:** The organisation segments the network into multiple, separate trust or security zones with strategies to mitigate potential cyber attacks.
Does your organisation protect transmission of data?	The organisation does not have a defined approach to protect the transmission of data.	Some transmission of data is encrypted when it occurs across public or untrusted networks.	The transmission of all data is encrypted when it occurs across public or untrusted networks.	**In addition to C:** The transmission of all data is encrypted when it occurs across private and public connections.	**In addition to D:** Proactive controls are in place to prohibit the transmission of data displaying unusual or suspicious behaviour.
How does your organisation maintain the resiliency of information assets? *	The organisation has not generally implemented any resilience controls.	The organisation has implemented some resilience requirements and controls for operating states.	The organisation has a documented plan that sets out resilience requirements for all operating states, including for business as usual and disaster recovery The organisation periodically tests its resilience controls,	**In addition to C:** Resilience controls include distributing information assets. The organisation regularly tests the resilience controls that support its critical business services.	**In addition to D:** The organisation has established an alternate processing site to enable the resumption of information assets that support critical business services, including necessary agreements to permit the transfer and resumption of information

			including load balancing and fail-safe.		assets within a period consistent with established recovery time and recovery point objectives.

CONTINUOUS MONITORING: This section assesses how the organisation continuously monitors its information assets and network.

	A	B	C	D	E
Does your organisation monitor network activity?	The organisation does not generally monitor network activity.	The organisation monitors some network activity or monitors network activity occasionally.	Appropriately qualified personnel and tools continuously monitor activity on the network for unexpected behaviour. The organisation has defined roles and responsibilities for responding to unexpected behaviour in accordance with documented requirements.	**In addition to C:** The organisation has deployed automated tools to detect potentially unexpected behaviour. The organisation frequently reviews logs of following the detection of unexpected behaviour.	**In addition to D:** The organisation analyses patterns of unexpected behaviour are reported to improve controls and mitigate organisational risk.
Does your organisation baseline normal network activity?	The organisation generally does not baseline network activity.	The organisation baselines some network activity.	The organisation periodically baselines normal network activity and configures information assets to report unexpected behaviour.	**In addition to C:** The organisation uses security event monitoring tools (SIEM) to monitor network activity and baselines and report any unexpected behaviour.	**In addition to D:** The organisation uses security event monitoring tools (SIEM) to monitor baselines of identities, information assets and network activity, and report any unexpected behaviour.
How does the organisation perform vulnerability scans of information assets?	The organisation does not generally conduct vulnerability scans.	The organisation conducts some vulnerability scanning.	The organisation regularly monitors and scans information assets for vulnerabilities, including before deployment. Information assets are equipped with endpoint detection and response controls (EDR). When new vulnerabilities potentially affecting the information assets are	**In addition to C:** Information assets are equipped with enhanced endpoint detection and response controls (XDR).	**In addition to D:** The organisation employs vulnerability scanning tools that can identify emerging vulnerabilities. The organisation analyses vulnerability scan reports to determine whether similar vulnerabilities exist in other information assets.

			identified, they are reported, and remediated.		
Does your organisation patch information assets?	The organisation does not generally patch information assets.	The organisation conducts patching on an ad hoc basis.	The organisation regularly conducts scheduled patching of information assets.	**In addition to C:** The organisation prioritises patching relative to the criticality of the vulnerabilities.	**In addition to D:** The organisation has ongoing visibility of its patching status.
Does your organisation monitor user and personnel activity, including employees, contractors and third parties?	The organisation does not generally monitor user or personnel activity on information assets.	The organisation monitors some user or personnel activity on information assets.	Appropriately qualified personnel and tools continuously monitor user and personnel activity on information assets for unexpected behaviour (network use patterns, work hours, and known devices) and provide alerting for unexpected behaviour. The organisation has defined roles and responsibilities for responding to unexpected behaviour in accordance with documented requirements.	**In addition to C:** The organisation monitors the users and personnel for unexpected behaviour. A central security incident and event monitoring platform (SIEM) correlates all information asset and user events to alert for the organisation to detect unexpected behaviour.	**In addition to D:** The organisation has implemented and manages endpoint and network protection tools that profiles user and personnel behaviour and device usage patterns. The user and personnel profile and behaviour characteristics informs investigations and control effectiveness.
Does your organisation monitor for unauthorised connections, devices, and software?	The organisation does not generally monitor unauthorised connections, devices, and software.	The organisation occasionally monitors for the presence of unauthorised connections, devices, and software.	The organisation regularly monitors for the presence of unauthorised connections and devices and prohibits the unauthorised installation of software.	**In addition to C:** Monitoring is achieved through various tools and techniques (i.e., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software).	**In addition to D:** Monitoring is used to identify potentially compromised information asset or information asset components.

INCIDENT MANAGEMENT: These questions assess how the organisation responds to cyber security incidents.

	A	B	C	D	E
Does your organisation have a cyber security incident response plan? *	The organisation does not have a cyber security incident response plan.	The organisation has a cyber security incident response plan	The organisation has a documented cyber security incident response plan.	**In addition to C:** The cyber security incident response plan includes the requirement for the	**In addition to D:** The organisation has established criteria for

				organisation to document incident investigation and mitigation activities.	escalating cyber security incidents to leadership.
Does your organisation ensure appropriate steps are taken to contain, remediate a cyber security incident?	The organisation generally does not consider containment and remediation of cyber security incidents	The organisation does not have a formal plan for the containment and remediation of cyber security incidents.	The organisation has a documented plan that includes strategies to contain and mitigate various types of cyber security incidents (e.g., DDoS, malware, ransomware).	**In addition to C:** Containment strategies include notifying impacted third parties, consumers, and relevant regulators. Mitigation strategies are designed to minimise disruption to critical business services.	**In addition to C:** Cyber security incidents response testing includes testing of containment strategies, such as red and blue teaming.
Does your organisation test its response to cyber security incidents and events?	The organisation does not generally test its response to cyber security incidents and events.	The organisation occasionally tests its response to cyber security incidents and events	Desktop exercises are conducted regularly to assess the effectiveness of the cyber security incident response plan.	**In addition to C:** Desktop exercises scenarios include range of different threat scenarios. Lessons learnt from real-life cyber security incidents experienced by others are incorporated into the plan and the awareness training.	**In addition to D:** The organisation participates in intelligence exercises and cyber security incident simulations with external stakeholders, using threat intelligence relevant to the organisations sector.
Does your organisation investigate cyber security events?	The organisation does not generally investigate cyber security events.	The organisation occasionally investigates cyber security events.	Appropriately qualified personnel have the tools to investigate cyber security events. The organisation has a documented process is in place for conducting incident triage or investigations	**In addition to C:** Cyber security events that are deemed to be cyber security incident are escalated in accordance with a documented process.	**In addition to D:** Cyber security events are analysed for broader behavioural patterns.
Does your organisation use external sources of threats intelligence?	The organisation does not generally use external threat intelligence sources.	The organisation relies on third parties to notify them of threat intelligence that may affect information assets.	The organisation consistently monitors the ACSC and other reputable sources for the most recent threat intelligence and identifies corresponding vulnerabilities.	**In addition to C:** Detection and response controls are adapted in in response to threat intelligence when required.	**In addition to D:** The organisation conducts threat modelling using recognised standards.

Does your organisation seek to understand the root cause of cyber security incidents?	The organisation does not generally perform root cause analysis on cyber security incident.	The organisation occasionally conducts root cause analysis on select cyber security incident.	The organisation consistently conducts root cause analysis on all cyber security incident.	**In addition to C:** Security investigations, analysis, and remediation are performed by qualified personnel, including forensic analysis when required.	**In addition to D:** The organisation uses best practices and industry approved forensic procedures, including chain-of-custody to collect and collate evidence to support discovery and documentation of evidence.
RECOVERY PLANNING: These questions assess to what extent the organisation maintains recovery processes and procedures to restore information assets affected by cyber security incidents.					
	A	**B**	**C**	**D**	**E**
Does your organisation have a plan to recover from cyber security incidents?	The organisation does not generally have a formal recovery plan.	The organisation has some elements of a recovery plan.	The organisation has a recovery plan that is regularly reviewed and updated.	**In addition to C:** The recovery plan identifies key personnel and recovery procedures. Recovery operations focus on critical business services including recovery points, recovery time, and recovery objectives.	**In addition to D:** The organisation conducts business continuity and failover testing on a regular basis. The recovery plan also includes assessments of fully restored system capabilities, re-establishment of continuous monitoring activities, system reauthorisation, and activities to prepare for future disruptions, breaches, compromises, or failures.
Does your organisation incorporate lessons learnt in its cyber security incident response plan?	The organisation does not generally conduct post-incident reviews of cyber security incident.	The organisation conducts some post-incident reviews of cyber security incident.	**In addition to B:** Qualified personnel lead post-incident reviews of all cyber security incidents. The organisation identifies the lessons learnt from post-incident reviews and updates the cyber security incident response plan and other relevant controls.	**In addition to C:** Lessons learnt from cyber security incidents informs investment in the organisation's cyber risk controls and capabilities.	**In addition to D:** The organisations' leadership participates in post-incident reviews.

CONSEQUENCE MANAGEMENT: This question assesses how the organisation communicates its restoration activities and interacts with internal and external parties, including coordinating centres, service providers, owners of systems, government, regulators, victims, other security incident response teams, and vendors.					
	A	**B**	**C**	**D**	**E**
Does your organisation have a strategy for the consequences of cyber security incidents?	The organisation does not generally consider potential consequences of cyber security incidents.	The organisation has a strategy to manage the consequences of cyber security incidents to the organisation.	The organisation has a strategy to manage the direct consequences of cyber security incidents to the organisation, consumers and regulators, including a communication plan. The communication plan includes a current list of government agencies to notify if cyber security incident occurs.	**In addition to C:** The strategy sets out the controls to reduce the indirect harm to other stakeholders. The strategy includes sharing of information relevant to the cyber security incident where practical.	**In addition to D:** The organisation has identified the potential harm that could result from common types of cyber security incidents and has developed specific strategies to reduce those harms, including a position on payments resulting from ransomware.

Appendix A: Interpretations

TERM	MEANING
administrative privileges	user access ability to modify information asset above the level of basic access.
privileges	the level of access required for the user to perform the required task on behalf of the organisation.
user	personnel or service accounts with access to the organisation’s information assets.
business email compromise	a type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential information.
capability	the collective human and technological skills, abilities, and expertise of the organisation.
cloud computing	storage and access of information and programs over the internet without the need for physical infrastructure.
confidential information	any information that is confidential in nature, including information that has commercial value and personal information.
control	a method or means to manage risk.
critical business services	any activity, function, process, operation or service, the loss of which, for even a short period, would materially affect the continued operation of the organisation, or its consumers or investors, market integrity or the broader Australian financial system.
cyber attack	a deliberate or malicious attempt to gain unauthorised access to an information asset connected to a network.
cyber security event	an occurrence in an information asset.
cyber security incident	an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising critical business services.
cyber security incident response plan	a set of instructions on how to respond to a cyber security incident.
cyber security strategy	a plan of action to manage an organisations’ cyber risk and maintain its cyber resilience, whether standalone or integrated into other strategies.
cyber risk	the likelihood and impact of a threat exploiting a vulnerability and adversely impacting an information asset or the organisation.
cyber resilience	an organisation’s ability to prepare for, respond to and recover from cyber security incidents.
dependencies	relationships of reliance within and among information assets.
elements of a recovery plan	Elements include having a detailed cyber incident response plan, a business continuity plan, and safe backups to resume operations and recover or rebuild the lost data
event monitoring	the process of collecting, analysing, and communicating event occurrences of information assets.
framework	a system of organisational policies, procedures, practices, and controls, whether standalone or integrated into other frameworks.
harden configuration	Configuring information assets by prohibiting or restricting functionality and reducing the attack surface.
IT function	a function responsible for providing technical support in relation to organisation’s information assets, whether that function is within the organisation or provided by a third party.
insider threat	a malicious threat to an organisation that comes from personnel within the organisation.
information asset	information and information technology (including software, hardware, firmware, systems, and data (both hard and soft copy)), whether managed by the organisation or a third party (e.g., vendor or supplier).
leader or leadership	the person or people responsible for setting strategy and overseeing the management of the organisation.
load balancing	the method of distributing network traffic and processing across information assets.
malware	software that has a malicious intent.
malicious actor	An individual or individuals that is partially or wholly responsible for an incident that impacts, or has the potential to impact, an organisation’s security.
multifactor authentication	an authentication method that requires the user to provide two or more verification factors.
network	connected computer infrastructure such as computers, digital devices, and other information assets.

patching	the act of applying a change to installed software that corrects security or functionality problems or adds new capabilities to information assets.
personal information	information or an opinion about an identified individual, or an individual who is reasonably identifiable.
personnel	people employed or engaged by the organisation.
penetration testing	a simulated set of cyber attacks against information assets to determine the exploitability of vulnerabilities.
phishing	a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing confidential information.
ransomware	a type of malware that threatens to publish the victim's confidential information or permanently block access to it unless a ransom is paid.
recognised standard	a standard, guideline, document, or practice that is generally accepted by the industry in which the organisation operates.
risk appetite	the amount of risk the organisation is willing to accept to achieve its objectives
senior management	personnel at the highest level of management of an organisation who are responsible for day-to-day management of that organisation.
social engineering	a manipulation technique that exploits human error to gain access to confidential information.
software threats	malicious computer code and applications that can cause damage to information assets.
supply chain	a network of people, organisations, information assets and resources involved in delivering goods or services.
threat	any activity that has the potential to exploit a vulnerability.
threat intelligence	information about existing and emerging cyber threats that relate directly or indirectly to information assets or the organisation.
threat hunting	a proactive security search through information assets, including networks and data sets, to hunt malicious, suspicious, or unusual activities.
unauthorised access	when person or organisation gains logical or physical access without permission to a network, information asset, data, or other resource.
vulnerability	a weakness in information asset security, design, implementation, or operation that can be exploited.
vulnerability scanning	an inspection of the information assets or the network to identify vulnerabilities.
vulnerability management plan	a risk-based, established continuous process within the organisation designed to address the need to identify and remediate vulnerabilities.