AUCLOUD

CYBER SECURITY MATURITY ASSESSMENT

Client: ACME PTY LTD
Conducted by: John Citizen
Date of assessment: 09-11-2023
Version 1.0

SAMPLE

1800 282 568
assurance@aucloud.com.au

Table of Contents

SAMPLE

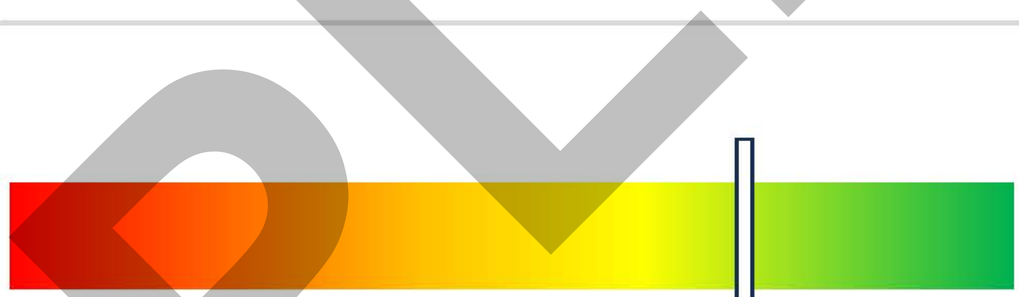
1800 282 568
assurance@aucloud.com.au

Cyber Security Maturity Assessment Summary

ACME PTY LTD
ABN: 00 000 000 000
Conducted by: John Citizen
Date of Assessment: 09 November 2023

Governance	✓
Risk Management	⚠
Security Awareness	⚠
Access Control	✓
Patch Management	✓
Application Whitelisting	⚠
Network Security	✓
Data Protection	✓
Multi-Factor Authentication	✓
Incident Response	⚠

72 Overall Assessment Rating



General information about this rating:

This Cyber Security Maturity Assessment has been conducted by AUCloud using a proprietary assessment model which adopts industry best practices and guidance. The assessment includes 10 domain areas and comprises of 55 security control statements. Using the information from client interviews, AUCloud has reviewed the responses and applied a weighting indicator to produce an overall security rating.

From the assessment completed it was identified that ACME PTY LTD were effective in Governance, Access Control, Patch Management, Network Security, Data Protection and Multi-Factor Authentication, requiring only minor improvements in these domains. Further recommendations have been made in the domains of Risk Management, Security Awareness, Application Whitelisting, and Incident Response to strengthen the organisation's security posture.

The Overall Assessment Rating was 72%. The higher the score the lower the cyber security risk. This score indicates a mature level of security controls have been implemented across the organisation. A targeted investment of resources could reduce risk and improve the organisation's cyber security protection and capabilities.

SAMPLE

1800 282 568
assurance@aucloud.com.au

From the AUCloud CISO

On behalf of AUCloud, I would like to thank you for choosing our cyber security services to safeguard your valuable assets and sensitive information.

At AUCloud, we understand the importance of maintaining a secure and resilient digital environment in today's rapidly evolving technology landscape, including both the risks and opportunities that it presents us. We are pleased to have been able to partner with Acme Pty Ltd on this engagement and look forward to future opportunities. AUCloud is committed to excellence and endeavour to build a culture of continuous improvement and a proactive approach to cyber security.

I trust that this report and the advice from the AUCloud team will provide additional understanding of your strengths and weaknesses and assist in achieving your cyber security goals and objectives.

Once again, thank you for choosing AUCloud as your cyber security partner. Should you have any questions, concerns or feedback, please do not hesitate to reach out to our dedicated team who can assist you further.

Regards,

Peter Fitzgerald
Chief Information Security Officer
AUCloud

SAMPLE

1800 282 568
assurance@aucloud.com.au

Executive Summary

AUCloud was engaged by Acme Pty Ltd to conduct a Cyber Security Maturity Assessment. The assessment focussed on the organisation's cyber security controls and practices in 10 security domains and was performed by AUCloud using a proprietary assessment model which adopts industry best practices and guidance. An interview was conducted with Mr Duncan Little (Chief Executive Officer) and Mr Luiz De Almeida (Chief Information Officer) from Lavlantiss who provide an MSP function to MCW. AUCloud has analysed the responses and the assessment findings and recommendations are presented in this report.

AUCloud noted the effective management of security controls across six of the 10 domains. The organisation has implemented an overarching governance process and have effective technical controls in place. It was noted however that there was a small degree of ambiguity about roles and responsibility, but we believe that was due to the nature of changing service responsibilities within MCW.

The onboarding and offboarding processes are followed and align to a fully managed account management lifecycle. The issue and use of privileged and Administrator accounts is also controlled.

The organisation has a mature patch management capability, guided by a policy and controlled through technical controls. There is the capability to rapidly deploy security patches to address critical security vulnerabilities and ongoing and frequent scanning for system vulnerabilities on internal and external facing systems.

Controls in the network security domain are effectively addressed with the implementation of technical solutions and processes. This includes the ability to monitor network activity and the transfer of large files and specific file types, email filtering, web access controls and monitoring of the dark web for signs of account compromise.

Backups of systems and data have been implemented for internal and cloud-based systems. The restoration from backup systems is frequently tested to ensure that backup data is accessible.

Authentication to systems is fully managed with the enforcement of complex password requirements and multi-factor authentication across internal and cloud-based systems for all users. A policy and technical controls are also in place for the management of privileged, system, local and service accounts.

SAMPLE

1800 282 568
assurance@aucloud.com.au

The domains which AUCloud assessed which could be improved are Risk Management, Security Awareness, Application Whitelisting, and Incident Response.

It was noted that a risk management framework is in place and risk assessments were conducted annually and there was an opportunity to mature these processes and increase frequency. There is also an understanding of the critical business information and services however this should be formalised. There are various sources which capture asset information, but formal hardware and software registers could be developed to ensure completeness and centralised management as a way of reducing the organisations attack surface and risk profile.

The organisation has recognised that there are gaps in incident response capabilities. This includes the need for an Incident Response Plan and clearer processes for handling incidents internally and externally, establishing an Incident Response Team, and conducting regular testing exercises to simulate security incidents and events. Consideration should also be given to crisis communications in the event of a cyber security incident or data breach.

The technical controls which could be implemented by the organisation to reduce security risks include application whitelisting, Microsoft Office macro security, and removeable media (e.g. USB drives) access monitoring and controls. At the time of assessment, no gaps were evident for these topics, but they are commonly known as being effective ways of reducing the risk of cyber security incidents. These controls also form part of the Australian Cyber Security Centre (ACSC) Essential 8 framework which continues to gain traction across a variety of industries within Australia.

Further information is available in the Key Recommendations section of this report.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Assessment Process

This Cyber Security Health Assessment has been conducted by AUCloud for ACME PTY LTD. The intent of the assessment was to review the organisation's cyber security posture through understanding the current security policies, procedures, and technical controls in place.

AUCloud has developed this assessment report using information provided by ACME PTY LTD and its representatives during interviews. The assessment focuses on key security domains and controls which are developed from best practice security frameworks. Responses to each question have been captured using pre-defined response options with the addition of a free text field where necessary.

The report highlights ACME's strengths and weaknesses and provides recommendations to guide improvement. AUCloud has prioritised the high risk areas and provided detailed remediation actions to address these. The report focuses on outcomes and does not recommend specific technologies, products, or vendors.

The following people have contributed to the assessment and report:

Name	Role
Duncan Lima	Lead Ethical Hacker
Luiz De Almeida	Lead Ethical Hacker
Joel Robertson	AUCloud Territory Sales Manager
Peter Connolly	AUCloud Chief Information Security Officer

SAMPLE

1800 282 568
assurance@aucloud.com.au

Key Recommendations

This section details the key recommendations. These are the recommendations which AUCloud have assessed as being the most important and effective. Additional recommendations are included in the respective security domain tables.

Recommendation 1
Develop Incident Response Capabilities

- Develop an Incident Response Plan (IRP) which is tailored to the organisation's needs. The IRP should be developed with the support and input of the executive and business stakeholders. Testing of the IRP should be conducted to ensure it remains executable, relevant and comprehensive.

- Establish an Incident Response Team (IRT). The membership of the IRT should consist of management and technical roles which are required in the event of an incident. The membership of the IRT should be defined in the Incident Response Plan.

- Determine the legislative and contractual obligations for communicating and notifying customers of a security incident. The steps to be taken by the organisation should be defined in the Incident Response Plan.

- Conduct regular tabletop exercises that involve the IT service provider, business representatives, and the executive. Tabletop exercises allow various common and uncommon scenarios to be simulated and provides the organisation an understanding of its abilities in handling security incidents and addressing potential consequences.

- Develop a Data Retention Policy which defines the storage and handling requirements for the categories of data stored and processed by the organisation. Ensure archive and backup solutions are adequate to meet regulatory and customer obligations.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Recommendation 2:
Consider Implementing Application Whitelisting Controls

- Consider implementing an application whitelisting solution. The solution should be tailored to the organisation's requirements and business operations. Application whitelisting should be applied on end-user systems (laptops and workstations) and servers to prevent the execution of malicious applications particularly from the internet and to control the installation of unauthorised software. Enable logging and where possible, logs should be forwarded to a central storage and monitoring capability.

- Develop internal procedures for the review of new software requests and executable files shared with the organisation. An appropriate review and installation procedure should be in place to meet business needs and reduce security risks from unapproved software and unverified files.

- Establish a Software Register and standard operating procedure which ensures that all software assets are captured and classified. An Asset Owner should be assigned to each asset or asset class. The software register could also be expanded to include external services such as cloud-based applications.

Recommendation 3:
Consider Implementing a Microsoft Office Macro Security Strategy

- Assess the risk of malicious office macros being received/transferred to the organisation's systems. Consider implementing a macro security strategy using guidance from the ACSC. There are five documented strategies, each with varying levels of effectiveness and restrictions. Business use cases should be considered when selecting a strategy. Ensure logging is enabled and capture successful and failed executions. Where possible, logs should be forwarded to a central storage and monitoring capability.

SAMPLE

1800 282 568
assurance@aucloud.com.au

- Review Windows Group Policy settings to restrict employee access to modify Microsoft Office security settings. This will prevent employees, or an attacker from disabling security controls to execute a malicious macro file.

Recommendation 4:
Consider Implementing a Removeable Device Monitoring and Control Solution

- Review the business requirement and user case for the use of USB devices and other removeable media within the organisation. Evaluate the requirements against risks. Implement a Media Device Control Management Policy. This should include the use of storage devices such as USB drives and external hard drives, as well as the connection of devices such as printers and mobile phones.

- Implement security controls which enforce the organisation's policy. This could involve restricting the use or blocking access to particular roles and specific devices. Ensure the solution has a logging and auditing capability. Where possible, logs should be forwarded to a central storage and monitoring capability.

- Where technical controls cannot be implemented, consider alternate controls which include monitoring and logging of transactions and ensure devices are scanned before execution.

SAMPLE

Recommendation 5:
Mature the Organisation's Governance and Risk Management Framework

- Continue to develop and align the cyber security framework. Formalising the framework is critical as it sets the guidance for the security program and operations. The framework will provide a structured approach to risk management and the implementation and delivery of security controls. Where security policies have been developed and endorsed by the

1800 282 568
assurance@aucloud.com.au

executive. These should be communicated and accessible to employees for awareness and guidance.

- Formally document a Business Impact Assessment (BIA). This allows mission critical information and services to be defined and agreed. The BIA should be used to inform priorities for business continuity and decisions around risk management.

- Increase the frequency of conducting risk assessments and hosting risk/security meetings as appropriate.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Assessment Questions

This following tables include the assessment questions, the response provided by Acme Pty Ltd, and the respective recommendation. Each question also includes an explanation of the importance of the domain area.

The domains covered in the assessment are:

- Governance
- Risk Management
- Security Awareness Training
- Access Control
- Patch Management
- Application Whitelisting
- Network Security
- Data Protection
- Multi-Factor Authentication
- Incident Response

SAMPLE

1800 282 568
assurance@aucloud.com.au

Governance

Governance refers to the set of policies, processes, and controls that guide and oversee an organisation's approach to managing and securing its information assets. Effective governance is integral to managing risks, complying with regulations, making informed decisions, responding to incidents, and safeguarding an organisation's assets and reputation.

This section reviews the organisation's level of executive support for cyber security and adoption and implementation of frameworks.

ID	Question	Importance	Answer Provided	AUCloud Recommendation
GOV	The organisation has executive level support for establishing cyber security goals and objectives.	Executive level support for cyber security ensures that the necessary resources and authority are allocated to implement and maintain cyber security measures, complying with regulations, and aligning security efforts with the organisation's strategic goals.	N/A	Continue to manage risk and compliance. Develop and track progress towards cyber security goals with the support of the executive.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Governance	Importance	Assessor Prescribed	AUCloud Recommendation
GV02	Cyber security risks and issues are an ongoing agenda topic at the executive / board level.	Ongoing discussions about cyber security risks and issues at the executive level ensures that cyber security remains a priority, receives the necessary resources, and that all stakeholders are informed and engaged in safeguarding their organisation against cyber threats.	Monthly or more frequently	Continues to prioritise cyber security as an agenda topic in executive level discussions to ensure it remains up-to-date with evolving threats and risks.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question	Importance	Answer Provided	AUCloud Recommendation
1010	The organization has a designated person or team responsible for overseeing cyber security	Having a designated person or team responsible for overseeing cyber security ensures that the organization has the expertise, focus, and structure needed to effectively protect against cyber threats, manage risks, and respond to security incidents	Clearly designated with authority	Continues to develop and promotes cyber security goals and outcomes with the Head of Security

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Question	Importance	Answer Provided	AUCloud Recommendation
GOV-1	The organization adheres to a cyber security framework and has well-defined and documented policies and procedures in place that are communicated to all staff.	Adherence to a cyber security framework and the presence of well-defined policies and procedures that are communicated to all staff are essential for maintaining a consistent, secure, and compliant cyber security posture, while promoting a culture of accountability and awareness.	Partially Established	Continue to develop and align the cyber security framework. Emphasizing the importance of robust policies for the security program and operations. The framework will provide a structured approach to risk management and the implementation and delivery of security controls. Where security policies have been developed and endorsed by the executive, these should be communicated and accessible to employees for awareness and guidance.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question	Importance	Answer Provided	AUC Recommendation
1015	The organization has a well-documented disaster recovery and business continuity plan that are tested on a regular basis.	A well-documented disaster recovery and business continuity plan, along with regular testing, is essential for ensuring the organization's ability to recover from disruptions, protect data and assets, maintain operations, comply with regulatory and [illegible]	Formally approved plan which is reviewed at least annually	Continue to review and refine the Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP), ensuring they remain up-to-date and [illegible] Plans are [illegible] to system changes.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Risk Management

Risk management is a systematic process of identifying, assessing, prioritising, and mitigating risks to an organisation's objectives. A risk management framework provides a structured approach to understanding, evaluating, and addressing potential threats, allowing the organisation to proactively protect information assets and support overall business objectives.

This section reviews the organisations approach to managing risk and its understanding and ability to prioritise protection of business assets.

ID	Question	Importance	Answer Received	AUCloud Recommendation
[illegible]	The organization regularly conducts risk assessments to identify cyber security vulnerabilities and threats that are relevant to the organization and the industry it conducts business in.	Regular risk assessments are essential for developing a understanding of the organization's risk profile and formulating cohesive actions and responsibilities.	[illegible]	Consider adjusting the frequency for conducting assessments as business and security roles can quickly evolve. Risk assessments and reviews are recommended to be conducted quarterly or more frequent if necessary. The risks identified from these assessments should be formulated with the risk owner and where appropriate raised with the executive for awareness and prioritisation.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Statement	Importance	Assessor Perception	AUC Recommendation
MM2	The organization has adopted a risk management framework and developed a risk management plan.	The adoption of a risk management framework and the development of a risk management plan are crucial for identifying, assessing, and mitigating risks, aligning security efforts with strategic goals, ensuring compliance, and effectively managing the organization's risk landscape.	A documented plan exists, and processes are mostly implemented.	Continue to implement the risk management plan. The plan should be fully operational to ensure the risk management framework is maintained. The organization could benefit from a higher level of executive engagement, either through the Executive Management Committee or the Risk Management Committee. This would also assist other programs such as DISP which require similar oversight.
MM3	Mission critical information and services that would cause significant disruption, if interrupted or lost, have been identified and mechanisms put in place to protect them.	Identifying and protecting mission critical information and services is fundamental for business continuity, data security, risk management, and maintaining stakeholder trust.	Established but not formally documented	Formally document a Business Impact Assessment (BIA). This allows mission critical information and services to be defined and agreed. The BIA should be used to inform priorities for business continuity and decisions around risk management.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Question	Importance	Answer Provided	AUC Cloud Recommendation
WM4	The organization maintains an inventory of all hardware and software assets.	Maintaining an inventory of all hardware and software assets is crucial for efficient resource management, cost control, security, compliance, and strategic planning.	No inventory or only partial inventory	Formally establish hardware and software inventory processes. These processes should include regularly updating the asset inventory and implementing responsible officer. While there are options to use tools to track assets, a spreadsheet is sufficient as starting point. In order to establish the register it is recommended that an internal audit be conducted to gather the required information from relevant stakeholders.
WM5	There is clear ownership established for all assets, and responsibilities are specified.	Establishing a clear ownership structure for all assets and formalizing responsibility is essential for promoting accountability, efficient management, cost control, security, and compliance.	Clear and defined ownership structure	Continue to manage assets through maintaining a Software Register and Hardware Register. Ensure these are updated and revised where ownership changes.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Security Awareness

Security awareness is a proactive approach to building a resilient cyber security culture, reducing the likelihood of security incidents caused by human error, and developing a sense of responsibility across the organisation.

The security culture of an organisation is driven and championed by management and the security maturity of employees is influenced by their understanding of security risks and knowledge of best practices and organisational policy and procedures. Awareness is developed through education and training but also through practice.

This section reviews the organisation's processes and tools used to develop awareness amongst employees and management.

ID	Question	Importance	Answer Provided	AUCloud Recommendation
SAT	Employees receive cyber security training and awareness programs on a regular basis	Conducting regular cyber security training activities is vital for reducing risks, staying compliant, fostering a culture of security, and protecting the organisation's reputation.	When onboarded and annual training sessions	In addition to onboarding training and annual training, consider a combination of ongoing activities such as phishing tests, email reminders, short videos, and webinars. Also consider tailored training activities for privileged users and executives as these groups are higher value targets for threat actors.

SAMPLE

ID	Question	Importance	Answer Provided	AUCloud Recommendation
SA2	Simulated phishing exercises are conducted to evaluate the effectiveness of awareness programs.	Simulated phishing exercises are a valuable tool for assessing employee awareness and the organisation's maturity. They aid in improving the effectiveness of security awareness programs and promoting a culture of security.	Annually	Conduct regular phishing exercises to gauge employee awareness levels. Through regular phishing exercises, the organisation can establish a benchmark and identify areas of risk and topics which can feed back into awareness training. There are managed solutions for conducting phishing exercises and awareness training, but these can also be developed internally.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Question	Importance	Answer Provided	AUC Cloud Recommendation
1.11	Regular security scenarios or tabletop exercises are conducted across all levels of the business to test preparedness for cyber security incidents.	Regular security tabletop exercises are vital for assessing, improving, and testing an organisation's preparedness for cyber security incidents. They help identify weaknesses, enhance incident response capabilities, reduce risks, and ensure compliance.	Never	Conduct regular tabletop exercises that involve all security levels of teams and executives. Tabletop exercises are a crucial component and proactive approach to be prepared and provide the organisation and understanding of its duties in handling security incidents and addressing potential consequences. Tabletop exercises can be developed and run internally, or the expertise of a service provider can be used to simulate an externally directed event and allow all relevant stakeholders within the organisation to participate.

SAMPLE

ID	Question	Importance	Answer Provided	AUCloud Recommendation
[illegible]	The incident response team is well-prepared and trained to respond to cyber security incidents.	A well-prepared and trained incident response team is essential for minimising the impact of cyber security incidents and protecting sensitive data.	No incident response team	Consider the requirement for this capability and evaluate options of [illegible] employees, recruiting for the capability or using a managed service for dedicated monitoring and alerting. The incident response role/team requires specialist skills and access to security tools which will aid with detection and response. This capability ties into the organisations Incident Response Plan.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question/Area	Importance	Answer Provided	AUC Cloud Recommendation
1241	Guidelines for staff using their personal computers or mobile devices to access company systems and data are well documented and communicated.	Well-documented and communicated guidelines for using personal computers or mobile devices to access company systems and data are essential for ensuring security, data protection, compliance, legal liability, and overall risk management.	Yes but personal devices are unmanaged	Access the risks of unmanaged personal devices and evaluate the need of company data. Identify and classify the risk associated and provide guidance to update the organization's policy or set the requirement of a technical solution.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Access Control

Access control is fundamental in controlling access to systems and information. It is the key set of security controls which uphold the need-to-know principle and protects against unauthorised access. In addition, operation with a minimum and defined set of permissions reduces the risks when a system or user account is compromised.

This section reviews the processes for granting and removing access, use of administrator and privileged access and the ability to review and monitor access.

ID	Question	Importance	Answer Provided	AUCloud Recommendation
AC1	There are established and controlled processes for onboarding and offboarding employees.	Established and controlled processes for onboarding and offboarding employees is essential for maintaining data protection, compliance and access control.	Yes, both onboarding and offboarding	Continue to maintain onboarding and offboarding processes and adjust where necessary. Ensure records are kept which meet compliance and can be audited.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Questions	Importance	Answer Provided	AUCloud Recommendation
AC2	There are policies and controls in place to limit the number of staff that have admin permissions and privileged accounts.	Admin privileges generally provide the highest level of access across systems and can cause a high level of impact if compromised or abused. Policies and controls to limit permissions and privileged accounts is fundamental for protecting data, reducing risks and ensuring compliance.	Fully managed policies, procedures and lifecycle management implemented	Continues to maintain the policies, procedures and role account changes. To further improve cyber security, consider applying controls to limit the number of admin accounts across requirements to remain relevant.
AC3	The use of admin permissions across the environment is restricted.	Administrative permissions should be limited to perform their duties. Restricting the use of admin permissions is fundamental for data protection, risk mitigation, and ensuring compliance.	Strictly controlled and monitored use of admin accounts	Conduct regular audits to determine the relevant level of administrative permissions is required for each Administrator. Revise account permissions where roles change and where possible employ a just-in-time permissions model.
				Consider the implementation of a Privileged Access Management (PAM) solution to manage the account lifecycle.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Question	Importance	Answer Provided	AUCloud Recommendation
ACA	Access permissions to IT systems are reviewed on a regular basis or when staff members change positions.	Regular reviews of access permissions should be conducted to reflect changes in the business and are fundamental for maintaining access control, compliance, and data protection.	Not true as requested	Conduct regular audits to determine the ongoing need for privileged access. Revoke access permissions when staff change roles or when there is a change in a business requirement. Implement security monitoring use cases to address scenarios such as insider threat. Consider the implementation of a Privileged Access Management (PAM) solution to manage the account lifecycle.
ACB	There is a dedicated team that use monitoring tools such as SIEM or EDR to detect and respond to security events in real-time.	Having a dedicated team using monitoring tools for real-time security event detection and response enables early threat detection, rapid response, and protection of data and resources.	Full monitoring and response capability implemented	Continue to refine monitoring and response procedures with your managed service provider. Regularly review procedures and ensure tools are up to date. Where possible, conduct regular threat hunts based on known threat actors of concern or common attacks being exploited within the region.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Statement	Importance	Assessor Preferred	AUCloud Recommendation
ACS	The organisation has established processes in place to analyse and investigate security incidents.	Having established processes for analysing and investigating security incidents is crucial for incident resolution, threat understanding, root cause analysis, resource allocation, and organisational learning.	Informal / ad hoc investigative processes implemented	Develop formal processes for investigating security incidents. These should be documented and include guidelines for the Incident Response Team along with the Incident Response Plan. Review the technical capability of the team and consider specialised training where required. An alternative is to use a managed service which can provide or assist with this capability.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Patch Management

Patch management involves the process of planning, testing, deploying, and maintaining updates to operating systems, software applications, and firmware. The purpose of patch management is to address vulnerabilities in software that could be exploited by malicious actors to compromise the security and functionality of systems. It is important for organisations to implement effective patch management process to reduce its attack surface and reduce risks.

This section reviews the management of authorised software, the ability to identify and assess vulnerabilities and the ability to respond by deploying patches.

ID	Question	Importance	Answer Required	AUCloud Recommendation
PM5	Only trusted and supported operating systems and software are allowed to be used within the organisation?	Allowing only trusted and supported operating systems and software within the organisation is fundamental for maintainability, service support, reliability, and resource efficiency.	Policy controls in place.	Conduct auditing of operating systems and software to identify unauthorised installations. Report and identify risks. Consider implementing technical controls which will assist with alerting or controlling the installation of unapproved operating systems and software. Monitor vendor announcements for end of life/support messages so that appropriate planning can be conducted for significant version or release updates.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Question	Importance	Answer Provided	AUCloud Recommendation
PM[1]	The organisation has established formal procedures for reviewing and evaluating security patches and vulnerabilities on a regular basis.	Establishing formal procedures for reviewing patches and vulnerabilities is fundamental for security, data protection, compliance, vendor support, and resource efficiency.	Yes, a patch management policy and technical solution is implemented	Continue to assess vendor announcements and issue patching advice. Periodically review implementation and verify the successful application of patches.
PM[2]	The organisation has the ability to quickly deploy, install and validate critical security patches within 48 hours of them being released.	The ability to rapidly deploy, install, and validate critical security updates is important to safeguard an organisation's systems and data from potential cyber threats.	Answer not known	Continue to maintain policy and processes that will allow the organisation to sustain a 48-hour turnaround time for critical patches. If required, seek further executive support to prioritise security updates for critical vulnerabilities, or when it is known that vulnerabilities are being commonly exploited.

SAMPLE

1800 282 568
assurance@aucloud.com.au

[illegible]	Specialised software is used to ensure that software updates and patches are applied to IT systems and configured properly	Having specialised software or a dedicated capability optimises the patching process, reduces the risk of vulnerabilities, and contributes to the organisations patch management strategy	A technical solution is used to deploy updates and report on compliance levels	Continues to maintain the solution and provide oversight of patches which have errored and manage exceptions where required.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question/Area	Importance	Answer/ Provided	AUC Cloud Recommendation
[illegible]	Specialised software is used to regularly scan for vulnerabilities in IT systems and applications, especially those available on the internet.	Having specialised software to scan for vulnerabilities allows the organisation to identify vulnerable systems and gaps in patching and ultimately understand the areas/systems to focus on.	Weekly scanning with daily scans for external facing infrastructure	Continues to refine processes and reporting of vuln. Integrates vulnerability scanning capabilities with the patch management process. Develops dashboarding metrics for key systems and report to the [illegible] Management Committee on a regular basis.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Application Whitelisting

Application whitelisting is centred around having a defined and controlled set of applications and processes to review and authorise the installation of new software. The intent of application whitelisting is to permit only authorised software which has been assessed and approved for use within the organisation and reducing the risk of malicious and unknown software from executing.

This section reviews the organisation's ability to manage operating systems and software on endpoints and servers.

ID	Question	Importance	Answer Provided	Actions/ Recommendation
AWH	The organisation has implemented application whitelisting security measures and configurations.	When implemented and kept updated effectively, application whitelisting will prevent malicious software from executing. It is an important defence-in-depth security strategy.	No application whitelisting in place.	Consider implementing an application whitelisting solution. The solution should be tailored to the organisation's requirements and business operations. Application whitelisting should be applied on end-user systems (laptops and workstations) and servers to prevent the execution of malicious applications, particularly from the internet and to control the installation of unauthorised software.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question/Issue	Impact/Agency	Answer/ Threshold	AUC Cloud Recommendation/Action
AM01	A list of software and applications used by the organisation is reviewed and updated on a regular basis.	Maintaining an up-to-date register of software allows the organisation to control and maintain systems and the associated risks. This feeds into processes such as patch management and change control.	Rarely	Establish a Software Register and standard operating procedure which ensures that all software assets are identified and classified. An Asset Owner should be assigned to each asset or asset class. The software register should also be extended to include external services such as cloud-based applications.
AM03	Workstations/laptops and IT equipment are centrally managed to ensure secure and consistent deployments.	By maintaining centralised management of workstations and devices, the organisation can enhance the security, efficiency, and consistency of IT systems. This directly affects the reliability of internal systems and the user experience.	Centralised solution and deployment status regularly checked with missing deployments followed up on	Continue to maintain the centralised solution and check the deployment status of endpoints and investigate alerts. Ensure the process and solution captures provisioning of new endpoints.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question/Issue	Impact/Significance	Answer/ Procedural	AUC Cloud Recommendation/Solution
AM14	Servers (physical and virtual) are centrally managed to ensure secure and consistent deployments.	By implementing centralised management of the server fleet, the organisations will enhance the security, efficiency, and consistency of IT systems. For external facing systems, this directly affects the reliability of the systems for internal users, external users	Centralised solution and deployment status regularly checked with missing deployments followed up on	Continue to maintain the centralised solution and check the deployment status of servers and investigate any changes to the process and software captured. Monitoring of new updates and security hardening of servers as industry standards
AM15	Security measures have been implemented to protect against Microsoft Office macro exploits	Malicious macros, with the use of Office files commonly distributed through email and file transfers. These macros can execute harmful code when the files are opened. Controlling the use of macros reduces the risk of Office files being used in cyber attacks.	No specific policy	Assess the risk of malicious office macros being received/transferred to the organisation's systems. Consider implementing a macro security strategy using guidance from the ACSC. There are five documented strategies, each with varying levels of effectiveness and restrictions. Business use cases should be considered when selecting a strategy

SAMPLE

1800 282 568
assurance@aucloud.com.au

Network Security

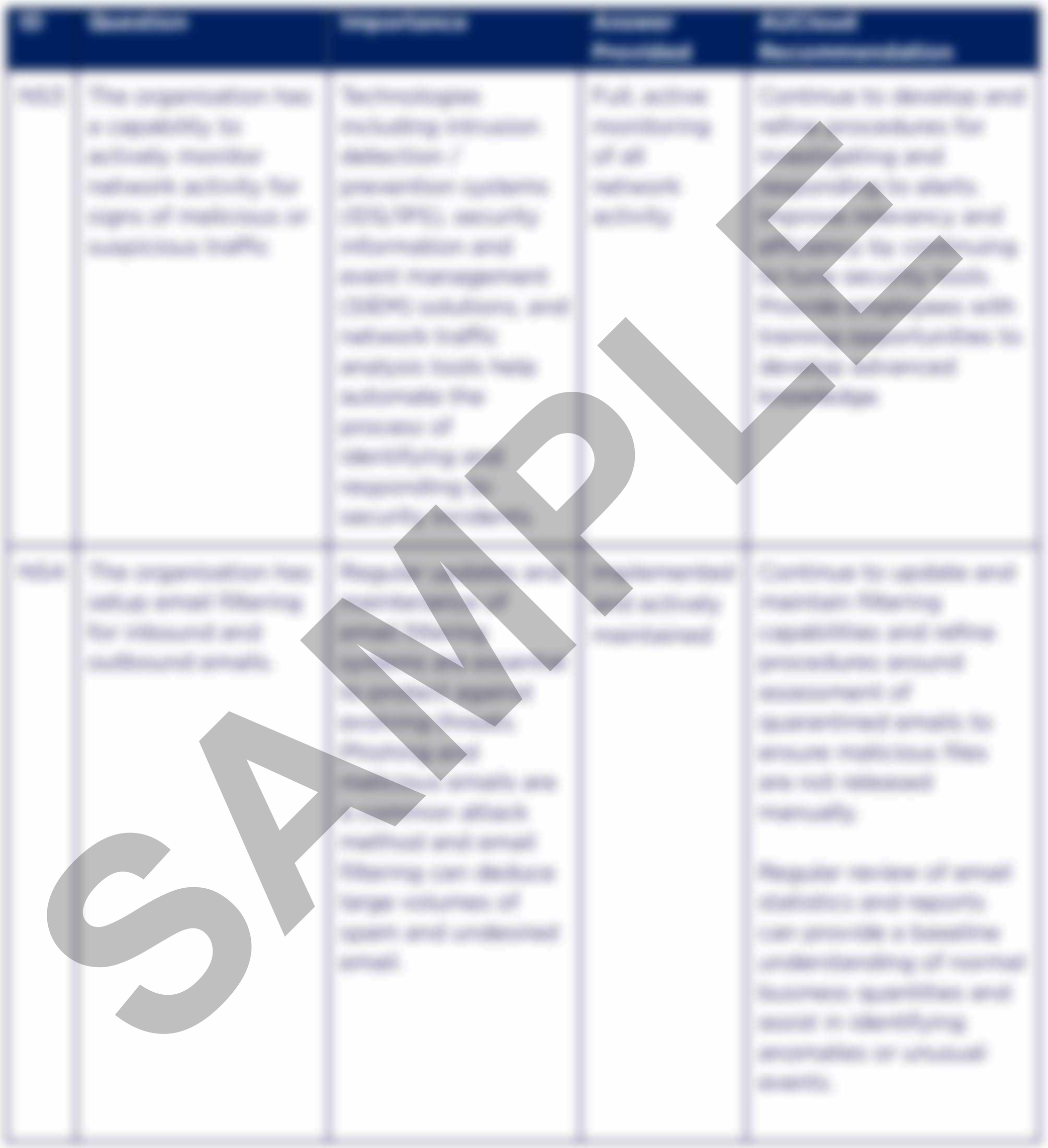
Network security provides an organisation with perimeter controls and security for the transmission of data as it passes to systems and endpoints. The implementation of technical controls and solutions can reduce the risk of unauthorised access to the network and systems.

This section reviews the organisation's technical capabilities in place to secure the network and systems.

ID	Question	Importance	Answer Provided	Actions Recommended
NS1	The organisation has implemented firewalls and intrusion detection/prevention systems across the IT environment to prevent cyber attacks.	The implementation of firewalls and intrusion detection/prevention systems helps to safeguard the organisation's IT environment against cyber attacks and unauthorised access.	All of these implemented and updated regularly	Continue to maintain these capabilities and ensure that updates and patches are applied. Continue monitoring and alerting.
NS2	The organisation has implemented an anti-virus or endpoint security as an application that stops and removes malware protection.	Implementing anti-virus and endpoint security solutions is a fundamental step in protecting the organisation's digital assets and data. Endpoint security is most effective on internet facing systems and devices and systems where data transfers are conducted.	Active protection on all endpoints	Continue to develop and refine procedures for investigating and responding to alerts. This should include working with a managed service provider or training IT staff on how to isolate and remove malicious files where the security tool is unable to do so. Where possible, response actions should be automated and enforced to provide the maximum level of protection.

SAMPLE

1800 282 568
assurance@aucloud.com.au



SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question	Impact/Agency	Answer/ Response	AUC Value Recommendation
NSS-1	A policy and procedure are in place that prevent or limit the use of external devices such USBs and hard drives.	USB devices can be used to store and transfer large amounts of data. Policies and procedures that restrict or control the use of external devices like USBs and hard drives are crucial for protecting the organisation's data, networks and systems from security threats, data breaches, and compliance violations.	Not Implemented	Review the business requirement and user needs for the use of USB devices within the organisation. Evaluate the risks associated with USB devices, including data loss, malware infections, and unauthorised access. Develop and implement a policy and controls which restrict the use or limit access to USB and devices. Ensure these controls cannot be implemented, consider alternate controls which include monitoring and logging of transactions and ensure devices are scanned before execution.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question	Implementation	Assessed Procedural	Audit Issue / Recommendation
NS8	Technical controls are in place that prevent large volumes of data being sent externally	Implementing technical controls to prevent the excessive external transfer of large volumes of data is crucial for data protection, compliance, and risk mitigation. These controls help the organisation maintain data security, prevent data breaches, and reduce the potential for unauthorised data sharing.	Implemented and actively maintained	Continue to monitor and ensure transactions are logged and regularly reviewed. Where deployed, review policy and procedures in line with new business requirements. Where encryption keys are used, ensure that these are managed and removed when no longer required.
NS27	The organisation uses content filters to restrict access to websites that may be malicious, suspicious, or inappropriate for the workplace.	Blocking access to potentially harmful or inappropriate websites is essential for enhancing security, productivity, and compliance. Content filters also assist in maintaining a safe working environment.	Implemented and actively maintained	Continue to review content filter categories to ensure they align with the organisation's policies. Review processes for managing exceptions.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question	Importance	Answer Provided	AUCloud Recommendation
MSR	The organisation has the ability to carry out threat hunting using indicators of compromise in the event of a suspected cyber attack.	The ability to carry out threat hunting in the event of a suspected cyber-attack is essential for early threat detection, and rapid incident response. It plays a crucial role in minimising the impact of cyber-attacks and protecting sensitive data and critical systems.	Ability to threat hunt, but not utilised	Review the ability to exercise threat hunting and consider developing this capability as part of the organisation's incident response capability. When working with a managed service provider ensure that threat hunts are scheduled to occur regularly.
MSR	The company regularly monitors the dark web for any indication of compromised accounts or data.	Dark web monitoring can reveal indications of compromise such as stolen credentials and insider threats. It is a crucial step in detection, containment and forms a linkage between incident detection and response.	Active monitoring. Dark Web monitoring capability implement ed	Continue to refine processes for how suspected compromises are investigated and handled. This should include defining the source and method of compromise so remediation tasks can be implemented.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Data Protection

Data protection refers to the practices, policies, and technologies uses to safeguard information. The purpose of data protection is to ensure the confidentiality, integrity, and availability of data, while also addressing privacy concerns and complying with relevant regulations. The threats to an organisation include cyber-attacks, data breaches, and accidental or intentional misuse.

This section reviews the controls the organisation has implemented to secure data in transit and at rest and the ability to maintain and restore from backups.

ID	Question	Importance	Answer Provided	AUCloud Recommendation
DP1	There is a well-documented data retention and disposal policy that defines the criteria and length of time to retain data.	A well-documented data retention and disposal policy is a fundamental aspect of data management, ensuring compliance with regulations, optimising storage, and safeguarding sensitive information. It helps the organisation protect data, and reduce potential liabilities associated with data mishandling.	Not policy in place	Identify assets and data stores to develop a policy that is relevant to the organisation's activities. Data retention should align to legal requirements and contractual requirements with Customers and Partners. Technical settings for logging and archiving should be configured to align with the retention requirements in policy. Users should be made aware of the policy and adhere to the retention requirements and processes for asset disposal.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question	Importance	Acceptable Procedural	AUC Cloud Recommendation
[XP1]	The organisation has implemented regular backup processes to ensure that copies of important or sensitive information is protected.	Regular backup processes are a fundamental aspect of data protection, disaster recovery, and business continuity. They ensure that essential and sensitive information is safeguarded against various threats and can be readily restored when needed.	Fully automated backups are conducted to offsite or cloud services	Continue to review backup requirements and ensure new systems are configured with an appropriate backup solution and schedule.
[XP2]	Processes have been implemented to regularly backup cloud-based systems (SaaS) that contain sensitive customer, company or employee information.	Implementing processes to regularly back up cloud-based systems is essential for data protection, compliance, disaster recovery, and business continuity. It ensures the organisation can recover, protect, and manage their sensitive information effectively.	Fully automated backups are conducted to offsite or cloud services	Continue to review backup requirements and ensure new systems are configured with an appropriate backup solution and schedule.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question	Importance	Example Provided	AUC Cloud Recommendation
[ID]	The organisation frequently tests the integrity of backup solutions to ensure data can be recovered in the event of a cyber attack.	Regular testing of backup solutions is essential for data recovery assurance, business continuity, and effective response to cyber attacks. Recovery tests provide assurance that backup solutions are functioning as expected and that critical data can be successfully recovered when required.	Backup procedures and tests are documented and are tested annually	Continue to maintain backup systems and procedures. Regularly perform and document backup and recovery tests.
[ID]	The organisation has implemented data encryption solutions.	Implementing data encryption solutions is a critical step in protecting sensitive data. This includes data at rest and data in transit. Data encryption can reduce the impact of unauthorised access and compromised systems or network traffic.	Both in transit and at rest	Continue to ensure that new systems are designed and configured with an adequate level of encryption for data in transit and at rest. This should also be a consideration when selecting cloud based applications.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Multi-Factor Authentication

The use of unique complex passwords is a fundamental control in securing against unauthorised access to system. The use of Multi-Factor Authentication (MFA) is a control which strengthens the authentication process and is an effective control against attacks where a primary user account password has been compromised.

This section reviews the organisation's authentication policy and controls.

ID	Question	Importance	Answer Provided	AUCloud Recommendation
MF1	The organisation has implemented multi-factor authentication for all critical applications.	Implementing multi-factor authentication for critical applications is a fundamental security measure that enhances the protection of sensitive data, and reduces the risk of unauthorised access, where the primary authentication credentials are compromised.	[redacted]	Continue to ensure that new systems are designed and configured with multi-factor authentication enforced as a default security control.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question	Importance	Answer Provided	AUCloud Recommendation
1.1.1	The organisation has implemented multi-factor authentication for all cloud-based systems that include sensitive customer, company or employee information.	Implementing multi-factor authentication for cloud systems is a fundamental security measure that enhances access control, protects sensitive data, and reduces the risk of unauthorised access where the primary authentication credentials are compromised.	Fully implemented for all users and systems	Continue to apply this requirement when considering new cloud-based services. Review this risk and associated controls when the cloud service undergoes significant changes.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Question	Importance	Answer Provided	AUCloud Recommendation
MFA	Complex passwords are enforced, as well as encouraging the use of password managers.	Enforcing complex passwords and encouraging the use of password managers are fundamental steps in protecting user accounts and mitigating the risk of unauthorised access and data breaches.	Password manager implemented and enforced with strong password requirements.	Continue to enforce the use of the password manager for employees. Where possible, also implement multi-factor authentication to increase password security.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Question	Importance	Answer Provided	AUCloud Recommendation
IAM 4	Unique and complex passwords are used for privileged accounts such as local administrator, system and service accounts.	Using unique and complex passwords for privileged accounts is a fundamental security practice that helps protect critical systems and data and reduces the risk of unauthorised access. Reuse of credentials across a compromised	A policy is in place and a technical solution has been implemented to enforce	Centrally manage the use of complex passwords across privileged accounts. Where possible, use technical controls to ensure privileged accounts should also be reset if triggered by events such as an administrator offboarding or suspected security incidents.

SAMPLE

1800 282 568
assurance@aucloud.com.au

Incident Response

An organisation's incident response capability will determine its preparedness in detecting, containing and responding to security incidents. This includes having the technical capability and expertise to handle and recover from incidents but more importantly a rehearsed and tested whole of organisation plan which determines the processes and priorities.

This section reviews the organisation's preparedness to handle security events and incidents.

ID	Question	Importance	Answer / Response	AUCloud Recommendation
49	The organisation has a well-developed incident response plan that is tested frequently	A well-developed incident response plan that is tested frequently helps the organisation respond effectively to security incidents, reduce damage, and ensure compliance with legal and regulatory requirements.	Not given in place	Develop an Incident Response Plan which is tailored to the organisation's needs. As a starting point, review available industry resources which include templates and guidance on the aspects to be covered in the IRP. The IRP should be developed with the support and input of the executive and business stakeholders. Testing of the IRP should be conducted to ensure it can be executed relevant and comprehensive.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question	Importance	Answer Provided	AUCloud Recommendation
#42	The organisation has the ability to quickly respond to and contain cyber security incidents when they occur	The ability to quickly respond to and contain cyber security incidents is a critical component of an effective cybersecurity strategy. It helps protect data, systems, and the organisation's reputation. A delayed and uncoordinated response can result in more significant impacts and damage.	Rapid response, swift containment, and recovery	Response capabilities should be documented with consistent response processes. Continual training, drills, and simulations to keep teams prepared for real threats and techniques through training and experience.
#43	There are formal processes in place to notify customers and authorities if there has been a data breach.	Responding and handling of data breach is a critical element of organisations data management and incident response. It helps the organisations meet legal obligations, protect individuals, and maintain trust with customers and stakeholders.	Informal process in place	Identify external parties and legal obligations for notifying of data breaches. Develop a formal process which defines the organisation's approach and assigned roles and responsibilities. This process should be incorporated into the Incident Response Plan or be referred to if maintained as a separate document.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Question/Area	Importance	Answer/ Provided	AUC Cloud Recommendation
864	In the event of a cyber attack, the organisation understands its legal position and risk.	Understanding the legal position and risks in the event of a cyber attack is essential for protecting against liability, and effectively managing the aftermath of the attack. It helps the organisation make informed decisions and minimise the consequences	Fully understands legal risk and obligations	Regularly review obligations and ensure cyber security [illegible] and [illegible] compliance. The incident response plan should include communication and reporting requirements as part of handling a security incident.

SAMPLE

1800 282 568
assurance@aucloud.com.au

ID	Assessment Statement	Importance	Assessor Perception	AUC Cloud Recommendation
#45	The organization is fully aware of regulatory obligations with relation to cyber security	Being fully aware of regulatory obligations with respect to cyber security is a foundational aspect of risk management and legal compliance. It ensures that the organization can protect sensitive data, meet legal requirements, and maintain the trust of customers and stakeholders.	Fully understands legal risk and obligations	Regularly review obligations and ensure cyber security responsibilities are addressed in both contracts and supplier contracts. The incident response plan should include communication and reporting requirements as part of handling a security incident.
#46	Lessons learned from security incidents are used to improve cyber security practices	Conducting lessons learned after a security incident enables the organization to learn from mistakes, improve processes and adapt their security measures to address evolving threats and vulnerabilities.	Lessons learned conducted after every incident	Continue to conduct tabletop exercises and use lessons learned to improve the respective areas of the business relating to people, process and technology

SAMPLE

1800 282 568
assurance@aucloud.com.au

Disclaimer

This report is intended for the Customer's internal use only. The report should be used as a guide and should not solely be relied upon for decision making.

This report does not constitute a formal security audit or certification assessment.

This report has been produced by AUCloud using information shared by the Customer and its representatives. The accuracy of the information has not been verified and is based on responses provided in a question and answer interview without sampling evidence or verifying controls.

SAMPLE

1800 282 568
assurance@aucloud.com.au

About AUCloud

AUCloud (ASX:SOV) is an Australian owned and operated Managed Security Service Provider (MSSP) and Sovereign Cloud Specialist supporting Australian Governments and Critical National Industries (CNIs) with the latest sovereign cloud infrastructure, backup and cyber security threat defence, monitoring and response services.

Canberra
Unit 7, 15-21 Beaconsfield Street
Fyshwick ACT 2609

Sydney
Level 14, 175 Pitt Street
Sydney NSW 2000

Melbourne
Level 6, 24-28 Collins Street
Melbourne VIC 3000

Brisbane
Level 7, 324 Queen Street
Brisbane QLD 4000

Contact an AUCloud cyber security specialist today:
1800 282 568
assurance@aucloud.com.au

SAMPLE