AUCYBER

CYBER SECURITY MATURITY ASSESSMENT

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

1800 282 568
assurance@aucyber.com.au

Table of Contents

1800 282 568
assurance@aucyber.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 AUCyber 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, AUCyber 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. [redacted]

[redacted]

1800 282 568
assurance@aucyber.com.au

From the AUCyber Head of Cyber Security

[redacted]

Regards,

[redacted]
Head of Cyber Security
AUCyber

1800 282 568
assurance@aucyber.com.au

Executive Summary

[redacted]

1800 282 568
assurance@aucyber.com.au

[redacted]

1800 282 568
assurance@aucyber.com.au

Assessment Process

[redacted]

[redacted]

[redacted]

[redacted]

Name	Role
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

Key Recommendations

This section details the key recommendations. These are the recommendations which AUCyber 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

[redacted]

1800 282 568
assurance@aucyber.com.au

Recommendation 2:
Consider Implementing Application Whitelisting Controls

[redacted]

Recommendation 3:
Consider Implementing a Microsoft Office Macro Security Strategy

[redacted]

1800 282 568
assurance@aucyber.com.au

[redacted]

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

[redacted]

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

[redacted]

1800 282 568
assurance@aucyber.com.au

[redacted]

1800 282 568
assurance@aucyber.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

1800 282 568
assurance@aucyber.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	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.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 Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.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	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.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	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.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.

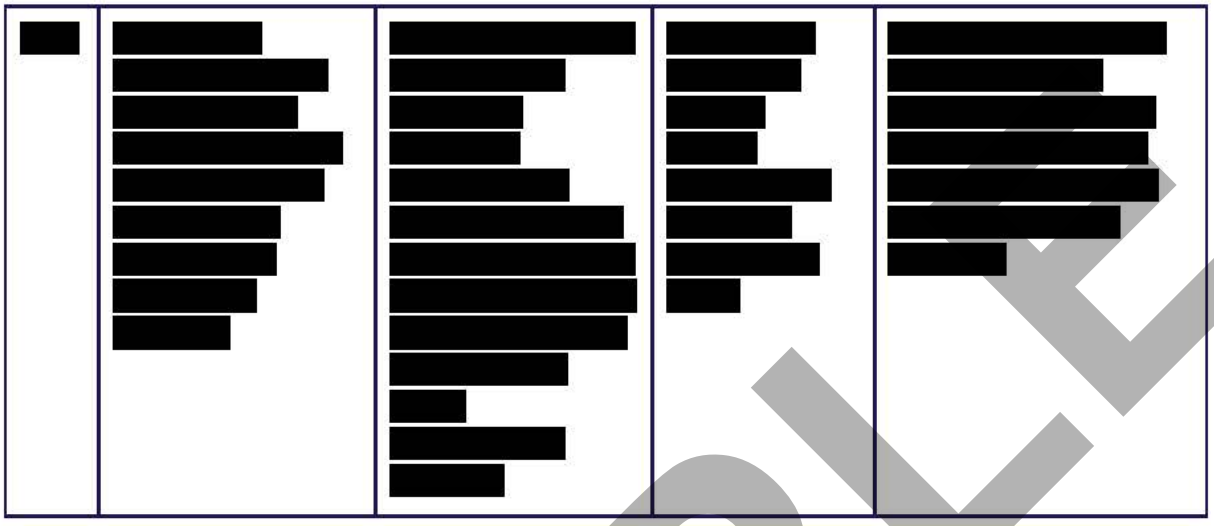
This section reviews the management of authorised software, the ability to identify and assess vulnerabilities and the ability to respond by deploying patches.

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au



1800 282 568
assurance@aucyber.com.au

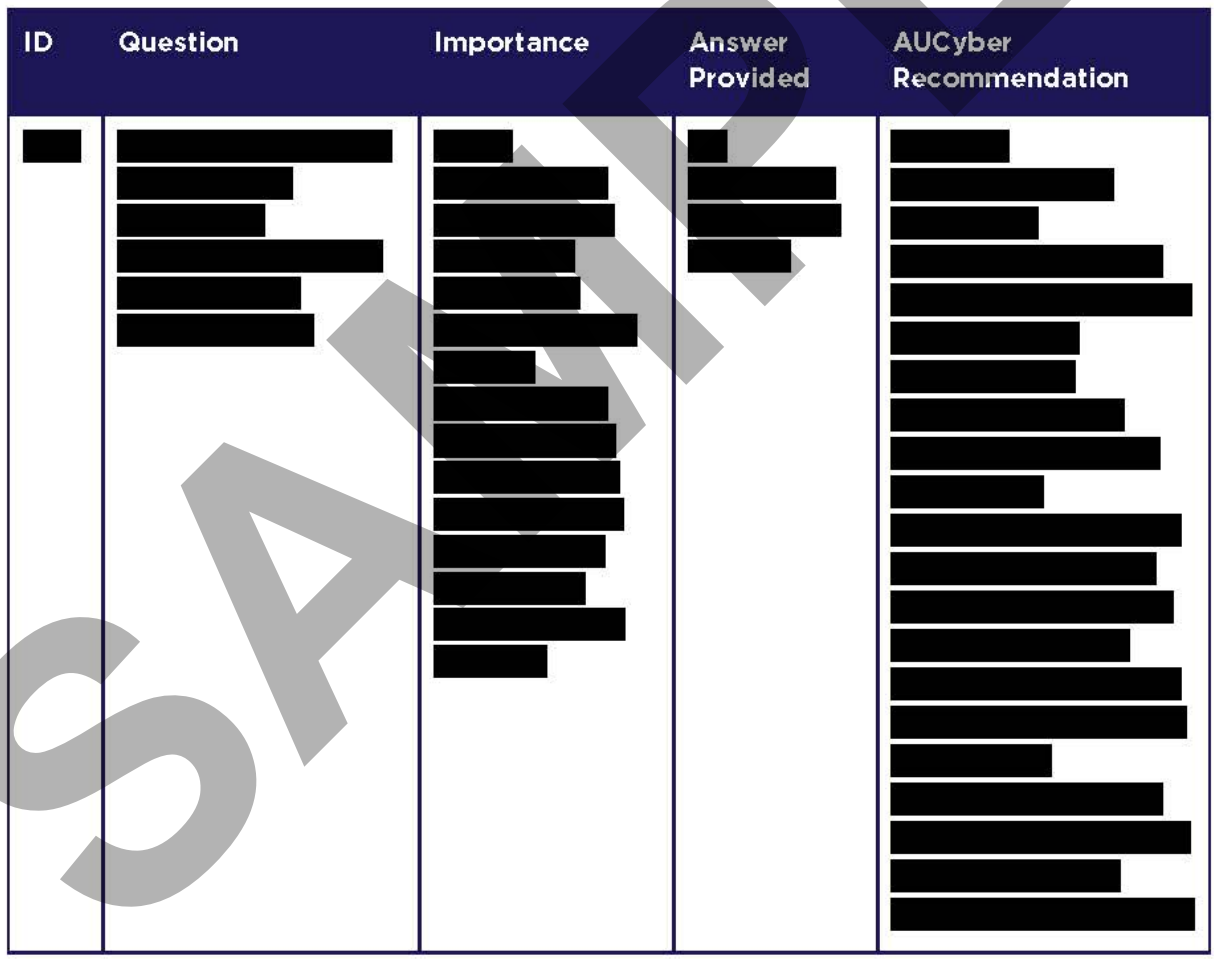
ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.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.



1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.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	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.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	AUCyber 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, regulatory compliance, risk mitigation, and responsible data governance. It helps the organisation protect data, and reduce potential liabilities associated with data mishandling.	No 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.

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
DP2	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 maintain backups in line with the organisation's archival and retention requirements defined in policy. Regularly test the restoration of backups to ensure accessibility and completeness of records
DP3	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 system 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.

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.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	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.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 Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

ID	Question	Importance	Answer Provided	AUCyber Recommendation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1800 282 568
assurance@aucyber.com.au

Disclaimer

[redacted]

About AUCyber

AUCyber (ASX:CYB) 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.

Contact an AUCyber cyber security specialist today:
1800 282 568
assurance@aucyber.com.au