

<Client Name>

Security Gap Assessment Report

Dd Month yyyy
v1.0

Presented by



P: 1300 794 777

E: info@whiterookcyber.com.au

W: whiterookcyber.com.au



Document Control

Document Identification

File Name	WRC-[REDACTED]-Security Gap Assessment Report
Version	1.0

Document Contributors

Name	Role	Phone Number	Email Address

Revision History

Version	Date Released	Author	Changes
0.1 0.2	dd Month yyyy		Initial draft
0.3 1.0	dd Month yyyy		Technical QA
	dd Month yyyy		Presentation QA
	dd Month yyyy		First release

Document Distribution

Name	Company	Date	Version
		dd Month yyyy	1.0

Table of Contents

Executive summary	4
Background	4
Summary of findings	4
Summary of key recommendations.....	5
General observations.....	6
Introduction	7
Background	7
Scope of Assessment	7
Limitations	7
Overview of Essential Eight Maturity	8
Essential Eight Maturity Model and Target Maturity Level	8
Assessed Essential Eight Maturity by Mitigation Strategy	8
Patch Applications and Operating Systems	9
Multi-factor Authentication	9
Restrict Administrative Privileges	9
Application Control	10
Restrict Microsoft Office Macros	10
User Application Hardening	10
Regular Backups	11
Overview of Cyber Security Governance and Operations	12
Privacy Legislative Compliance	12
Risk Management	12
Audit Program and/or Security Calendar	12
Awareness and Training	12
Incident Response Planning	12
Overview of Security Architecture	13
Microsoft Office 365 CIS Audit	13
Microsoft Azure CIS Audit	14
Security Architecture Domains	14
Appendix A Essential Eight Maturity Model (November 2023)	18
Appendix B CIS Microsoft 365 Foundations Benchmark v3.0.0 (09-29-23)	19
Appendix C Detailed recommendations for Essential Eight	20
Appendix D Detailed recommendations for Security Architecture	23
Appendix E Documents Reviewed	32
Appendix F Essential Eight Maturity Assessment workbook	33
Appendix G Office 365 CIS control audit	34
Appendix I Azure CIS controls	43



Executive summary

Background

[REDACTED] and [REDACTED] is with products sold in more than 100 countries worldwide. Founded [REDACTED] three [REDACTED] core business is divided between proprietary, licensed and distributed brands.

[REDACTED] has recognised the need to assess the current state of cyber security across its various environments within the [REDACTED] in regions in which the [REDACTED] corporate offices are situated.

The objective of this current state assessment is to assist in understanding alignment and adherence of the business to industry security best practices against the selected cyber security framework. This security gap assessment was conducted against ASD's Essential Eight Maturity Model, CIS Office 365, and general Security Architecture best practice. It combined a security architectural review, testing of its security controls and technical environments to identify vulnerabilities and risks within the various IT environments within scope.

The report provides a summary of findings and recommendations for improving the security posture of [REDACTED] by identifying potential security gaps, vulnerabilities and risks to its assets, data and infrastructure. Ultimately informing a program of remediation work to uplift its cyber security and governance operations, a part of its ongoing security maturity planning.

Summary of findings

All mitigation strategies within the Essential Eight were assessed, with varying degrees of maturity observed against each strategy. [REDACTED] is assessed as having an overall maturity level of zero (0) against the Essential Eight mitigation strategies. Table 1 below shows each mitigation strategy as assessed against the Essential Eight Maturity Model¹ published in November 2023 (refer to Appendix A) and the recommended maturity level.

Essential Eight Mitigation Strategy	Assessed Maturity Level	Recommended Maturity Level
Patch applications	0	1
Patch operating systems	0	1
Multi-factor authentication	0	2
Restrict administrative privileges	0	1
Application control	0	1
Restrict Microsoft Office macros	0	1
User application hardening	0	1
Regular backups	0	1

Table 1 - Essential Eight – assessed and recommended maturity levels

¹ <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model>

An Office 365 Audit for ██████ > tenancy was conducted against the industry hardening standard, “CIS Microsoft 365 Foundations Benchmark”, v3.0.0 (09-29-23) (refer to Appendix B). The tenancy audited against this standard was noted to be relatively old. More modern tenancies have a different baseline level of security control configurations. Due to the age of the tenancy, the findings are reasonable, but uplift and alignment with best practice is recommended. Table 2 below shows the summary of CIS Control compliance.





CIS Control compliance summary	Total
 Control in place	16
 Control not, partially in place, and/or periodic	62
 Validate, further investigation needed	27
 Periodic, operational calendar task required	11

Table 2 – CIS Control compliance summary

Summary of key recommendations

A number of themes for improvement were identified during the assessment, which if addressed will further enhance the overall cyber security operations at ██████.

There are thirty-three (33) recommendations identified that would raise the Essential Eight maturity level to the target maturity level across each of the eight mitigation strategies (refer to Appendix C), if implemented.

Many of the recommendations are minor and minimal effort would be required to implement the technical control; however, there are several more complex changes that would require additional funding, planning and cultural change to implement effectively.

Security domains were analysed against ██████ current architecture, including WAN-connected and service provider assets with detailed findings included in Appendix D.

Table 3 highlights the identified themes in the recommendations.

Theme	Recommendation
Policies, procedures, standards and guidelines	The findings show that policies and procedure documents to support Essential Eight mitigation strategies do not exist. Development of policies and procedures for controls and areas that don't have formalised documentation is recommended. The policies and procedures should be developed to a level commensurate with the size and low complexity of ██████ > technology environment. The policies and procedures should be communicated to and be available to all staff.
Approach to cyber security	Develop a standard approach to cyber security for all jurisdictions, with bespoke policies and practices developed by exception only.
Access control	Remove local admin privileges for all users who do not have a role-based requirement to have those privileges so that security configurations cannot be changed. Implement multi-factor authentication for all systems and users.



Theme	Recommendation
Workstation environment	Implement a Standard Operating Environment (SOE) for workstations, with consideration to all Essential Eight mitigation strategies, including a solution to allow remote access and control to all endpoints.
Cyber Strategy/Program	To support an effective IT strategy, a Cyber Security Program should be established to address all recommendations. This will support the formalisation and agreement of the cyber security roadmap for [REDACTED]. The Program should develop a formal communication and change plan, including training, communication of related policies/standards and procedures, roles, and responsibilities across [REDACTED] and expected performance standards as part of the overall information security posture.
Incident response, business continuity and disaster recovery	Incident response and business continuity should be addressed to prepare <client> for any future incidents that may arise. Standalone Incident Response Procedure and Business Continuity Plans (supported by Backup and Recovery Procedures for each system) should be developed. Testing of the incident response procedures, business continuity and disaster recovery plans should occur at least annually. This should include testing of Notifiable Data Breach procedures as a subset of incident response testing. Develop a Risk Management Framework, inclusive of risk appetite
Risk Management	and risk assessment procedures to be applied globally. The overall risks to the organisation should be identified strategically, and operationally for every department, even if it is not Technology related.
Security Architecture	The findings show that improvements to Security Architecture controls is required. This should be incorporated into the Security Strategy/Program with priority given to the remote VPN, firewall management, and implementation of Essential 8 MFA mitigation strategy maturity level 2.

Table 3 – Key themes and recommendations for improvement

General observations

During the assessment, we identified several positive management points and processes that contribute to the capability of [REDACTED] to effectively manage cyber security and governance operations. These included the following:

- Commitment to developing a roadmap to uplift cyber security and governance operations.
- Annual legal review and uplift of privacy policies and practices for each jurisdiction.

Introduction

Background

[REDACTED] is a global producer and distributor specialising in [REDACTED] and [REDACTED] with products sold in more than 100 countries worldwide. Founded in [REDACTED] [REDACTED] core business is divided between proprietary, licensed and distributed brands.

[REDACTED] has recognised the need to assess the current state of cyber security to inform a program of work to uplift its security and governance operations.

Scope of Assessment

The scope of the assessment was to conduct a maturity assessment against the Australian Signals Directorate's (ASD) Essential Eight mitigation strategies and Security Architecture review for [REDACTED] operations in [REDACTED]. The assessment considered the following information assets:

- Microsoft Office 365.
- LAN/WAN and Network Infrastructure.
- Internet-facing services.
- Managed Service Providers.
- [REDACTED] – separate instances and databases for each jurisdiction.
- Supporting applications.

The Microsoft Azure platform is used minimally but has configuration in place. It was not assessed, but configuration guidance has been provided.

Microsoft Office 365 was investigated using the “Global Reader” role, and direct findings are included within this report.

Limitations

The assessment was conducted remotely, with participants joining meetings online and utilising screen sharing to review and verify relevant information or through direct access to the relevant documents and systems. This report is based on information (documents, demonstrations, and interviews) provided at the time of the assessment. Any new documentation or implementation of technical controls since the conduct of the assessment are not included and may alter the recommendations. A list of documents reviewed is included in Appendix E.





Overview of Essential Eight Maturity

Essential Eight Maturity Model and Target Maturity Level

The Essential Eight has been designed to protect an organisation’s internet-connected information technology networks. ASD recommends organisations identify and plan for a target maturity level suitable for their environment and to then progressively implement each maturity level until that target is achieved, with implementation using a risk-based approach. Exceptions should be minimised, and if used, they should be documented, approved and monitored.²

Based on existing maturity, it is recommended that [redacted] target Maturity Level One for all mitigation strategies, with the exception of multi-factor authentication, which should target Maturity Level Two.

Assessed Essential Eight Maturity by Mitigation Strategy

While all mitigation strategies were overall assessed to be at Maturity Level Zero, progress toward the target maturity level varied. Detailed recommendations to uplift maturity are outlined in Appendix C.

The eight (8) mitigation strategies each have a differing number of requirements to meet the target maturity level. Figure 1 below shows the number of individual requirements to meet the target maturity for each mitigation strategy, alongside the requirements assessed as being met.

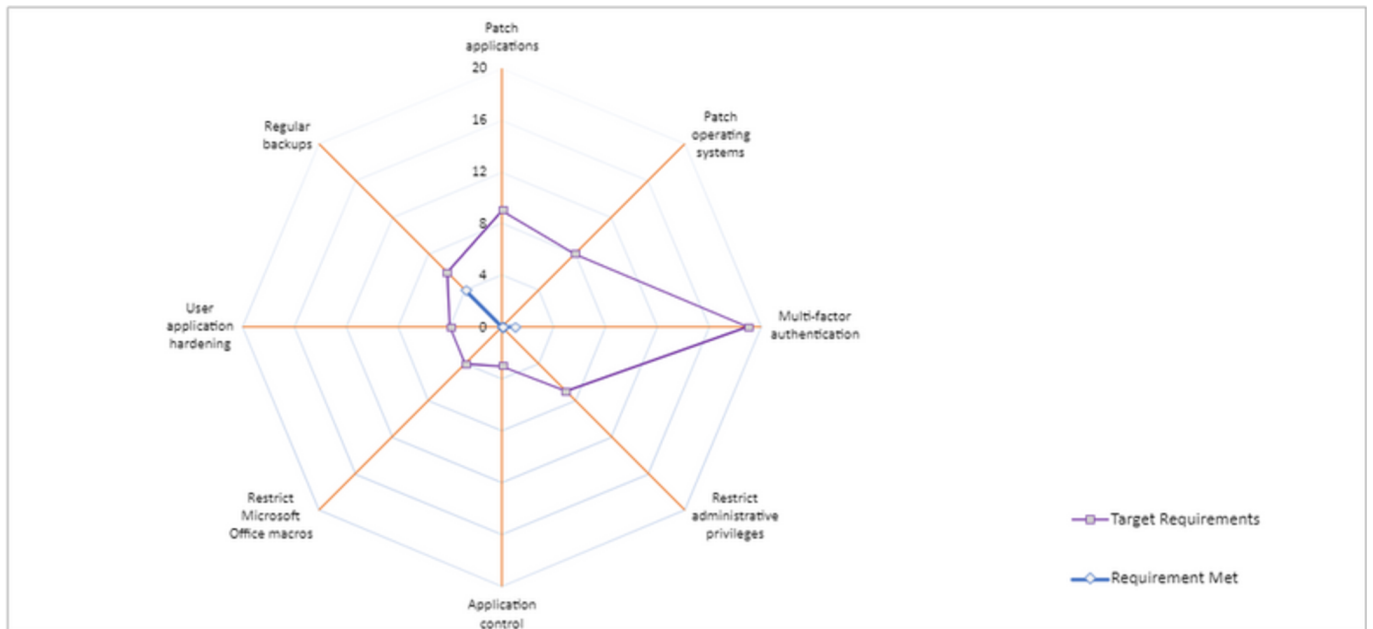


Figure 1 – Essential Eight maturity by requirements within each mitigation strategy

The Essential Eight Maturity Assessment workbook is in Appendix F.

² <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model>

Patch Applications and Operating Systems

Applying patches to applications and operating systems is critical to ensuring the security of systems. Of

the nine (9) requirements to meet Maturity Level One for Patching applications, none were met. This was primarily due to inconsistent patching practices across different applications and adherence to the time constraints of Maturity Level One.

Of the eight (8) requirements to meet Maturity Level One for Patching operating systems, none were met. This was again primarily due to inconsistent patching practices across different systems and adherence to the time constraints of Maturity Level One.

By maintaining clear and streamlined patch management processes and procedures organisations can position themselves to act swiftly upon vulnerability announcements and patch releases. Guidance on patching considerations, and implementation in different contexts is provided in ASD's '*Patching Applications and Operating Systems*'.³

Multi-factor Authentication

Multi-factor authentication is one of the most effective controls an organisation can implement to prevent malicious actors from gaining access to online services, systems or data repositories and accessing sensitive data. When implemented correctly, multi-factor authentication can also make it more difficult for malicious actors to steal legitimate credentials to facilitate further malicious activities.

At Maturity Level Two, this mitigation strategy also includes consideration of log monitoring, event analysis, incident response and reporting of cyber security incidents to ASD as soon as possible after they occur or are discovered. This requirement would not be applicable to cyber security incidents that are wholly contained to operations in the US or Europe.

Of the seven (7) requirements to meet Maturity Level One, one was met. Of the twelve (12) requirements to meet Maturity Level Two, none were met. This was primarily due to incomplete view of MFA capable systems.

Multi-factor authentication is defined as 'a method of authentication that uses two or more authentication factors to authenticate a single claimant to a single authentication verifier'. Guidance on the implementation options is provided in ASD's '*Implementing multi-factor authentication*'.⁴

Restrict Administrative Privileges

Users with administrative privileges for operating systems and applications are able to make significant changes to their configuration and operation, bypass critical security settings and access sensitive data. Domain administrators have similar abilities for an entire network domain, which usually includes all of the workstations and servers on the network.

Malicious actors often use malicious code (also known as malware) to exploit vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for malicious actors to elevate privileges, spread to other hosts, hide their existence, persist after reboot, obtain sensitive data or resist removal efforts.

³ <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-administration/patching-applications-and-operating-systems>

⁴ <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication>

Of the seven (7) requirements to meet Maturity Level One, none were met. This was primarily due to requirements not being implemented.

There are a number of approaches which, while they may appear to provide many of the benefits of restricting administrative privileges, do not meet the intent of this mitigation strategy. Guidance on the approaches to implement is provided in ASD's *'Restricting Administrative Privileges'*.⁵

Application Control

Application control is a security approach designed to protect against malicious code (also known as malware) executing on systems. When implemented robustly, it ensures that only approved applications (e.g. executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers) can be executed.

While application control is primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unapproved applications.

Of the three (3) requirements to meet Maturity Level One, none were met. This was due to application control not being implemented.

Windows Defender Application Control (WDAC) is a security feature of Microsoft Windows 10 and Microsoft Windows 11 that can be used for application control. Guidance on WDAC Group Policy settings, and alternative implementation approaches, are provided in ASD's *'Implementing Application Control'*.⁶

Restrict Microsoft Office Macros

To securely manage the use of macros within an organisation, all macros should be checked by assessors that are independent of macro developers, to ensure that they are safe before being digitally signed or placed within trusted locations.

Of the four (4) requirements to meet Maturity Level One, none were met. This was primarily due to user's ability to change their security settings.

An assessment of security benefit, business impact and implementation difficulty of different approaches is required to determine the appropriate implementation for [REDACTED]. Guidance on these approaches and impacts is provided in ASD's *'Restricting Microsoft Office Macros'*.⁷

User Application Hardening

Workstations are often targeted by malicious actors using malicious websites, emails or removable media in an attempt to extract sensitive information. Hardening workstations is an important part of reducing this risk.

Of the four (4) requirements to meet Maturity Level One, none were met. This was in part due to user's ability to change their security settings and in part due to not being implemented.

⁵ <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-administration/restricting-administrative-privileges>

⁶ <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-application-control>

⁷ <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/restricting-microsoft-office-macros>



Applications should have any in-built security functionality enabled and appropriately configured, along with unrequired functionality disabled. This is especially important for key applications such as office productivity suites (e.g. Microsoft Office), PDF readers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash), email clients (Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .NET Framework). In addition, vendors may provide guidance on configuring their products securely. Guidance on system hardening of applications and ICT equipment can be found on ASD's System hardening webpage.⁸

Regular Backups

To mitigate the security risk of losing system availability or data as part of a ransomware attack, or other form of destructive attack, backups of data, applications and settings should be performed and retained in accordance with an organisation's business criticality and business continuity requirements.

Of the six (6) requirements to meet Maturity Level One, four (4) were met. The requirements not met related to business criticality assessments and disaster recovery procedures.

Formalisation of roles and responsibilities for cyber security within ██████████, including the appointment of a CISO (or equivalent). Guidance on the cyber security roles and responsibilities is provided in ASD's 'Guidelines for Cyber Security Roles'.⁹

⁸ <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-365-office-2021-office-2019-and-office-2016>

⁹ <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-roles>

Overview of Cyber Security Governance and Operations

Privacy Legislative Compliance

With operations in [REDACTED] has discrete privacy legislative obligations depending on the jurisdiction, with each jurisdiction publishing their specific Privacy Policy on their respective websites. Privacy obligations are subject to annual legal review within each jurisdiction to ensure ongoing compliance with the local legislative requirements. A Notifiable Data Breach Policy has been established as a subset of the Australian Privacy Policy. The procedures within this plan have not been tested.

Risk Management

Digital IP Risk Management Policy and Privacy Risk Management Policy exist as separate documents; however, they contain details of controls to be implemented rather than providing a framework for risk management and procedures for risk assessments.

A risk management framework and risk assessment procedures should be suitable for use across all jurisdictions, be able to be used for risk assessment of patches, updates or vendor mitigations, and include a risk register to record decisions and treatment plans, and to monitor status.

Audit Program and/or Security Calendar

An internal audit program, supported by a security calendar, has the benefits of identifying risks and providing a mechanism to monitor and improve overall cyber security posture.

Establishment of a programmatic approach to security testing and monitoring of controls, underpinned by a risk management framework, is recommended.

Awareness and Training

Cyber security awareness training and communication of cyber security policies across the organisation should be considered as a means of creating a culture of people-centric security and contributing to the prevention of data breaches and phishing incidents.¹⁰

Incident Response Planning

While a Notifiable Data Breach Policy and associated procedures exist for Australia, incident response and business continuity plans were not observed for any jurisdiction. In the event of an incident or disruption to business continuity, the Notifiable Data Breach policy may provide guidance. Responsibilities for some incident response and business continuity activities have been outsourced to third parties.

Guidance on cyber security incident response planning is provided in ASD's 'Cyber Security Incident Response Planning: Practitioner Guidance'.¹¹

¹⁰ <https://www.cyber.gov.au/protect-yourself/securing-your-email/email-security/preventing-business-email-compromise>

¹¹ <https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/incident-response/cyber-security-incident-response-planning-practitioner-guidance>



Overview of Security Architecture

Microsoft Office 365 CIS Audit

An Office 365 Audit for [redacted] tenancy was conducted against the industry hardening standard, "CIS Microsoft 365 Foundations Benchmark", v3.0.0 (09-29-23).

CIS hardening and controls are an industry standard for service hardening, and they exist for operating systems, cloud platforms, and other services. The benchmarks represent best practice configuration and aims to result in a secure state for the tenancy. It is not imperative that every control within the standard is met, but any deficiencies introduce some risk. It is accepted that alignment should be considered and applied by default, where possible and where cost-benefit permits.

The tenancy audited was noted to be relatively old. More modern tenancies have a different baseline level of security control configurations. Due to the age of the tenancy, the findings are reasonable, but uplift and alignment with best practice is recommended. The audit measured against controls with in-use services only and covered 105 controls, with results summarised in Table 4.

CIS Controls	MED	MED-HIGH	PERIODIC	VALIDATE
Microsoft 365 Admin Center	0	9	1	2
Microsoft 365 Defender	7	6	5	4
Microsoft Purview	3	1	1	0
Microsoft Entra admin center	9	9	3	7
Microsoft Exchange admin center	1	1	1	9
Microsoft Sharepoint admin center	2	6	0	4
Microsoft Teams admin center	3	5	0	1
Total	25 ❌	37 ❌	11 ?	27 📅

Table 4 – CIS Control summary table

Key review notes:

- The MED/MED-HIGH metric count includes 'PERIODIC' and 'PARTIAL' but not VALIDATE status. A control with the status 'VALIDATE' needs to be further qualified/quantified, with PowerShell execution or consideration towards specific environment requirements and status.
- A periodic control is one which should be included in the IT operational calendar and reviewed or executed on a determined frequency (DAILY, WEEKLY, MONTHLY, QUARTERLY, 6 MONTHLY, YEARLY).
- Criticality ratings are set to differentiate and recommend remediation prioritisation efforts. These are auditor assessments for consideration against the environment and risk-based prioritisation. Remediation effort should focus on quick wins, easy configuration MED-HIGH findings, and with a focus on 'Microsoft 365 Admin Center', 'Microsoft 365 Defender' and 'Microsoft 365 Entra' as priorities over other areas.

Office 365 control audit findings and supporting details are included in Appendix G.

Microsoft Azure CIS Audit

Azure has not been audited in detail, as only a limited number of virtual machines are in use as part of backup/disaster recovery solution. A standard similar to that for Office 365 exists for security assurance and hardening approach, and “*CIS_Microsoft_Azure_Foundations_Benchmark_v2.1.0.pdf*” has been attached in Appendix I.

More so than the Office 365 tenancy, which has received some configuration to date – Azure hardening controls, in general, will be default and initial. Should the Azure environment be considered a production environment, or further workloads are utilised within Azure in the future – the environment should be prepared with hardening where possible, as recommended in the benchmark.

At a minimum, general access to user and administrator user accounts should be reviewed, with an aim to minimise access to least-privilege and apply MFA appropriately.

Security Architecture Domains

Security domains were analysed against [REDACTED], current architecture ([REDACTED]), including WAN-connected and service provider assets. Detailed findings are listed in table within Appendix D.

Some identified well-managed areas are:

- AP21, which has reasonable processes, baselines, recovery and support – complemented by specialist vendor support.
- General backups have reasonable recovery mechanisms, a layered approach, and multi-platform solutions. An exception here is the enablement of MFA for backup, delete or overwrite.
- EDR for Windows, which uses a best-of-breed CrowdStrike platform. The platform can be complimented with strong configuration, monitoring, alerting and extensions – but it is in a good starting point.

A summary of recommendations below is in general order of criticality. Appendix D includes detailed implementation recommendations.

Network Infrastructure should be enhanced with:

- Standardised network design, documentation and management.
- Standardised and least privileged firewall rules.
- Improved and centralised management of firewalls either with MSP or internal.
- Segmentation for DMZ, Server, WIFI, LAN's.
- Standardised switching and routing brands, versions and firmware.
- Replacement of the VPN / remote access solution:
 - This is currently critical as basic authentication is in place for VPN connections rather than 2FA or certificates, and once terminated, connections are not segmented from broader LAN and WAN resources.
- Creation of dedicated computing resources for administrative tasks.
- Removal and decommission of legacy or non-required equipment.

Multi-factor authentication and Data recovery should be enhanced with:

- Use of hardware keys for administrators and employees.
- Backup files and images delete/overwrite requiring MFA.
- Data recovery documentation, recovery prioritisation, and periodic testing.



Audit logging should be enhanced with:

- An established audit log management process.
- Development of the centralised SIEM (testing, partially in place).
- Alerting and incident response integration.

Secure configuration should be enhanced with:

- Secure configuration processes and definitions detailing standard operating environments (SOE/MOE), and validation methodologies.
- Tooling integrations to aid in the configuration and management of secure environments.

Access control should be enhanced with:

- The establishment and maintenance of an enterprise authentication/authorisation systems inventory.
- Centralised access control for all enterprise assets, where possible, via directory service or SSO.
- Active directory migration to Entra, though limited by core application, should be driven where possible.
- Definition and maintenance of role-based access controls.
- Shadow IT observability through tooling such as proxy.
- Periodic access control review processes and periodic scheduling.

Vulnerability management should be enhanced with:

- Establishment of a Vulnerability Management platform and program.
- Alignment of the program with risk-based remediation strategy.
- Reporting and remediation approach definitions.
- Threat intelligence source monitoring.
- Static and dynamic tooling.

Application layer filtering should be enhanced with:

- Web Application Firewall (WAF) implementation for any internet-facing API or websites.
- Outbound application internet access proxying, which enhances logging/observability of servers to internet access, and limits applications internet access to websites they need.

Application allow listing should be enhanced with:

- Native or third-party solutions to restrict the execution of binaries on servers and workstations for all SOE environments.
- Best practice protections to authorise library loads or script executions.

User account management should be enhanced with:

- HR integrated processes for onboarding/offboarding or change of roles.

Email and web browser protection should be enhanced with:

- Permitted and configured browser definition for SOE environments.
- DNS and category filtering to block access to known malicious domains.
- Blocking of malicious file types via email gateway.

Malware defences should be enhanced with:

- Coverage of all enterprise assets, with policy including local and removable media scanning.
- Anti-exploitation feature configuration (DEP is in place for Windows, but MacOS could be enhanced with Gatekeeper).

Staff security awareness should be enhanced with:

- Development of a staff security awareness program.
- Training against the program conducted upon hire, and periodically.

Penetration testing should be enhanced with:

- The development of a penetration testing program, optimised for cost-effective exposure management for external and internal assets.
- Maintenance and management of findings and remediations.

Enterprise/personal segregation should be enhanced with:

- Separate enterprise workspace use on mobile and end-user devices where supported (Application Configuration profile, Android Work profile).
- App protection policy configuration within Intune (work in progress).

General account management should be enhanced with:

- Establishment and maintenance of user and service account inventory.
- Centralised views and reporting to validate accounts, count, and adds/moves/changes (e.g., alerting that a new Administrator account has been created).
- Minimal and standardised data field collection for user accounts.
- Password policies that ensure unique and enforced configuration against password standards.
- Automated or alerting to manually or automatically disable dormant accounts.

Intrusion detection (NIDS/HIDS) should be enhanced with:

- Deployment of host-based intrusion detection and prevention (HIDS/HIPS) systems, which validate file integrity of key operating system and application binaries on servers and workstations.
- Deployment of network-based intrusion detection and prevention (NIDS/NIPS) systems, which monitor enterprise subnets and network segments via switch SPAN ports. This capability should be incorporated with network design.

Asset discovery should be enhanced with:

- Zone-based IP address and host discovery automation systems. This can be an integrated system, including Vulnerability Management tooling.
- Internal and External port and services visibility and reporting.
- Observability of software installed on servers and workstations.
- A process for investigating findings and changes to the environment.

Data management should be enhanced with:

- Definition of a data catalogue containing key information relating to enterprise data sets.
- Policy and definition of key data-related controls, such as retention, classification, data flow and disposal requirements.
- Periodic and global review, from a data perspective, of ACLs associated with each data set and based on user-need-to-know.

Data encryption – removable media should be enhanced with:

- Hardware and software solutions to ensure that removable media for managed SOE environments ensures enterprise data is encrypted on workstations and servers.

Data encryption – at rest should be enhanced with:

- Review and assurance that all sensitive data defined in the data catalogue is encrypted with strong mechanisms at rest. AP21 data on Oracle is currently non-encrypted, and may be limited by cost-of-software for Oracle table-level encryption solution, or performance.



Data loss prevention should be enhanced with:

- Implementation of a DLP solution to identify sensitive data stored, processed or transmitted through enterprise assets.

Asset Management should be enhanced with:

- The expanded use of the Asset Management system (currently Snipe IT) by adding all switches, virtual machines etc. and standardising meta-data handling.
- Expansion and standardisation of Asset Management standards and solutions to all regions.
- Validation of the Asset Management system contents using discovery tooling.

Physical security should be enhanced with:

- CCTV installation for all comms equipment, server rooms, and key office facilities.
- Centralised or localised proxy management solutions to manage staff access.
- Visitors register for key offices and comms facilities.

Software management should be enhanced with:

- Definition and maintenance of an approved software list.
- Review and compliance, supported by the Asset Management system.
- A process to periodically validate all software within vendor support, tracking EOL dates to ensure support and continuity.

Service provider management should be enhanced with:

- Establishment and maintenance of service provider inventory.
- Maintaining a view and capability understanding of service provider compliance and security (e.g., using CAIQ).
- Process definition for securely decommissioning service providers.

IT operations should be enhanced with:

- Creation and definition of an IT security operational calendar.
- Management and maintenance of activities included within the calendar, including ticketing and assignment, alerting to upcoming major tasks (e.g., quarterly, yearly tasks), and follow-up review/assurance that tasks are being completed.

Remote assets should be enhanced with:

- Access control integration and visibility for any asset connecting to enterprise resources (Intune is in place for Melbourne, requires global configuration).
- Compliance policy enforcement to ensure anti-virus software is installed and up to date, and that system configurations comply with SOE/patching standards prior to connecting to enterprise assets.

Appendix A Essential Eight Maturity Model (November 2023)



PROTECT - Essential
Eight Maturity Mode





Appendix B CIS Microsoft 365 Foundations Benchmark v3.0.0 (09-29-23)



CIS_Microsoft_365_
Foundations_Benchm

Appendix C Detailed recommendations for Essential Eight

Patch application

R1: Implement a unified solution to patch management to cover all operating systems and all applications in all jurisdictions, inclusive of contractual requirements for third-party managed systems.

R2: Implement a policy and procedures for risk assessment of all patches, updates or vendor mitigations, including a risk register to record decisions on criticality in a <client> context.

R3: Implement a policy and procedures for Change Management, including requirement to retain records of changes applied.

R4: Implement a policy and procedures for patch management that includes the (minimum) requirement for application of patches within the time constraints provided in the Essential Eight Maturity Level One.

R5: Implement a policy and procedures for internal vulnerability management that includes the (minimum) requirement for a vulnerability scanner to be used at least as frequently as outlined in the Essential Eight Maturity Level One.

R6: Implement a policy, and procedures for asset management that includes end of life management for Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products.

R7: Establish and maintain an asset register, inclusive of discovery of Business Managed IT and shadow IT, and supported by regular asset discovery.

R8: Establish a BYOD Policy.

Patch operating systems

R1: Implement a unified solution to patch management to cover all operating systems and all applications in all jurisdictions, inclusive of contractual requirements for third-party managed systems.

R2: Implement a policy and procedures for risk assessment of all patches, updates or vendor mitigations, including a risk register to record decisions on criticality in a <client> context.

R3: Implement a policy and procedures for Change Management, including requirement to retain records of changes applied.

R4: Implement a policy and procedures for patch management that includes the (minimum) requirement for application of patches within the time constraints provided in the Essential Eight Maturity Level One.

R5: Implement a policy and procedures for internal vulnerability management that includes the (minimum) requirement for a vulnerability scanner to be used at least as frequently as outlined in the Essential Eight Maturity Level One.

R7: Establish and maintain an asset register, inclusive of discovery of Business Managed IT and shadow IT and supported by regular asset discovery.

R8: Establish a BYOD Policy.

R9: Implement a policy and procedures for asset management that includes end of life management for operating systems.





Multi-factor authentication

- R10:** Implement a policy and procedures for identity and access management that includes the (minimum) requirements for the configuration of MFA provided in the Essential Eight Maturity Level Two and privileged access provided in Essential Eight Maturity Level One.
- R11:** Update references to MFA policy settings in employee documentation and communications.
- R12:** Establish and maintain a list of MFA capability of third party and online services within an asset register.
- R13:** Implement MFA for all users for all internet facing services that includes the (minimum) requirements of Essential Eight Maturity Level Two, and if not available consider alternative solutions.
- R14:** Include MFA unsuccessful attempts and security events from internet-facing servers in SIEM dashboards.
- R15:** Implement a policy and procedures for cyber security incident response, including clear articulation of roles, responsibilities and accountability.
- R16:** Consider registering as an ACSC Business Partner.
- R17:** Conduct tabletop testing of the cyber security incident response plan and notifiable data breach plan.

Restrict administrative privileges

- R10:** Implement a policy and procedures for identity and access management that includes the (minimum) requirements for the configuration of MFA provided in the Essential Eight Maturity Level Two and privileged access provided in Essential Eight Maturity Level One.
- R18:** Remove local admin privileges for all users who do not have a role-based requirement to have those privileges.
- R19:** Verify the requests for new or changed access via IT Ticketing System and maintain records of those with access.
- R20:** Restrict privileged accounts from accessing the internet, email and web services.
- R21:** Consider setting all privileged accounts and access to systems to automatically disable after 45 days of inactivity.

Application control

- R8:** Establish a BYOD Policy.
- R22:** Implement a Standard Operating Environment for workstations, with consideration to all Essential Eight mitigation strategies.
- R23:** Consider implementing Windows Defender Application Control (WDAC).

Restrict Microsoft Office macros

- R10:** Implement a policy and procedures for identity and access management that includes the (minimum) requirements for the configuration of MFA provided in the Essential Eight Maturity Level Two and privileged access provided in Essential Eight Maturity Level One.
- R18:** Remove local admin privileges for all users who do not have a role-based requirement to have those privileges.
- R22:** Implement a Standard Operating Environment for workstations, with consideration to all Essential Eight mitigation strategies.
- R24:** Disable permissions for users to change Microsoft Office macro security settings.
- R25:** Disable permissions for users to change web browser security settings.
- R26:** Review CrowdStrike configuration to ensure antivirus scanning is enabled for Microsoft Office macros.

User Application Hardening

- R18:** Remove local admin privileges for all users who do not have a role-based requirement to have those privileges.
- R22:** Implement a Standard Operating Environment for workstations, with consideration to all Essential Eight mitigation strategies.
- R25:** Disable permissions for users to change web browser security settings.
- R27:** Disable or remove Internet Explorer for all regions.
- R28:** Implement controls to block web browsers from processing java from the internet.
- R29:** Establish and implement baseline configuration for web browsers.
- R30:** Review endpoint protection and web browser configurations to protect against vulnerabilities introduced as a result of web advertisements being enabled.

Regular Backup

R7: Establish and maintain an asset register, inclusive of discovery of Business Managed IT and shadow IT, and supported by regular asset discovery.

R10: Implement a policy and procedures for identity and access management that includes the (minimum) requirements for the configuration of MFA provided in the Essential Eight Maturity Level Two and privileged access provided in Essential Eight Maturity Level One.

R31: Document and implement Business Impact Assessments for key assets.

R32: Document and implement Disaster Recovery and Business Continuity policy and procedures, including backup and restoration requirements.


R33: Establish a security testing schedule/calendar.


Table 5 – Detailed recommendations for improvement









Appendix D Detailed recommendations for Security Architecture

Findings within the table are listed in priority order, first by criticality, and secondly by size/complexity associated with remediation(s). Items highlighted with a  symbol, should be integrated with the IT periodic operational calendar.

CIS18 MAP	Key item	Recommendation	Criticality	Sizing
12/13	Network Infrastructure Management	<ul style="list-style-type: none"> • Centralise and standardise network diagrams for WAN/LAN and data-flow. • Perform a complete firewall rule review and consolidation: <ul style="list-style-type: none"> ◦ Many current router ANY/ANY rules and/or with ALL service exist. ◦ Rule conventions throughout enterprise not standard, managed by multiple MSP's. • Validate MSP firewall and router management standards, SLA, & current configuration status: <ul style="list-style-type: none"> ◦ Change seems only to be enacted from  instruction, at a cost, with MSP's having write access. Over time this has deteriorated configuration and management standards. ◦ Fortigate manager host has been identified, with 0 hits inbound traffic on router – implying it has not had connections for some time, and represents a potentially exposed or unmanaged host Melbourne (10.0.0.99). • Establish a secure network architecture, ensuring: <ul style="list-style-type: none"> ◦ Segmentation, with traffic filtering between segments where possible. ◦ Infrastructure as Code deployment for switch & router configurations. ◦ Integrated SIEM logging (LibreNMS currently doing SNMP only). ◦ Only secure network protocols in use ◦ Centralised AAA for network devices (RADIUS, TACACS+ etc). ◦ Ensure Least privilege. ◦ Availability. • Standardise Switch and Router brands, versions and firmware: <ul style="list-style-type: none"> ◦ Currently Fortigate upgrade pattern is not current / behind required standards. ◦ Multiple switch versions exist, making standardised secure configuration/hardening difficult. ◦ Configure 802.1x port access control for LAN devices • Replace or uplift VPN solution for remote access: <ul style="list-style-type: none"> ◦ Currently basic auth and should be certificate or 2FA based. ◦ Terminating to the VPN leaves connection on broad/flat network with over-exposed access to network devices and services. • Separate/dedicate administrative computing resources for administrative tasks or tasks requiring administrative access: <ul style="list-style-type: none"> ◦ Segmented from primary network. ◦ With no internet access. • Maintain separate environments for production and non-production systems: 	CRITICAL	LARGE

CIS18 MAP	Key item	Recommendation	Criticality	Sizing
		<ul style="list-style-type: none"> o AP21 is compliant. • Shutdown non-required equipment (e.g., rack 3 legacy backup solution). 		
6	Multi factor authentication	<ul style="list-style-type: none"> • Utilise MFA where possible, prioritising external resources and sensitive data/platform access: <ul style="list-style-type: none"> o Consider hardware-based authorisation for endpoints, e.g. (YubiKey / FIDO2) • Require MFA for all externally-exposed enterprise or third-party applications where supported. <ul style="list-style-type: none"> o SSO is satisfactory implementation for this requirement. • Require MFA for all administrative access. • Require MFA for remote network access (currently VPN is basic auth). 	CRITICAL	MED
11	Data recovery	<ul style="list-style-type: none"> • Establish and maintain a data recovery process (documentation/process), addressing scope of activities, recovery prioritisation and security of backup data. • Enable MFA delete for critical data backups. • Validate UPS capabilities, and power-out alerting are adequate for safe-shutdown window processes. <p>Establish and maintain an audit log management process,</p>	CRITICAL	MED
3,13	Audit Logging	<ul style="list-style-type: none"> • that defines the enterprises logging requirements: <ul style="list-style-type: none"> o At a minimum address the collection, review and retention of audit logs. • Develop a centralised logging platform/SIEM: <ul style="list-style-type: none"> o Collect all logs per audit log management process. o Standardise time synchronisation with at-least 2x time sources where supported. o Configure detailed audit logging for enterprise assets containing sensitive data, including: <ul style="list-style-type: none"> ▪ Event source. ▪ Date. ▪ Username. ▪ Timestamp. ▪ Source address. ▪ Destination address. o Retain audit logs for a minimum of 90 days. o Ensure adequate storage requirements to comply with audit log management process. • Include/automate ingestion of all logging asset types: <ul style="list-style-type: none"> o Sensitive data access, defined in data catalogue. o Router and switch key security and access logs. o All server event and security logs. o WAF, DLP, IDS/IPS, HIDS/NIDS, DNS. o URL requests. o Command line audit logs, e.g., PowerShell, BASH. o Vulnerability management data. o Key application security/export logs (AP21). • Configure alerts based on standard security event patterns, and specific implementations (e.g., AP21). • Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat, at a minimum (weekly).  	HIGH	LARGE




CIS18 MAP	Key item	Recommendation	Criticality	Sizing
		<ul style="list-style-type: none"> Include review and uplift of both policy and logging system as periodic activity via operational calendar (quarterly).  		
4	Secure configuration	<ul style="list-style-type: none"> Establish a secure configuration process for enterprise assets includes: <ul style="list-style-type: none"> Documented security standards. Documented SOE/MOE. Configuration policies. Validation methodology to periodically test controls.  Utilise hardening standards where possible (e.g., CIS, Vendor). Tailor based off: <ul style="list-style-type: none"> Organisational appetite. Risk assessment/cost-benefit. Industry best practice. Utilise appropriate tools, and manual configuration as required: <ul style="list-style-type: none"> Infrastructure as code (e.g., Terraform, ARM templates). Policy driven (e.g., Active Directory). Environment management (e.g., Intune, ManageEngine). Third (3rd) party (e.g., CSPM). Manual configuration. Key categories: <ul style="list-style-type: none"> O365 (CIS). Azure (CIS). Windows Server (CIS). Windows and Apple macOS client (CIS). AP21 (vendor best practice). Router and Switch (vendor best practice). Mobile and BYOD. Achieve at a minimum for each category: <ul style="list-style-type: none"> Default account disable/rename. Password complexity & MFA. Removal of unnecessary services & minimised feature-set availability based off business need. Access control based of RBAC/need-to-know. Least-privilege/deny-by-default. Managed firewall rulesets. Immutable logging. Configuration + data backup retention. Minimise number of vendor solutions where possible: <ul style="list-style-type: none"> Switches and routers hardware & firmware versions. Server hardware. Server hardware and operating system versions. Workstation and Laptop hardware and operating system versions. 	HIGH	LARGE
6	Access control	<ul style="list-style-type: none"> Establish and maintain an inventory of all enterprise authentication and authorisation systems, including those hosted at service providers. <ul style="list-style-type: none"> Review and update the register periodically.  	HIGH	LARGE

CIS18 MAP	Key item	Recommendation	Criticality	Sizing
		<ul style="list-style-type: none"> • Centralise access control for all enterprise assets where possible via directory service or SSO provider. <ul style="list-style-type: none"> ◦ Entra ID is in place, but does not currently service all enterprise assets. ◦ AD on prem is legacy, limited by C21 (not Entra ready). ◦ Support and roadmap legacy systems where possible. • Define and maintain role-based access control, through determining and documenting access rights necessary for each role within the enterprise to successfully carry out assigned duties. • Gain understanding of shadow IT, with view to gain control over time. • Perform access control reviews of enterprise assets to validate all privileges are authorised (quarterly-yearly). 📅 		
7	Vulnerability Management	<ul style="list-style-type: none"> • Establish a Vulnerability Management Program: <ul style="list-style-type: none"> ◦ Document a vulnerability management process for enterprise assets. Review and update documentation annually or after significant infrastructure change. (yearly). 📅 ◦ Establish and maintain a risk-based remediation strategy. Establish a process for discovered vulnerability risk acceptance, and responsible party handling. • Implement a Vulnerability Management Platform (e.g., Tenable, Rapid7, Qualysguard, OpenVAS). <ul style="list-style-type: none"> ◦ Zone based, SCAP compliant scanners. ◦ Network Discovery -> Non-authenticated -> Authenticated scan modes and progression. ◦ Integrated logging with SIEM. • Perform monthly scans (monthly). 📅 • Remediate detected vulnerabilities in software through tooling, manual configuration, software removal. • Monitor vulnerability threat intelligence sources, in order to get early heads up and align VMS plugins/scans with enterprise owned assets (daily). 📅 • Compliment the core program with static and dynamic analysis tooling (e.g., static code analysis for scripts/application code, and DAST for dynamic application security testing (pre-penetration testing). 	HIGH	LARGE
13	Application layer filtering	<ul style="list-style-type: none"> • Configure WAF for any internally or MSP hosted web-service or API: <ul style="list-style-type: none"> ◦ Not in place for current API's. ◦ Configure Geoblocking, and tune API(s) / websites against WAF. • Configure outbound application internet access proxying: <ul style="list-style-type: none"> ◦ Applications or servers can be grouped into an "AppSpace". ◦ Force servers via proxy/gateway solution (e.g., Netskope). ◦ Monitor mode -> Active mode. 	HIGH	LARGE



CIS18 MAP	Key item	Recommendation	Criticality	Sizing
		<ul style="list-style-type: none"> o Ensure servers only access internet sites that they require (e.g., Windows update, www.myapplicationsintegration.com etc. o Integrate with logging solution. • This control stops issues like command and control services phoning home. 		
2	Application allow-listing	<ul style="list-style-type: none"> • Implement application allow-listing (e.g., AppLocker, or third-party solutions such as Airlock Digital): <ul style="list-style-type: none"> o Apply to all environments where possible, including workstations/servers, Linux, Windows & Mac clients. • Configure to allow only permitted software to be executed. • Implement best practice per solution, e.g., authorised library loads only, blocking script execution (.ps1, .py etc). • Capability delivered in conjunction with general operating system hardening standards application (Intune policy, CIS hardening etc). 	HIGH	MED
6	User account management	<ul style="list-style-type: none"> • Establish a process, integrated with HR for access to enterprise assets. • Access is granted or revoked based on new hire, approval process, and role change. • Ensure accounts are disabled immediately upon termination. 	HIGH	MED
9	Email and web browser protection	<ul style="list-style-type: none"> • Ensure only fully supported browsers and email clients are allowed to run on enterprise assets. • Use DNS filtering on all enterprise assets to block access to known malicious domains. Utilise category based filtering. • Enforce and update network-based URL filters to limit enterprise server/service assets to least-privilege (application proxy, e.g., Netskope). • Ensure unnecessary file types blocked in email gateway (some legacy policy is in place, validate all file types and global applicability). 	HIGH	MED
10	Malware defences	<ul style="list-style-type: none"> • Ensure anti-malware solution covers all enterprise assets, with appropriate policy that includes local and removable media scanning. • Enable anti-exploitation features where possible, e.g. DEP (in place for Windows), Gatekeeper requires implementation on MacOS. • Validate globally applied to all enterprise assets. 	HIGH	MED
14	Staff security awareness	<ul style="list-style-type: none"> • Establish and operate an enterprise “staff security awareness program”: <ul style="list-style-type: none"> o Educate workforce on how to interact with assets and data in a secure manner. o Conduct training at hire, and annually for all staff. o Train members on. <ul style="list-style-type: none"> ▪ Recognising social engineering attacks such as phishing and tailgating. ▪ Authentication best practices such as MFA, password composition and credential management. 	HIGH	MED

CIS18 MAP	Key item	Recommendation	Criticality	Sizing
		<ul style="list-style-type: none"> ▪ How to identify, properly store, transfer, archive and destroy sensitive data. ▪ Clean screen and desk policies, locking screens, and erasing whiteboards. ▪ Portable end user device management, such as encrypted USB keys. ▪ Reporting of incidents. Validating out-of-date software patches, or ▪ notifying in cases of failures of automated processes or tools. Transmitting data over insecure networks. 		
16/18	Penetration testing	<ul style="list-style-type: none"> • Develop the penetration testing program: <ul style="list-style-type: none"> o Apply appropriate to the size of the organisation and value of assets being protected. o Periodically test all external public facing assets annually. o Periodically test key internal or WAN facing key services. o Iterate on changes with penetration testing providers, e.g. the testing of new fields as a v1.1, upon mid-year release in a mini penetration test. o Integrate program and results with vulnerability scanning, and DAST services. o Consider whitebox and blackbox approaches, as-well as social engineering. • Maintain a register of findings and remediations. 	HIGH	MED
4	Enterprise/personal segregation	<ul style="list-style-type: none"> • Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. • Example systems: <ul style="list-style-type: none"> o Apple Configuration Profile. o Android Work Profile. • Complete App protection policy configuration within Intune (WIP). 	HIGH	SMALL
5	General account management	<ul style="list-style-type: none"> • Establish and maintain an inventory of all user and service accounts managed in the enterprise. • Create a centralised view via automation to validate accounts, and count. • At a minimum ensure collection and up to date data fields: <ul style="list-style-type: none"> o Name. o Username. o Start/stop dates. o Department. o Purpose (service accounts). • Ensure unique passwords are used for all enterprise assets: <ul style="list-style-type: none"> o Minimum 8-character password for MFA protected accounts. o Minimum 14-character password for non-MFA protected accounts. • Remove or disable any dormant accounts after a period of 45 days inactivity where supported. <ul style="list-style-type: none"> o Validate all active accounts are authorised.  	MED	LARGE



CIS18 MAP	Key item	Recommendation	Criticality	Sizing
13	Intrusion detection (NIDS/HIDS)	<ul style="list-style-type: none"> Deploy a host-based intrusion detection/prevention solution on enterprise assets (HIDS/HIPS), e.g., OSSEC: <ul style="list-style-type: none"> Host based agents that validate checksum of key system/application files etc. Deploy a network intrusion detection/prevention solution, monitoring enterprise subnets and network segments (span port) (NIDS/NIPS) e.g., SNORT: <ul style="list-style-type: none"> Being span port and network segment based, network intrusion detection/prevention in particular as compared with host – is highly integrated with network architecture design (i.e., Network Infrastructure Management recommendations), 	MED	LARGE
1,2	Asset discovery	<ul style="list-style-type: none"> Implement an asset discovery system – identifying hosts (anything with an IP address), and installed software: <ul style="list-style-type: none"> Consider utilising scanners with Zone based approach. Consider WAN impact if centralized. Core capability is ‘discovery’ mode scanning with a non-authenticated view, like via a Vulnerability Management system. Secondary capability is authenticated inventory query. May utilise active directory or other asset discovery tools (e.g., ManageEngine, Snipe IT, Intune). May utilise SPAN ports from core switches for passive host detection. Automate discovery and review as a periodic activity via operational calendar (monthly). 📅 Investigate any newly discovered hosts, non-approved software and non-approved software versions. Cross check findings to maintain Asset Manager (manual inspection is required, but integration workflow is higher capability). 	MED	LARGE
3	Data management	<ul style="list-style-type: none"> Establish a data catalogue (record of key data sets, location, key controls, criticality, sensitivity, owner). Define: <ul style="list-style-type: none"> Handling requirements. Data retention limits/standards. Classification, (Sensitive, Confidential, Public). Data flows, including service provider. Disposal requirements. Globally review ACLs associated with each data set, based on user need-to-know. Ensure data disposal mechanisms and process exists and tested (particularly where managed by vendors). Include review and uplift as periodic activity via operational calendar (monthly). 📅 	MED	MED
3	Data encryption – removable media	<ul style="list-style-type: none"> Configure encryption at rest mechanisms for removable media: <ul style="list-style-type: none"> All end-user devices including mobile, Windows (Australia is in place, other regions require), and Mac. 	MED	MED

CIS18 MAP	Key item	Recommendation	Criticality	Sizing
		<ul style="list-style-type: none"> Consider policy enforcement for USB devices, e.g., allowing only physical hardware encryption USB brand/serials to be used. 		
3	Data encryption – at rest	<ul style="list-style-type: none"> Configure encryption at rest for data (servers, workstations): <ul style="list-style-type: none"> Reference data catalogue to ensure all sensitive data considered. Investigate and apply where possible either hardware or application layer solution. AP21 Oracle data currently non-encrypted. 	MED	MED
3	Data Loss Prevention	<ul style="list-style-type: none"> Implement DLP solution to identify all sensitive data stored, processed or transmitted through enterprise assets: <ul style="list-style-type: none"> Base off data catalogue. Extend to managed services infrastructure. Include review and uplift as periodic activity via operational calendar 📅 (monthly). 	MED	MED
1,2	Asset Management	<ul style="list-style-type: none"> Expand use of Asset Manager (currently Snipe IT): <ul style="list-style-type: none"> Add switches, virtual machines. Synchronise or centralise for EU and NA regions. Add software licensing and applications inventory. Include key metadata, {owner, location, logical-addr, physical-addr, description, deployment-mechanism, URL, version, etc}. Include review and uplift as periodic activity via operational calendar (monthly). 📅 Validate contents using discovery tooling, investigate findings that are not recorded in Asset Manager. 	MED	MED
N/A	Physical security	<ul style="list-style-type: none"> Validate CCTV in place for all comms equipment/server rooms. Validate CCTV in place for key office facilities, and locations where network access may be possible (e.g., warehouse). Ensure two (2) weeks on-motion recording capable: <ul style="list-style-type: none"> Validate that proxy access solutions at facilities account management is maintained and reviewed, separating proxy's to per-named users. Visitor register for key office and comms facilities. 	MED	MED
2	Software management	<ul style="list-style-type: none"> Utilise populated Asset Manager (monthly): 📅 <ul style="list-style-type: none"> Maintain an approved software list. Ensure unauthorised software is removed or documented as exception. Ensure all software is vendor supported, track EOL dates and ensure continuity / upgrade / replacement etc in advance of software EOL 	MED	SMALL
15	Service provider management	<ul style="list-style-type: none"> Establish and maintain an inventory of service providers. Establish and maintain a service provider policy, addressing classification, inventory, assessment, monitoring and decommissioning and risk. 	MED	SMALL




CIS18 MAP	Key item	Recommendation	Criticality	Sizing
		<ul style="list-style-type: none"> Maintain a view of service provider compliance and security (e.g., using CAIQ or other questionnaires). Securely decommission service providers, giving consideration to user accounts, termination of data-flows, secure disposal or enterprise data within service provider systems, and contractual requirements. 		
N/A	IT Operations	<ul style="list-style-type: none"> Create/define IT security operational calendar: <ul style="list-style-type: none"> Daily/Weekly/Monthly/Quarterly/Half-yearly/Yearly activities. Spread Quarterly -> Yearly activities out appropriately. Alert in advance and discuss during team meetings, key upcoming activities. Track completion via ticketing system and automation where appropriate, avoiding ticketing fatigue. Include: <ul style="list-style-type: none"> Known existing requirements/periodic activities. O365 related activities identified via CIS hardening. Azure related activities identified via CIS hardening. Periodic activities identified in this register, marked with  	MED	SMALL
13	Remote assets	<ul style="list-style-type: none"> Manage access control for assets connecting to enterprise resources: <ul style="list-style-type: none"> Intune compliance policies are in place (Melb only at this point). Needs NA/EU. Compliance policies to validate anti-virus software installed and up to date, configuration compliance with secure configuration process, and operating system/applications up to date – before access to network resources. 	LOW	SMALL

Table 6 – Detailed recommendations for Security Architecture

Appendix E Documents Reviewed

Title	Date / Version	Notes



Appendix F Essential Eight Maturity Assessment workbook

Appendix G Office 365 CIS control audit

CIS ref	Section	Subsection	Task	In place	Criticality
1.1.1 (L1)	Microsoft 365 admin center	Users	Ensure Administrative accounts are separate and cloud-only (Manual)	NO	MED-HIGH
1.1.2 (L1)	Microsoft 365 admin center	Users	Ensure two emergency access accounts have been defined (Manual)	NO	MED-HIGH
1.1.3 (L1)	Microsoft 365 admin center	Users	Ensure that between two and four global admins are designated (Automated)	YES	MED-HIGH
1.1.4 (L1)	Microsoft 365 admin center	Users	Ensure Guest Users are reviewed at least biweekly (Manual)	PERIODIC FORTNIGHTLY	MED-HIGH
1.2.1 (L2)	Microsoft 365 admin center	Teams & Groups	Ensure that only organisationally managed/approved public groups exist (Automated)	NO	MED-HIGH
1.2.2 (L1)	Microsoft 365 admin center	Teams & Groups	Ensure sign-in to shared mailboxes is blocked (Automated)	VALIDATE	MED-HIGH
1.3.1 (L1)	Microsoft 365 admin center	Settings	Ensure the 'Password expiration policy' is set to 'Set passwords to never expire (recommended)' (Automated)	YES	MED-HIGH
1.3.2 (L1)	Microsoft 365 admin center	Settings	Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices (Manual)	NO	MED-HIGH
1.3.3 (L2)	Microsoft 365 admin center	Settings	Ensure 'External sharing' of calendars is not available (Automated)	NO	MED-HIGH
1.3.4 (L1)	Microsoft 365 admin center	Settings	Ensure 'User owned apps and services' is restricted (Manual)	NO	MED-HIGH
1.3.5 (L1)	Microsoft 365 admin center	Settings	Ensure internal phishing protection for Forms is enabled (Manual)	YES	MED-HIGH
1.3.6 (L2)	Microsoft 365 admin center	Settings	Ensure the customer lockbox feature is enabled (Automated)	VALIDATE	MED-HIGH





CIS ref	Section	Subsection	Task	In place	Criticality
1.3.7 (L2)	Microsoft 365 admin center	Settings	Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web' (Manual)	NO	MED-HIGH
1.3.8 (L2)	Microsoft 365 admin center	Settings	Ensure that Sways cannot be shared with people outside of your organization (Manual)	NO	MED-HIGH
2.1.1 (L2)	Microsoft 365 Defender	Email & collaboration	Ensure Safe Links for Office Applications is Enabled (Automated)	PARTIAL	MED-HIGH
2.1.2 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure the Common Attachment Types Filter is enabled (Automated)	NO	MED-HIGH
2.1.3 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure notifications for internal users sending malware is Enabled (Automated)	NO	MED-HIGH
2.1.4 (L2)	Microsoft 365 Defender	Email & collaboration	Ensure Safe Attachments policy is enabled (Automated)	PARTIAL	MED-HIGH
2.1.5 (L2)	Microsoft 365 Defender	Email & collaboration	Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled (Automated)	YES	MED-HIGH
2.1.6 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure Exchange Online Spam Policies are set to notify administrators (Automated)	NO	MED-HIGH
2.1.7 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure that an anti-phishing policy has been created (Automated)	PARTIAL	MED-HIGH
2.1.8 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure that SPF records are published for all Exchange Domains (Manual)	VALIDATE	MED-HIGH
2.1.9 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure that DKIM is enabled for all Exchange Online Domains (Automated)	VALIDATE	MED-HIGH
2.1.10 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure DMARC Records for all Exchange Online domains are published (Manual)	VALIDATE	MED-HIGH
2.1.11 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure the spoofed domains report is reviewed weekly (Manual)	PERIODIC WEEKLY	MED

CIS ref	Section	Subsection	Task	In place	Criticality
2.1.12 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure the 'Restricted entities' report is reviewed weekly (Manual)	PERIODIC WEEKLY	MED
2.1.13 (L1)	Microsoft 365 Defender	Email & collaboration	Ensure all security threats in the Threat protection status report are reviewed at least weekly (Manual)	PERIODIC WEEKLY	MED
2.3.1 (L1)	Microsoft 365 Defender	Audit	Ensure the Account Provisioning Activity report is reviewed at least weekly (Manual)	PERIODIC WEEKLY	MED
2.3.2 (L1)	Microsoft 365 Defender	Audit	Ensure non-global administrator role group assignments are reviewed at least weekly (Manual)	PERIODIC WEEKLY	MED
2.4.1 (L1)	Microsoft 365 Defender	Settings	Ensure Priority account protection is enabled and configured (Manual)	PARTIAL	MED
2.4.2 (L1)	Microsoft 365 Defender	Settings	Ensure Priority accounts have 'Strict protection' presets applied (Manual)	NO	MED
2.4.3 (L2)	Microsoft 365 Defender	Settings	Ensure Microsoft Defender for Cloud Apps is enabled and configured (Manual)	VALIDATE	MED
3.1.1 (L1)	Microsoft Purview	Audit	Ensure Microsoft 365 audit log search is Enabled (Automated)	YES	MED-HIGH
3.1.2 (L1)	Microsoft Purview	Audit	Ensure user role group changes are reviewed at least weekly (Manual)	PERIODIC FORTNIGHTLY	MED
3.2.1 (L1)	Microsoft Purview	Data loss protection	Ensure DLP policies are enabled (Manual) Ensure DLP policies are enabled for	NO	MED
3.2.2 (L1)	Microsoft Purview	Data loss protection	Microsoft Teams (Manual) Ensure SharePoint Online Information Protection policies are set up and used (Manual)	NO	MED
3.3.1 (L1)	Microsoft Purview	Information protection		NO	MED-HIGH
5.1.1.1 (L1)	Microsoft Entra admin center	Overview	Ensure Security Defaults is disabled on Azure Active Directory (Manual)	YES	MED-HIGH
5.1.2.1 (L1)	Microsoft Entra admin center	Users	Ensure 'Per-user MFA' is disabled (Manual)	NO	MED-HIGH





CIS ref	Section	Subsection	Task	In place	Criticality
5.1.2.2 (L2)	Microsoft Entra admin center	Users	Ensure third party integrated applications are not allowed (Manual)	YES	MED-HIGH
5.1.2.3 (L1)	Microsoft Entra admin center	Users	Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes' (Automated)	YES	MED-HIGH
5.1.2.4 (L1)	Microsoft Entra admin center	Users	Ensure 'Restrict access to the Azure AD administration portal' is set to 'Yes' (Manual)	NO	MED-HIGH
5.1.2.5 (L2)	Microsoft Entra admin center	Users	Ensure the option to remain signed in is hidden (Manual)	NO	MED-HIGH
5.1.2.6 (L2)	Microsoft Entra admin center	Users	Ensure 'LinkedIn account connections' is disabled (Manual)	NO	MED
5.1.3.1 (L1)	Microsoft Entra admin center	Groups	Ensure a dynamic group for guest users is created (Manual)	VALIDATE	MED
5.1.5.1 (L1)	Microsoft Entra admin center	Applications	Ensure the Application Usage report is reviewed at least weekly (Manual)	PERIODIC WEEKLY	MED
5.1.5.2 (L2)	Microsoft Entra admin center	Applications	Ensure user consent to apps accessing company data on their behalf is not allowed (Manual)	NO	MED
5.1.5.3 (L1)	Microsoft Entra admin center	Applications	Ensure the admin consent workflow is enabled (Manual)	YES	MED
5.1.6.1 (L2)	Microsoft Entra admin center	External Identities	Ensure that collaboration invitations are sent to allowed domains only (Manual)	NO	MED
5.1.8.1 (L1)	Microsoft Entra admin center	Hybrid management	Ensure that password hash sync is enabled for hybrid deployments (Automated)	VALIDATE	MED
5.2.2.1 (L1)	Microsoft Entra admin center	Conditional Access	Ensure multifactor authentication is enabled for all users in administrative roles (Manual)	VALIDATE	MED-HIGH
5.2.2.2 (L1)	Microsoft Entra admin center	Conditional Access	Ensure multifactor authentication is enabled for all users (Manual)	NO	MED-HIGH

CIS ref	Section	Subsection	Task	In place	Criticality
5.2.2.3 (L1)	Microsoft Entra admin center	Conditional Access	Enable Conditional Access policies to block legacy authentication (Manual)	NO	MED-HIGH
5.2.2.4 (L1)	Microsoft Entra admin center	Conditional Access	Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users (Manual)	NO	MED-HIGH
5.2.2.5 (L2)	Microsoft Entra admin center	Conditional Access	Ensure 'Phishing-resistant MFA strength' is required for Administrators (Manual)	VALIDATE	MED-HIGH
5.2.2.6 (L2)	Microsoft Entra admin center	Conditional Access	Enable Azure AD Identity Protection user risk policies (Manual)	NO	MED-HIGH
5.2.2.7 (L2)	Microsoft Entra admin center	Conditional Access	Enable Azure AD Identity Protection sign-in risk policies (Manual)	NO	MED-HIGH
5.2.2.8 (L1)	Microsoft Entra admin center	Conditional Access	Ensure 'Microsoft Azure Management' is limited to administrative roles (Manual)	NO	MED-HIGH
5.2.3.1 (L1)	Microsoft Entra admin center	Authentication Methods	Ensure Microsoft Authenticator is configured to protect against MFA fatigue (Manual)	YES	MED-HIGH
5.2.3.2 (L1)	Microsoft Entra admin center	Authentication Methods	Ensure custom banned passwords lists are used (Manual)	NO	MED
5.2.3.3 (L1)	Microsoft Entra admin center	Authentication Methods	Ensure password protection is enabled for on-prem Active Directory (Manual)	NO	MED
5.2.4.1 (L1)	Microsoft Entra admin center	Password reset	Ensure 'Self-service password reset enabled' is set to 'All' (Manual)	NO	MED
5.2.4.2 (L1)	Microsoft Entra admin center	Password reset	Ensure the self-service password reset activity report is reviewed at least weekly (Manual)	PERIODIC WEEKLY	MED
5.2.6.1 (L1)	Microsoft Entra admin center	Risky activities	Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly (Manual)	PERIODIC WEEKLY	MED
5.3.1 (L2)	Microsoft Entra admin center	Identity Governance	Ensure 'Privileged Identity Management' is used to manage roles (Manual)	VALIDATE	MED





CIS ref	Section	Subsection	Task	In place	Criticality
5.3.2 (L1)	Microsoft Entra admin center	Identity Governance	Ensure 'Access reviews' for Guest Users are configured (Manual)	VALIDATE	MED
5.3.3 (L1)	Microsoft Entra admin center	Identity Governance	Ensure 'Access reviews' for high privileged Azure AD roles are configured (Manual)	VALIDATE	MED
6.1.1 (L1)	Exchange admin center	Audit	Ensure 'AuditDisabled' organizationally is set to 'False' (Automated)	VALIDATE	MED
6.1.2 (L1)	Exchange admin center	Audit	Ensure mailbox auditing for E3 users is Enabled (Automated)	VALIDATE	MED
6.1.3 (L1)	Exchange admin center	Audit	Ensure mailbox auditing for E5 users is Enabled (Automated)	VALIDATE	MED
6.1.4 (L1)	Exchange admin center	Audit	Ensure 'AuditBypassEnabled' is not enabled on mailboxes (Manual)	VALIDATE	MED
6.2.1 (L1)	Exchange admin center	Mail flow	Ensure all forms of mail forwarding are blocked and/or disabled (Automated)	NO	MED-HIGH
6.2.2 (L1)	Exchange admin center	Mail flow	Ensure mail transport rules do not whitelist specific domains (Automated)	YES	MED-HIGH
6.2.3 (L1)	Exchange admin center	Mail flow	Ensure email from external senders is identified (Automated)	VALIDATE	MED
6.3.1 (L2)	Exchange admin center	Roles	Ensure users installing Outlook add-ins is not allowed (Automated)	VALIDATE	MED
6.4.1 (L1)	Exchange admin center	Reports	Ensure mail forwarding rules are reviewed at least weekly (Manual)	PERIODIC WEEKLY	MED
6.5.1 (L1)	Exchange admin center	Settings	Ensure modern authentication for Exchange Online is enabled (Automated)	VALIDATE	MED-HIGH
6.5.2 (L2)	Exchange admin center	Settings	Ensure MailTips are enabled for end users (Automated)	VALIDATE	MED

CIS ref	Section	Subsection	Task	In place	Criticality
6.5.3 (L2)	Exchange admin center	Settings	Ensure additional storage providers are restricted in Outlook on the web (Automated)	VALIDATE	MED
7.2.1 (L1)	SharePoint admin center	Policies	Ensure modern authentication for SharePoint applications is required (Automated)	NO	MED-HIGH
7.2.2 (L1)	SharePoint admin center	Policies	Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled (Automated)	VALIDATE	MED
7.2.3 (L1)	SharePoint admin center	Policies	Ensure external content sharing is restricted (Automated)	YES	MED-HIGH
7.2.4 (L2)	SharePoint admin center	Policies	Ensure OneDrive content sharing is restricted (Automated)	NO	MED-HIGH
7.2.5 (L2)	SharePoint admin center	Policies	Ensure that SharePoint guest users cannot share items they don't own (Automated)	YES	MED-HIGH
7.2.6 (L2)	SharePoint admin center	Policies	Ensure SharePoint external sharing is managed through domain whitelist/blacklists (Automated)	NO	MED-HIGH
7.2.7 (L1)	SharePoint admin center	Policies	Ensure link sharing is restricted in SharePoint and OneDrive (Automated)	NO	MED-HIGH
7.2.8 (L2)	SharePoint admin center	Policies	Ensure external sharing is restricted by security group (Manual)	NO	MED-HIGH
7.2.9 (L1)	SharePoint admin center	Policies	Ensure guest access to a site or OneDrive will expire automatically (Automated)	NO	MED
7.2.10 (L1)	SharePoint admin center	Policies	Ensure reauthentication with verification code is restricted (Automated)	NO	MED-HIGH
7.3.1 (L2)	SharePoint admin center	Settings	Ensure Office 365 SharePoint infected files are disallowed for download (Automated)	VALIDATE	MED-HIGH
7.3.2 (L2)	SharePoint admin center	Settings	Ensure OneDrive sync is restricted for unmanaged devices (Automated)	NO	MED





CIS ref	Section	Subsection	Task	In place	Criticality
7.3.3 (L1)	SharePoint admin center	Settings	Ensure custom script execution is restricted on personal sites (Manual)	VALIDATE	MED-HIGH
7.3.4 (L1)	SharePoint admin center	Settings	Ensure custom script execution is restricted on site collections (Automated)	VALIDATE	MED-HIGH
8.1.1 (L2)	Microsoft Teams admin center	Teams	Ensure external file sharing in Teams is enabled for only approved cloud storage services (Automated)	NO	MED-HIGH
8.1.2 (L1)	Teams admin center	Teams	Ensure users can't send emails to a channel email address (Automated)	NO	MED
8.2.1 (L1)	Microsoft Teams admin center	Users	Ensure 'external access' is restricted in the Teams admin center (Automated)	NO	MED-HIGH
8.4.1 (L1)	Microsoft Teams admin center	Teams apps	Ensure app permission policies are configured (Manual)	VALIDATE	MED
8.5.1 (L2)	Microsoft Teams admin center	Meetings	Ensure anonymous users can't join a meeting (Automated)	NO	MED-HIGH
8.5.2 (L1)	Microsoft Teams admin center	Meetings	Ensure anonymous users and dial-in callers can't start a meeting (Automated)	YES	MED-HIGH
8.5.3 (L1)	Microsoft Teams admin center	Meetings	Ensure only people in my org can bypass the lobby (Automated)	NO	MED-HIGH
8.5.4 (L1)	Microsoft Teams admin center	Meetings	Ensure users dialing in can't bypass the lobby (Automated)	YES	MED-HIGH
8.5.5 (L2)	Microsoft Teams admin center	Meetings	Ensure meeting chat does not allow anonymous users (Automated)	NO	MED-HIGH

CIS ref	Section	Subsection	Task	In place	Criticality
8.5.6 (L2)	Microsoft Teams admin center	Meetings	Ensure only organizers and co-organizers can present (Automated)	NO	MED
8.5.7 (L1)	Microsoft Teams admin center	Meetings	Ensure external participants can't give or request control (Automated)	YES	MED
8.6.1 (L1)	Microsoft Teams admin center	Messaging	Ensure users can report security concerns in Teams (Automated)	NO	MED

Table 7 – Office 365 CIS control audit results





Appendix I Azure CIS controls



CIS_Microsoft_Azure
Foundations_Benc

About WhiteRook Cyber

WhiteRook Cyber is an Australian Cyber Security organisation changing the approach to supporting clients in building digital resilience and cyber security capability through offerings that include Awareness, Advisory, Leadership and Training.

Our purpose is to simplify cyber security and increase security awareness and resilience, enabling organisations to focus on their core business.

Our focus is on understanding cyber security vulnerabilities and gaps within your environment, across business, people, processes, and technology. Linking the cyber risks to your business risks, while translating and clarifying the issues associated with your cyber security technical requirements for leaders and managers within your business to better understand.

We do this by assisting organisations to increase their security maturity and ongoing digital resilience, through cyber security professional service and solutions, embedded with enablement and upskilling.

For more information on our cyber security programs, services, and solutions, please contact us at:

info@whiterookcyber.com.au

