FOCUSNET TECHNOLOGY

CIS Center for Internet Security®

Certified System Quality ISO 9001

Certified System Information Security ISO 27001

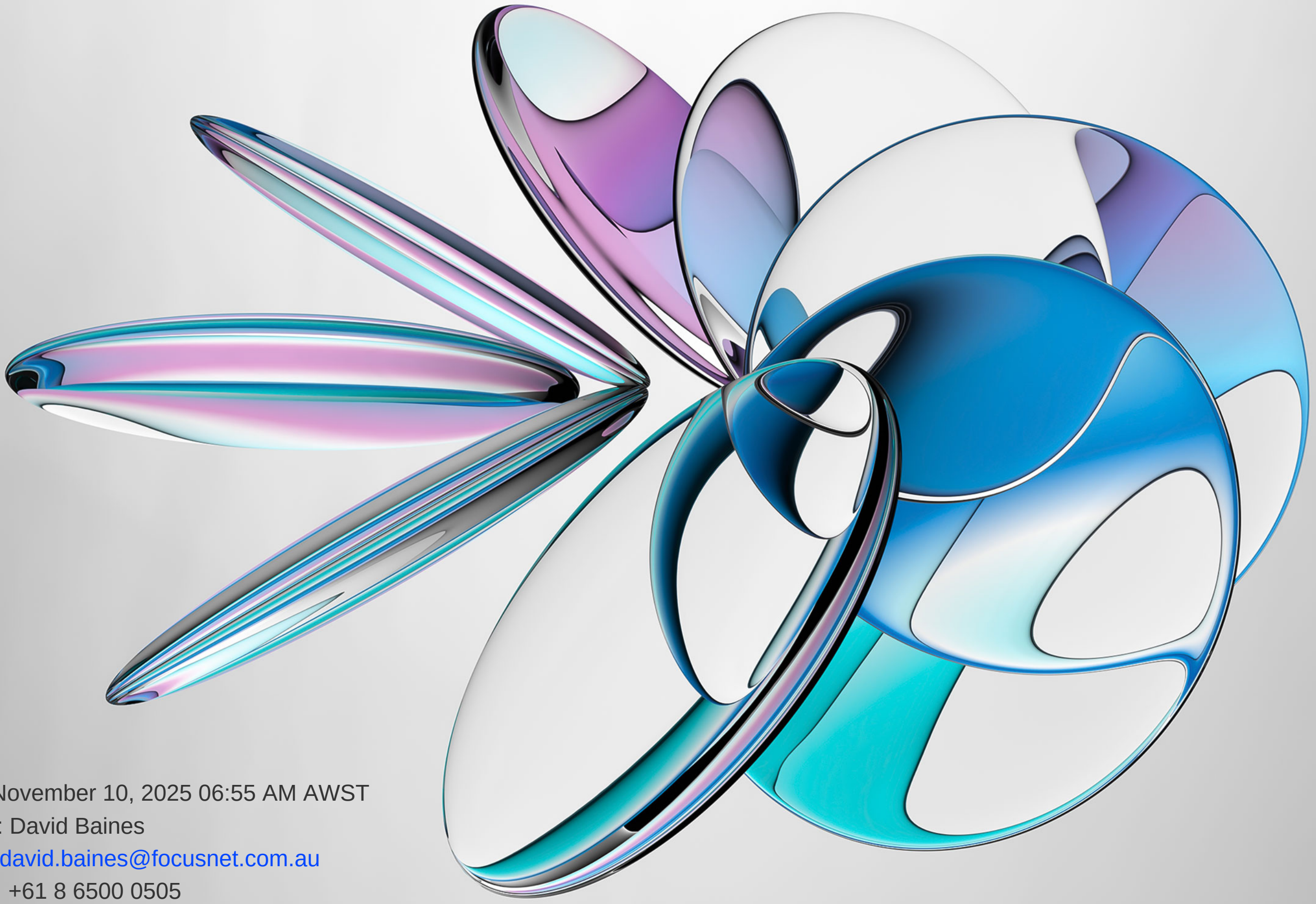
OFFENSIVE security OSCP

OFFENSIVE security OSEP

CIS M365 Benchmark Security Assessment

NoOneInParticular

Completed: November 10, 2025



Date: November 10, 2025 06:55 AM AWST
Author: David Baines
Email: david.baines@focusnet.com.au
Phone: +61 8 6500 0505

Executive Overview

This report provides a comprehensive assessment of NoOneInParticular's Microsoft 365 security posture, focusing on the implementation status of essential security controls and configurations across your Microsoft 365 environment.

Area Implementation Status

▨ Exchange Admin Center 0%	🟩 Microsoft Purview 100%	🟥 MS 365 Admin Center 33%
🟨 MS 365 Defender 63%	🟥 MS Admin Center 33%	🟥 MS Entra Admin Center 33%
🟥 MS Fabric 44%	🟥 MS Teams Admin Center 44%	🟨 Sharepoint Admin Center 67%
🟩 Teams & Groups 100%		

Coverage Overview

This grid shows the implementation status across all Microsoft 365 security areas. Red tiles indicate areas needing immediate attention (0-33%), yellow tiles show areas with moderate progress (34-74%), and green tiles represent well-implemented areas (75-100%).
Grey tiles indicate that the section has been administratively disabled and is not applicable to your environment.

CIS Microsoft 365 Benchmark

The CIS Microsoft 365 Benchmark is an internationally respected standard that offers clear, actionable guidance for securing Microsoft 365 environments. For Australian small and medium-sized enterprises (SMEs), adopting this benchmark is particularly valuable. It assists businesses in ensuring that critical security measures—such as account safeguarding, access controls, and threat detection—are properly configured in accordance with global best practices. In the context of Australia's increasingly complex cybersecurity landscape, following the CIS Benchmark helps SMEs strengthen their security posture, minimise their risk of cyber incidents, and meet the growing expectations for data protection and regulatory compliance. Aligning with this framework not only supports operational resilience but also demonstrates a proactive commitment to safeguarding client information and business assets—an essential factor in maintaining trust and fulfilling obligations under Australian standards such as the Australian Privacy Act and the Security of Critical Infrastructure reforms.

Assessment Methodology

Our assessment evaluates your Microsoft 365 environment across these key security domains:

- Identity and Access Management: Authentication methods and privilege management
- Data Protection: Classification, retention policies, and protection measures
- Threat Protection: Security monitoring and incident response capabilities
- Application Security: Permissions and endpoint protection configurations

Key Findings

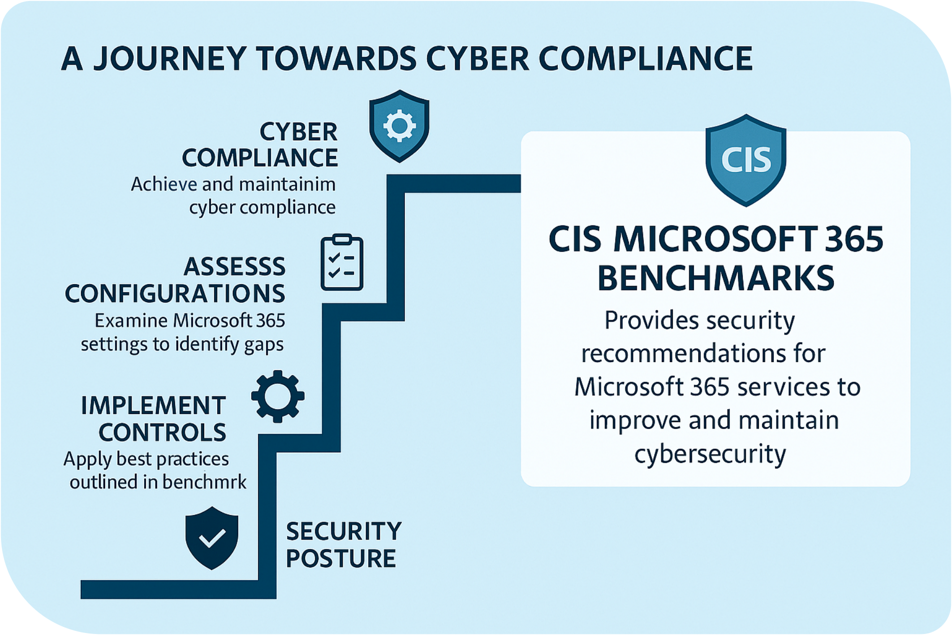
- Current implementation status across all control areas
- Priority-based analysis of security measures
- Identified areas requiring immediate attention
- Progress tracking against security objectives

How to Use This Report

This report is structured to provide a clear understanding of your Microsoft 365 security posture:

- Strategy Overview: Begin with the radar chart and implementation grid for a high-level view of your security status
- Priority Focus: Review the critical, high, medium, and low priority sections to understand implementation priorities
- Detailed Controls: Examine individual control sections for specific implementation details and recommendations
- Progress Tracking: Use the charts and metrics throughout to track your security journey

Your Progress



A JOURNEY TOWARDS CYBER COMPLIANCE

CYBER COMPLIANCE
Achieve and maintainim cyber compliance

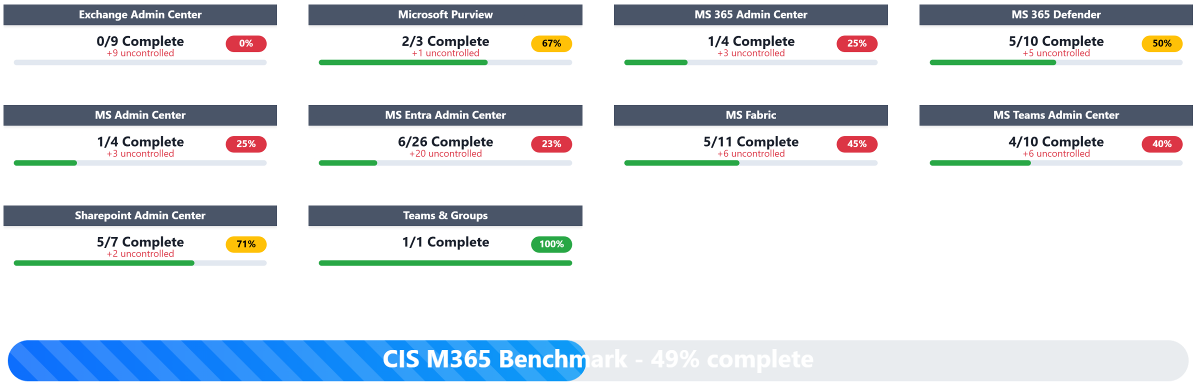
ASSESSS CONFIGURATIONS
Examine Microsoft 365 settings to identify gaps

IMPLEMENT CONTROLS
Apply best practices outlined in benchmrk

SECURITY POSTURE

CIS MICROSOFT 365 BENCHMARKS
Provides security recommendations for Microsoft 365 services to improve and maintain cybersecurity

Overall Progress to date



Exchange Admin Center
0/9 Complete 0%
+9 uncontrolled

Microsoft Purview
2/3 Complete 67%
+1 uncontrolled

MS 365 Admin Center
1/4 Complete 25%
+3 uncontrolled

MS 365 Defender
5/10 Complete 50%
+5 uncontrolled

MS Admin Center
1/4 Complete 25%
+3 uncontrolled

MS Entra Admin Center
6/26 Complete 23%
+20 uncontrolled

MS Fabric
5/11 Complete 45%
+6 uncontrolled

MS Teams Admin Center
4/10 Complete 40%
+6 uncontrolled

Sharepoint Admin Center
5/7 Complete 71%
+2 uncontrolled

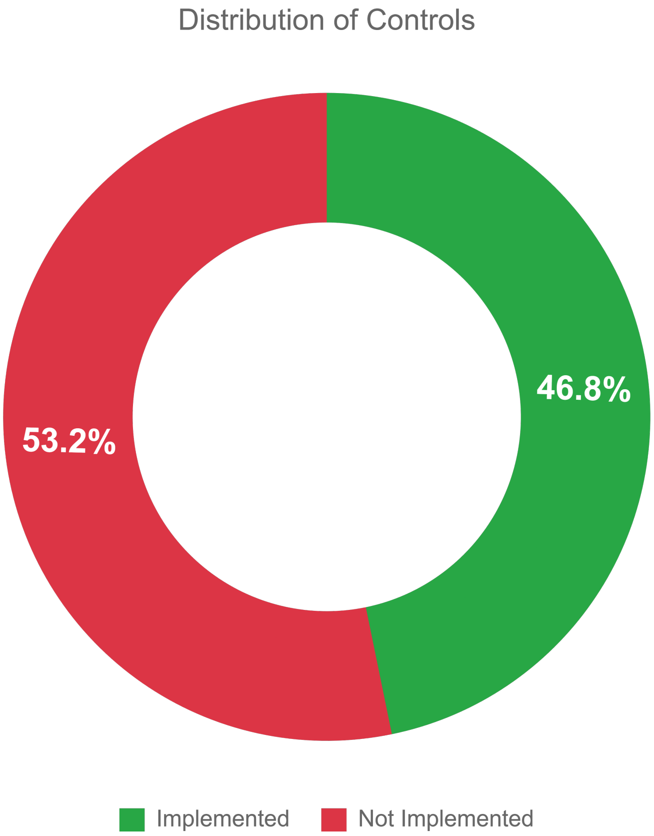
Teams & Groups
1/1 Complete 100%

CIS M365 Benchmark - 49% complete

Your CIS Microsoft 365 Benchmarks implementation is currently at **49%**, with 26 of 53 active controls in place. This reflects a strong foundation and a clear commitment to improving your Microsoft 365 security posture. While reaching 100% implementation is ideal, it's understood that in many environments—especially within Australian SMEs—some controls may not be practical or immediately applicable. Instead, the focus should be on progressive improvement, targeting the highest priority items first, particularly those that reduce exposure to known threats like phishing, unauthorized access, and data leakage. Continuing to align with the CIS Benchmark, even incrementally, helps ensure your Microsoft 365 environment remains secure, resilient, and defensible—while also supporting alignment with broader frameworks like the ACSC Essential Eight.

Your security strategy is taking solid shape. Keep refining and improving.

Control Management Insights



Implemented – controls that are properly configured and maintained.
Not Implemented – controls that require attention.

Current Status

- 49.1% complete - (26 of 53 active controls)
- 50.9% pending - (27 of 53 active controls)

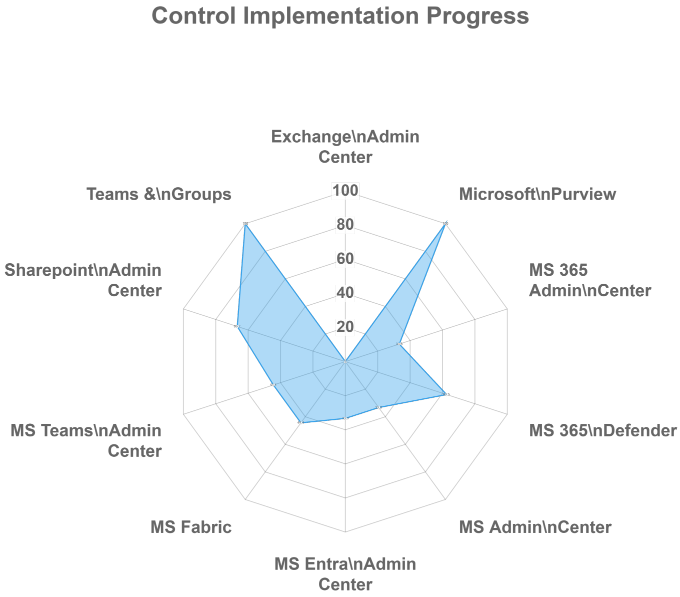
Next Steps

- Complete validation of controls
- Prioritize critical controls
- Schedule pending assessments

The doughnut chart illustrates that 49.1% of your active Microsoft 365 security controls are properly implemented, while 50.9% require attention. This balanced view shows both your security achievements and areas needing focus. With 26 controls already configured and maintained, your organization has established a solid foundation for cyber defense.

To strengthen your security posture, focus on implementing the remaining 27 active controls. These unimplemented controls may represent critical security gaps that could be exploited. Prioritize implementation based on control criticality and potential impact on your overall security framework. Regular assessment and validation of both implemented and pending controls will ensure continuous improvement of your Microsoft 365 security environment.

Strategy Overview



Key Insights

- Strong performance in Teams & Groups (100%) shows robust security implementation
- Sharepoint Admin Center (71%), Microsoft Purview (67%), MS 365 Defender (50%) show good progress, building a solid foundation
- Critical areas needing attention include MS Fabric (45%), MS Teams Admin Center (40%), MS 365 Admin Center (25%), MS Admin Center (25%), MS Entra Admin Center (23%)

Priority should be given to strengthening MS Entra Admin Center implementation (currently at 23%) to improve overall security posture.

Implementation Progress & Insights

Teams & Groups 100%
- The current security posture reflects a well-structured approach to risk management.

Sharepoint Admin Center 71%
- Implementation indicates systematic security development.

Microsoft Purview 67%
- Current status indicates ongoing security framework development.

MS 365 Defender 50%
- Implementation indicates steady security framework development.

MS Fabric 45%
- Implementation progress suggests need for structured development.

MS Teams Admin Center 40%
- Initial security implementation indicates areas for improvement.

MS 365 Admin Center 25%
- Security posture indicates potential for framework strengthening.

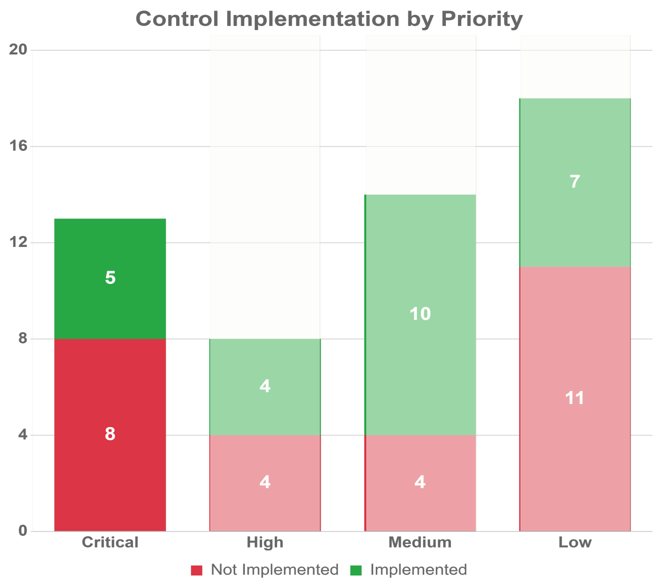
MS Admin Center 25%
- Current progress reflects areas needing security focus.

MS Entra Admin Center 23%
- Current status shows need for security framework development.

Exchange Admin Center 0%
- Security posture shows potential for systematic development.

Priority Focus - CRITICAL

Control Implementation by Priority



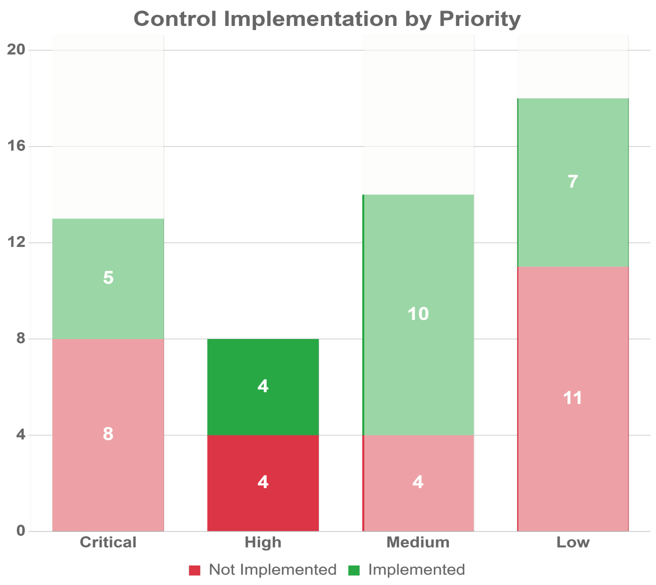
Critical Priority Classification

Critical controls represent the most essential security measures that require immediate attention. These controls directly impact core security functions and pose significant risks if not implemented. Implementation of critical controls should be prioritized to establish fundamental security baselines.

Control	Benchmark	Status
1.1.1	Ensure Administrative accounts are cloud-only	**Implemented**
2.1.9	Ensure that DKIM is enabled for all Exchange Online Domains	**Implemented**
5.1.2.4	Ensure access to the Entra admin center is restricted	**Implemented**
5.2.2.1	Ensure multifactor authentication is enabled for all users in administrative roles	**Implemented**
5.2.2.3	Enable Conditional Access policies to block legacy authentication	**Implemented**
1.1.2	Ensure two emergency access accounts have been defined	**Not Implemented**
1.1.3	Ensure that between two and four global admins are designated	**Not Implemented**
2.1.10	Ensure DMARC Records for all Exchange Online domains are published	**Not Implemented**
2.1.2	Ensure the Common Attachment Types Filter is enabled	**Not Implemented**
2.1.8	Ensure that SPF records are published for all Exchange Domains	**Not Implemented**
5.1.2.1	Ensure 'Per-user MFA' is disabled	**Not Implemented**
5.2.2.4	Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	**Not Implemented**
5.2.3.1	Ensure Microsoft Authenticator is configured to protect against MFA fatigue	**Not Implemented**

Priority Focus - HIGH

Control Implementation by Priority



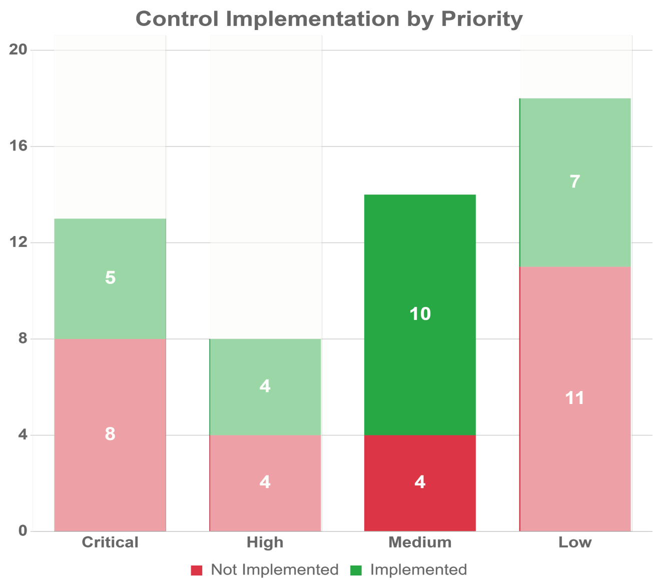
High Priority Classification

High priority controls represent important security measures that significantly contribute to your security posture. While not as urgent as critical controls, these measures play a vital role in maintaining robust security. Implementation of high priority controls should be addressed after critical controls are in place.

Control	Benchmark	Status
1.3.1	Ensure the 'Password expiration policy' is set to 'Set passwords to never expire	**Implemented**
2.1.3	Ensure notifications for internal users sending malware is Enabled	**Implemented**
3.2.1	Ensure DLP policies are enabled	**Implemented**
5.2.3.5	Ensure weak authentication methods are disabled	**Implemented**
5.1.3.1	Ensure a dynamic group for guest users is created	**Not Implemented**
5.1.5.2	Ensure the admin consent workflow is enabled	**Not Implemented**
5.2.3.3	Ensure password protection is enabled for on-prem Active Directory	**Not Implemented**
5.2.4.1	Ensure 'Self service password reset enabled' is set to 'All'	**Not Implemented**

Priority Focus - MEDIUM

Control Implementation by Priority



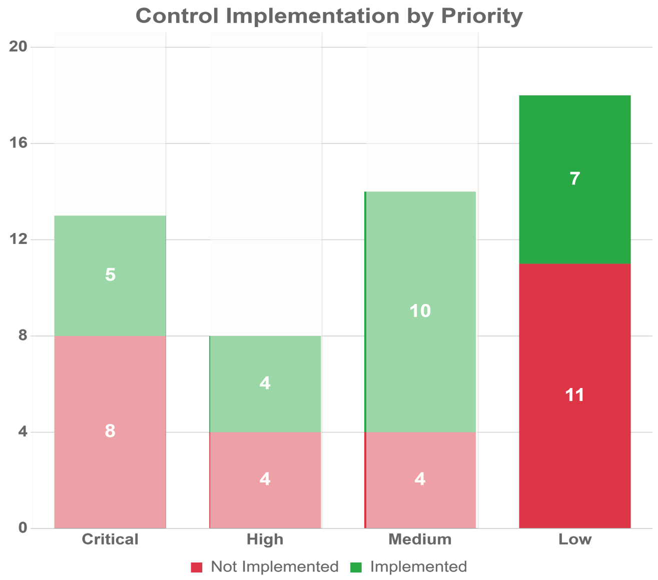
Medium Priority Classification

Medium priority controls represent important security measures that enhance your overall security posture. While not as urgent as critical or high priority controls, these measures provide additional layers of protection. Implementation of medium priority controls should be addressed after critical and high priority controls are in place.

Control	Benchmark	Status
2.1.13	Ensure the connection filter safe list is of	**Implemented**
2.1.14	Ensure inbound anti-spam policies do not contain allowed domains	**Implemented**
2.1.6	Ensure Exchange Online Spam Policies are set to notify administrators	**Implemented**
3.3.1	Ensure Information Protection sensitivity label policies are published	**Implemented**
7.2.1	Ensure modern authentication for SharePoint applications is required	**Implemented**
7.2.9	Ensure guest access to a site or OneDrive will expire automatically	**Implemented**
8.2.3	Ensure external Teams users cannot initiate conversations	**Implemented**
8.2.4	Ensure the organization cannot communicate with accounts in trial Teams tenants	**Implemented**
8.5.3	Ensure only people in my org can bypass the lobby	**Implemented**
8.5.4	Ensure users dialing in can't bypass the lobby	**Implemented**
5.1.2.3	Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes'	**Not Implemented**
7.2.11	Ensure the SharePoint default sharing link permission is set	**Not Implemented**
7.2.7	Ensure link sharing is restricted in SharePoint and OneDrive	**Not Implemented**
8.2.2	Ensure communication with unmanaged Teams users is disabled	**Not Implemented**

Priority Focus - LOW

Control Implementation by Priority



Low Priority Classification

Low priority controls represent supplementary security measures that further enhance your security posture. While these controls add value, they should be implemented after critical, high, and medium priority controls are in place. Implementation of low priority controls helps achieve a comprehensive security framework.

Control	Benchmark	Status
1.2.2	Ensure sign-in to shared mailboxes is blocked	**Implemented**
7.2.10	Ensure reauthentication with verification code is restricted	**Implemented**
7.2.2	Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled	**Implemented**
9.1.10	Ensure access to APIs by service principals is restricted	**Implemented**
9.1.3	Ensure guest access to content is restricted	**Implemented**
9.1.4	Ensure 'Publish to web' is restricted	**Implemented**
9.1.9	Ensure 'Block ResourceKey Authentication' is 'Enabled'	**Implemented**
1.3.4	Ensure 'User owned apps and services' is restricted	**Not Implemented**
1.3.5	Ensure internal phishing protection for Forms is enabled	**Not Implemented**
8.1.2	Ensure users can't send emails to a channel email address	**Not Implemented**
8.4.1	Ensure app permission policies are configured	**Not Implemented**
8.5.7	Ensure external participants can't give or request control	**Not Implemented**
8.6.1	Ensure users can report security concerns in Teams	**Not Implemented**
9.1.11	Ensure service principals cannot create and use profiles	**Not Implemented**
9.1.2	Ensure external user invitations are restricted	**Not Implemented**
9.1.6	Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled'	**Not Implemented**
9.1.7	Ensure shareable links are restricted	**Not Implemented**
9.1.8	Ensure enabling of external data sharing is restricted	**Not Implemented**

Your Controls

The following pages provide a detailed breakdown of your security controls across different Microsoft 365 services. Each section presents the current implementation status of controls specific to that service, helping you understand your security posture and identify areas that need attention.

Understanding the Control Tables

- **Priority:** Indicates the relative importance of each control (lower numbers = higher priority)
- **Control ID:** Unique identifier for each security control
- **Benchmark:** Description of the security requirement or standard being measured
- **Status:** Current implementation status (Implemented/Not Implemented)

Exchange Admin Center

0/9 Complete 0%

+9 uncontrolled

Exchange Admin Center

The Exchange Admin Center is crucial for managing email security and compliance in Microsoft 365. It provides controls for configuring email authentication, anti-spam policies, mailbox permissions, and other essential email security features. Proper configuration of these controls helps protect against email-based threats, unauthorized access, and data leakage through email channels.

Priority	Control ID	Benchmark	Status
20	6.5.4	Ensure SMTP AUTH is disabled	Inactive
32	6.2.1	Ensure all forms of mail forwarding are blocked and/or disabled	Inactive
33	6.2.2	Ensure mail transport rules do not whitelist specific domains	Inactive
34	6.2.3	Ensure email from external senders is identified	Inactive
35	6.5.1	Ensure email from external senders is identified	Inactive
36	6.5.2	Ensure MailTips are enabled for end users	Inactive
52	6.1.1	Ensure 'AuditDisabled' organizationally is set to 'False'	Inactive
53	6.1.2	Ensure mailbox audit actions are configured	Inactive
54	6.1.3	Ensure 'AuditBypassEnabled' is not enabled on mailboxes	Inactive

Information Protection Progress Card

Information Protection

Microsoft Information Protection is essential for safeguarding sensitive data across your Microsoft 365 environment. It provides comprehensive controls for data classification, labeling, and protection policies that help prevent data leakage and unauthorized access. These controls are crucial for maintaining data security and compliance with data protection regulations, ensuring that sensitive information remains protected wherever it resides or travels within your organization.

Priority	Control ID	Benchmark	Status

Microsoft 365 Admin Center Progress Card

Microsoft 365 Admin Center

The Microsoft 365 Admin Center serves as the central hub for managing your organization's Microsoft 365 environment. It provides essential controls for user management, license assignment, security settings, and organizational policies. Proper configuration of these controls is fundamental to maintaining a secure and well-managed Microsoft 365 tenant, ensuring that your organization's resources are protected and efficiently managed.

Priority	Control ID	Benchmark	Status

Microsoft 365 Defender Progress Card

Microsoft 365 Defender

Microsoft 365 Defender provides advanced threat protection across your digital estate. It combines security controls for endpoint protection, email security, identity monitoring, and threat detection. These controls are vital for defending against sophisticated cyber threats, including malware, phishing, and advanced persistent threats, providing comprehensive security coverage for your Microsoft 365 environment.

Priority	Control ID	Benchmark	Status

Microsoft Entra Admin Center Progress Card

Microsoft Entra Admin Center

Microsoft Entra Admin Center (formerly Azure AD) is the cornerstone of identity and access management. It provides essential controls for managing user identities, authentication methods, conditional access policies, and privileged identity management. These controls are fundamental to implementing a Zero Trust security model, ensuring that only authorized users can access your organization's resources.

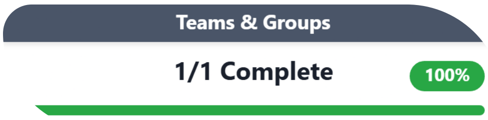
Priority	Control ID	Benchmark	Status

Microsoft Fabric Progress Card

Microsoft Fabric

Microsoft Fabric provides a unified analytics platform for your organization's data needs. It includes essential controls for data governance, security, and compliance across your analytics infrastructure. These controls ensure that your data assets are properly protected while remaining accessible for business intelligence and analytics purposes, maintaining the balance between security and productivity.

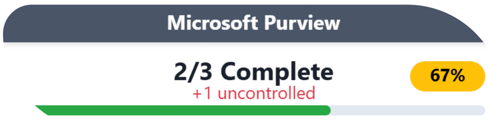
Priority	Control ID	Benchmark	Status



Teams and Groups

The Teams and Groups section focuses on security controls for Microsoft Teams and Microsoft 365 Groups. These controls ensure proper management of team creation, guest access, file sharing, and communication settings to maintain secure collaboration while protecting sensitive information.

Priority	Control ID	Benchmark	Status
67	1.2.2	Ensure sign-in to shared mailboxes is blocked	**Implemented**



Microsoft Purview

2/3 Complete

+1 uncontrolled

67%

Microsoft Purview

Microsoft Purview offers comprehensive data governance and compliance capabilities. It provides controls for data discovery, classification, and protection across your entire data estate. These controls are essential for maintaining regulatory compliance, protecting sensitive information, and ensuring proper data handling practices throughout your organization.

Priority	Control ID	Benchmark	Status
16	3.1.1	Ensure Microsoft 365 audit log search is Enabled	Inactive
17	3.2.1	Ensure DLP policies are enabled	**Implemented**
46	3.3.1	Ensure Information Protection sensitivity label policies are published	**Implemented**

Microsoft Teams Admin Center Progress Card

Teams Admin Center

The Microsoft Teams Admin Center provides essential controls for managing your Teams environment. It includes security settings for meetings, chat, file sharing, and external access configurations. These controls are crucial for ensuring secure collaboration while maintaining compliance with organizational policies and industry regulations.

Priority	Control ID	Benchmark	Status

Settings Progress Card

Settings

The Settings section contains critical security controls that form the foundation of your Microsoft 365 security posture. These controls include essential configurations for password policies, multi-factor authentication, and other fundamental security settings that protect your organization's data and user accounts.

Priority	Control ID	Benchmark	Status

System Progress Card

System

The System section encompasses core system-level security controls and configurations. These controls are essential for maintaining the overall security and integrity of your Microsoft 365 environment, including system updates, logging, and monitoring capabilities.

Priority	Control ID	Benchmark	Status

Executive Summary

This assessment of your Microsoft 365 environment reveals opportunities to enhance your security posture, with 49% of active controls implemented (26 out of 53 active controls). Your organization is at the beginning of its security journey, and this report provides a clear roadmap for improvement, starting with critical controls where currently 50% of high-priority measures are in place.

It's important to note that securing your Microsoft 365 environment is one crucial component of a comprehensive cybersecurity strategy. This assessment should be read in conjunction with your ACSC Essential Eight maturity assessment, as these frameworks complement each other in building a robust security posture. While this report focuses on Microsoft 365-specific controls, many of these measures directly support and align with Essential Eight strategies, particularly in areas such as:

- **Application Control:** Through Microsoft 365 Defender and Endpoint Manager integration
- **Patch Applications:** Via automated update policies and compliance monitoring
- **Multi-Factor Authentication:** Using Microsoft Entra ID (formerly Azure AD) security features
- **Backup Management:** Through Microsoft 365 backup and recovery capabilities

By implementing the controls outlined in this report alongside your Essential Eight maturity improvements, you're building a defense-in-depth approach that addresses both platform-specific and broader organizational security requirements. This integrated approach is particularly important for Australian organizations facing an evolving threat landscape.

To make implementation practical and achievable, we've organized the controls into three strategic tiers, aligned with your business context and the Australian cybersecurity landscape:

Critical Controls

These foundational controls provide maximum security impact with focused effort. They address the most prevalent cyber threats prioritizing the remaining high-impact measures will significantly strengthen your core Microsoft 365 security. Many of these controls directly support Essential Eight compliance, particularly for maturity level one requirements, providing dual benefits for your security investment.

Enhanced Controls

Building on critical protections, these controls provide comprehensive security coverage. Currently at 71% implementation, these measures strengthen your defense-in-depth strategy through advanced authentication, data protection, and threat detection capabilities. They complement Essential Eight maturity level two requirements, ensuring robust security across your Microsoft 365 environment. Implementation should follow after critical controls are addressed.

Advanced Controls

These controls optimize your Microsoft 365 security implementation. With 39% currently implemented, they represent longer-term objectives that should be addressed after establishing core security foundations . These measures help achieve a fully mature security posture aligned with industry best practices and support progression toward Essential Eight maturity level three, demonstrating your commitment to advanced cybersecurity capabilities.

Summary Recommendations

We understand that this comprehensive security assessment contains a significant amount of information that requires careful consideration and strategic planning to implement. To help you focus your immediate efforts and resources effectively, we have identified the five most critical areas that warrant priority attention.

Based on our assessment of your 49% implemented security controls, these recommendations have been carefully selected to provide the maximum impact on strengthening your cybersecurity posture. They represent the optimal balance of:

- Potential impact on reducing security risks
- Implementation effort and resource requirements
- Dependencies on other security controls
- Alignment with Australian cybersecurity guidelines

By focusing on these five key areas first, you will establish a strong foundation for your security program and create the necessary groundwork for implementing the remaining controls in a systematic and effective manner.

Priority	Control	Control ID	Class
1	Ensure that between two and four global admins are designated	1.1.3	General security
2	Ensure two emergency access accounts have been defined	1.1.2	General security
3	Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	5.2.2.4	General security
4	Ensure Microsoft Authenticator is configured to protect against MFA fatigue	5.2.3.1	General security
5	Ensure system-preferred multifactor authentication is enabled	5.2.3.6	General security

Appendix I: Complete Control List

This appendix provides a comprehensive list of all controls in the CIS Microsoft 365 Benchmark assessment, organized by priority (1 = Highest, 90 = Lowest). Each control's implementation status is indicated, providing a complete overview of your security posture. Controls are separated into active and inactive sections, with the inactive items being administratively disabled as they are not applicable to your environment.

Priority	Control ID	Benchmark	Status
1	5.2.2.1	Ensure multifactor authentication is enabled for all users in administrative roles	**Implemented**
2	1.1.3	Ensure that between two and four global admins are designated	**Not Implemented**
3	1.1.2	Ensure two emergency access accounts have been defined	**Not Implemented**
5	5.2.2.3	Enable Conditional Access policies to block legacy authentication	**Implemented**
6	1.1.1	Ensure Administrative accounts are cloud-only	**Implemented**
7	5.2.2.4	Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	**Not Implemented**
8	5.2.3.1	Ensure Microsoft Authenticator is configured to protect against MFA fatigue	**Not Implemented**
10	5.1.2.1	Ensure 'Per-user MFA' is disabled	**Not Implemented**
11	5.1.2.4	Ensure access to the Entra admin center is restricted	**Implemented**
12	2.1.8	Ensure that SPF records are published for all Exchange Domains	**Not Implemented**
13	2.1.9	Ensure that DKIM is enabled for all Exchange Online Domains	**Implemented**
14	2.1.10	Ensure DMARC Records for all Exchange Online domains are published	**Not Implemented**
15	2.1.2	Ensure the Common Attachment Types Filter is enabled	**Not Implemented**
17	3.2.1	Ensure DLP policies are enabled	**Implemented**
18	5.2.3.5	Ensure weak authentication methods are disabled	**Implemented**
23	5.1.3.1	Ensure a dynamic group for guest users is created	**Not Implemented**
24	5.1.5.2	Ensure the admin consent workflow is enabled	**Not Implemented**
25	5.2.4.1	Ensure 'Self service password reset enabled' is set to 'All'	**Not Implemented**
27	5.2.3.3	Ensure password protection is enabled for on-prem Active Directory	**Not Implemented**
28	1.3.1	Ensure the 'Password expiration policy' is set to 'Set passwords to never expire	**Implemented**
30	2.1.3	Ensure notifications for internal users sending malware is Enabled	**Implemented**
31	2.1.6	Ensure Exchange Online Spam Policies are set to notify administrators	**Implemented**
38	2.1.13	Ensure the connection filter safe list is of	**Implemented**
39	2.1.14	Ensure inbound anti-spam policies do not contain allowed domains	**Implemented**
41	7.2.1	Ensure modern authentication for SharePoint applications is required	**Implemented**
43	7.2.7	Ensure link sharing is restricted in SharePoint and OneDrive	**Not Implemented**
44	7.2.11	Ensure the SharePoint default sharing link permission is set	**Not Implemented**
45	7.2.9	Ensure guest access to a site or OneDrive will expire automatically	**Implemented**
46	3.3.1	Ensure Information Protection sensitivity label policies are published	**Implemented**
47	5.1.2.3	Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes'	**Not Implemented**
55	8.5.3	Ensure only people in my org can bypass the lobby	**Implemented**
56	8.5.4	Ensure users dialing in can't bypass the lobby	**Implemented**
58	8.2.2	Ensure communication with unmanaged Teams users is disabled	**Not Implemented**
59	8.2.3	Ensure external Teams users cannot initiate conversations	**Implemented**
60	8.2.4	Ensure the organization cannot communicate with accounts in trial Teams tenants	**Implemented**

Priority	Control ID	Benchmark	Status
61	7.2.2	Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled	**Implemented**
62	8.5.7	Ensure external participants can't give or request control	**Not Implemented**
63	8.6.1	Ensure users can report security concerns in Teams	**Not Implemented**
64	8.4.1	Ensure app permission policies are configured	**Not Implemented**
65	8.1.2	Ensure users can't send emails to a channel email address	**Not Implemented**
67	1.2.2	Ensure sign-in to shared mailboxes is blocked	**Implemented**
68	1.3.4	Ensure 'User owned apps and services' is restricted	**Not Implemented**
69	1.3.5	Ensure internal phishing protection for Forms is enabled	**Not Implemented**
73	7.2.10	Ensure reauthentication with verification code is restricted	**Implemented**
76	9.1.2	Ensure external user invitations are restricted	**Not Implemented**
77	9.1.3	Ensure guest access to content is restricted	**Implemented**
78	9.1.4	Ensure 'Publish to web' is restricted	**Implemented**
79	9.1.6	Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled'	**Not Implemented**
80	9.1.7	Ensure shareable links are restricted	**Not Implemented**
81	9.1.8	Ensure enabling of external data sharing is restricted	**Not Implemented**
82	9.1.9	Ensure 'Block ResourceKey Authentication' is 'Enabled'	**Implemented**
83	9.1.10	Ensure access to APIs by service principals is restricted	**Implemented**
84	9.1.11	Ensure service principals cannot create and use profiles	**Not Implemented**
		INACTIVE CONTROLS	
4	5.2.3.4	Ensure all member users are 'MFA capable'	Inactive
9	5.2.3.6	Ensure system-preferred multifactor authentication is enabled	Inactive
16	3.1.1	Ensure Microsoft 365 audit log search is Enabled	Inactive
19	5.2.2.9	Ensure a managed device is required for authentication	Inactive
20	6.5.4	Ensure SMTP AUTH is disabled	Inactive
21	5.2.2.12	Ensure the device code sign-in flow is blocked	Inactive
22	5.1.6.2	Ensure that guest user access is restricted	Inactive
26	5.2.3.2	Ensure custom banned passwords lists are used	Inactive
29	5.1.8.1	Ensure that password hash sync is enabled for hybrid deployments	Inactive
32	6.2.1	Ensure all forms of mail forwarding are blocked and/or disabled	Inactive
33	6.2.2	Ensure mail transport rules do not whitelist specific domains	Inactive
34	6.2.3	Ensure email from external senders is identified	Inactive
35	6.5.1	Ensure email from external senders is identified	Inactive
36	6.5.2	Ensure MailTips are enabled for end users	Inactive
37	2.1.12	Ensure the connection filter IP allow list is not used	Inactive
40	2.1.15	Ensure outbound anti-spam message limits are in place	Inactive

Priority	Control ID	Benchmark	Status
42	7.2.3	Ensure external content sharing is restricted	Inactive
48	5.1.3.2	Ensure users cannot create security groups	Inactive
49	5.1.4.2	Ensure the maximum number of devices per user is limited	Inactive
50	5.2.2.10	Ensure a managed device is required to register security information	Inactive
51	5.2.2.11	Ensure sign-in frequency for Intune Enrollment is set to 'Every time'	Inactive
52	6.1.1	Ensure 'AuditDisabled' organizationally is set to 'False'	Inactive
53	6.1.2	Ensure mailbox audit actions are configured	Inactive
54	6.1.3	Ensure 'AuditBypassEnabled' is not enabled on mailboxes	Inactive
57	8.5.2	Ensure anonymous users and dial-in callers can't start a meeting	Inactive
66	1.1.4	Ensure administrative accounts use licenses with a reduced application footprint	Inactive
70	5.1.4.5	Ensure Local Administrator Password Solution is enabled	Inactive
71	5.1.4.4	Ensure local administrator assignment is limited during Entra join	Inactive
72	5.1.4.3	Ensure the GA role is not added as a local administrator during Entra join	Inactive
74	1.3.9	Ensure shared bookings paged are restricted to select users	Inactive
75	9.1.1	Ensure guest user access is restricted	Inactive
85	9.1.12	Ensure service principals ability to create workspaces	Inactive