CyberByte SECURITY

CHECKLIST

ASD Essentials Phase 1 Checklist for Microsoft 365

On 15 October 2026 the Australian Signals Directorate (ASD) published ASD Essentials, the framework gradually taking over from the Essential Eight. This checklist covers the four domains to start with: priority phase 1 (Boundary and Identity services) plus the two that apply across every phase.

How to use this. Each section lists selected, plain-English checks based on the outcomes ASD Essentials describes for these four domains, applied to Microsoft 365. It isn't ASD's full list of actions, an ASD Essentials assessment or a rating. Mark "Yes" only where you've seen evidence, such as a report or a setting, across all your users and systems. The Essential Eight still applies during the transition, and ASD hasn't set an end date.

Sources: ASD Essentials for enterprise IT, ASD Essentials for cloud and Transitioning from the Essential Eight, cyber.gov.au. Checked 25 October 2026.

Start here: your chapter and scope

CHAPTER ☐ Cloud ☐ Enterprise IT

Only software or platform services (Microsoft 365, Xero, a hosted CRM), no servers or VMs? Start with ASD's Essentials for cloud. Own servers, VMs (even in Azure) or office network? Start with Essentials for enterprise IT.

Tenants and systems in scope _____ IT provider _____ Completed by _____ Date _____

MARK EACH ITEM ☐ **Yes** everywhere in scope, evidence seen ☐ **Partly** some users or systems only ☐ **No** not in place ☐ **Unsure** not checked yet

Log each Partly, No and Unsure in section 05. Tip: print it or annotate it; the boxes aren't form fields.

01 Governance and culture

Leadership, AI, suppliers and people. Runs across every phase.

	Yes	Partly	No	Unsure
A named executive is accountable for cyber risk, the board has agreed a risk appetite, and cyber is reported to the board at least twice a year.	☐	☐	☐	☐
Someone is accountable for AI use, and staff have written rules for Copilot, ChatGPT and AI features in your other systems.	☐	☐	☐	☐
You keep a list of suppliers that hold your data or run your systems (including your IT provider), and you check their security before signing and at least yearly.	☐	☐	☐	☐
Your contract with your IT provider says who looks after which Microsoft 365 security settings, and how they report on them.	☐	☐	☐	☐
Old or unsupported systems are listed, with an owner and a plan to replace or contain them.	☐	☐	☐	☐
All staff have had security awareness training in the last 12 months, including how to spot and report phishing.	☐	☐	☐	☐

Why it matters New since the Essential Eight: leadership, not IT, owns cyber risk, including AI and suppliers.

© 2026 CyberByte Pty Ltd · ABN 57 637 580 646

02 Visibility and response

Know what you have, see what happens, respond well. Runs across every phase.

	Yes	Partly	No	Unsure
You keep an up-to-date list of devices, accounts, apps and where important data lives (for example, devices enrolled in Intune).	☐	☐	☐	☐
The Microsoft 365 unified audit log is on, and sign-in and audit logs are kept long enough to investigate an incident.	☐	☐	☐	☐
Microsoft 365 and Defender alerts go to a named person or provider, and someone reviews them.	☐	☐	☐	☐
Files in SharePoint, OneDrive and Teams are checked for stored passwords, keys and other secrets.	☐	☐	☐	☐
You have a written incident response plan, have practised it in the last 12 months, and know your notification duties (including the OAIC Notifiable Data Breaches scheme).	☐	☐	☐	☐

`Why it matters` In ASD Essentials, you can't show a control works if you can't see it. Logging, alerting and a tested response plan sit beside every technical domain.

03 Boundary services

Everything you expose to the internet. Priority phase 1.

	Yes	Partly	No	Unsure
You know all your internet-facing services: domains, websites, remote access, Microsoft 365 and other cloud apps.	☐	☐	☐	☐
No remote desktop is exposed directly to the internet, and any remote access is protected by multi-factor authentication.	☐	☐	☐	☐
SPF, DKIM and DMARC are set up for your email domains, and Safe Links and Safe Attachments (or equivalent filtering) are on.	☐	☐	☐	☐
External sharing in SharePoint and OneDrive is limited, and “Anyone with the link” sharing isn’t the default.	☐	☐	☐	☐
Users can’t grant third-party apps access to your Microsoft 365 data without an admin approving it.	☐	☐	☐	☐

`Why it matters` ASD puts phase 1 first because these are common pathways for initial access. In Microsoft 365, many of these settings are off or permissive by default, and a default isn’t an effective control.

Three questions for your IT provider

01 Which of these can you show me evidence for today, across every user?

02 Which settings are still at Microsoft’s defaults, and why?

03 Who is responsible for each item: you, us or Microsoft?

© 2026 CyberByte Pty Ltd · ABN 57 637 580 646

04 Identity services

Accounts, sign-in and admin access. Priority phase 1.

	Yes	Partly	No	Unsure
Every user signs in with multi-factor authentication, enforced by Conditional Access or security defaults.	☐	☐	☐	☐
Everyone uses phishing-resistant sign-in (passkeys, FIDO2 security keys or Windows Hello for Business), admins first. SMS codes or app approvals are a gap.	☐	☐	☐	☐
Legacy authentication is blocked, and SMTP AUTH is off unless something genuinely needs it.	☐	☐	☐	☐
Global Administrators are kept to a small number of separate admin accounts that aren't used for email or browsing. Admin rights are time-bound where your licence allows (Privileged Identity Management).	☐	☐	☐	☐
Leavers', unused and guest accounts are removed promptly, and who has access to what is reviewed regularly.	☐	☐	☐	☐

`Why it matters` Identity is a common way into Microsoft 365. ASD Essentials looks for coverage (every account), consistency (applied the same way across them), currency (recent evidence) and evidence quality.

05 Gaps and unknowns

One line for each Partly, No or Unsure. Keep the evidence behind each Yes on file.

Item	Gap or question	Next step	Owner	Due date

NEXT STEP

Want an independent view of where you stand?

CyberByte's **ASD Essentials Readiness Snapshot** gives you a quick, evidence-based gap view of all four starting domains, a one-page summary for your board and a top-10 action list your IT provider can work from. We're independent: we check your IT provider's work, we don't sell it.

`From $4,500 ex GST · 1 week · credited in full against an ASD Essentials Assessment booked within 60 days`

Request a 20-minute scoping call →

hello@cyberbyte.au · 03 4422 2233 · Free Quick Check

General information only. It is not legal, insurance or professional advice, and it is not an ASD Essentials assessment, a rating or an assurance of compliance with any framework. CyberByte Security is not endorsed by ASD, and there is no ASD Essentials certification. Some Microsoft 365 changes can affect users, so plan them with whoever manages your tenant. Summarised as at 25 October 2026; check cyber.gov.au for changes.

SOURCES (CHECKED 25 OCTOBER 2026)

1. ASD, *ASD Essentials for enterprise IT* and *ASD Essentials for cloud*, October 2026: cyber.gov.au · cyber.gov.au
2. ASD, *Transitioning from the Essential Eight* and *Assessment process guide*, October 2026: cyber.gov.au · cyber.gov.au

© 2026 CyberByte Pty Ltd · ABN 57 637 580 646