

ASD Essentials

A practical guide for small business

Know who has access.

Prove you can recover the important work.

Prepared for small teams using email, cloud services, business websites and AI. Based on the ASD release of 15 October 2026.

This is A Dark Cloud Creative interpretation and a working guide. It does not provide certification or a formal assessment result.

SCOPE THE JOB

Decide what this review must answer

Choose a business problem before choosing a security product. You may need to recover from an account takeover, replace an unsupported computer, respond to a customer questionnaire or find out what your IT agreement includes. Write down that purpose and the services in scope.

List any contract, insurance condition or sector requirement separately. Keep meeting the obligations that currently apply. ASD has not given every small business a common Essentials migration deadline, and the release does not turn this worksheet into a certification process.

For a sole trader, the first review may cover one laptop, email and a domain. A larger team may need a formal assessment across several environments. A provider should explain why the proposed scope fits your operations.

Source guidance ASD frequently asked questions, The Essentials for senior executives

Choose the chapters that match your environment

The enterprise IT chapter is a useful starting point when you control servers, network architecture, operating systems or infrastructure hosted by someone else. The cloud chapter helps with SaaS and PaaS services where the security work is shared with a provider. The OT chapter addresses technology that monitors or controls physical processes.

Most small businesses have a mixture. Microsoft 365 can be part of the cloud review while the computers used to administer it need their own protection. A hosted website may leave its code, plugins, administrator accounts or recovery process under your control.

Make decisions using the actual responsibility, rather than the label on the invoice. Record the environments you included, anything excluded and why. A development system that can deploy to production or use production credentials belongs in the review too.

Source guidance Which chapter should I start with, Asset scoping guide for enterprise IT

UNDERSTAND THE STRUCTURE

Understand the domains without creating a new bureaucracy

For enterprise IT and cloud, two capabilities run throughout the work. Governance and culture covers accountability and the decisions that sustain security. Visibility and response covers the ability to notice and handle an incident.

The recommended technical sequence begins with boundary services and identity services. Critical processes and services, and privileged environments, follow. Business systems and user devices make up the later phase. The implementation phases are not maturity levels. A recorded risk or an existing obligation can justify a different sequence.

Use the domains to avoid gaps, rather than to duplicate a system eight times. One website can be externally exposed, commercially critical and administered through privileged accounts. A control can be implemented once while its relevant coverage is considered in each domain.

The OT sequence differs. Use its written chapter and matrix for an OT review, with the person responsible for safe operation involved in every proposed change.

Source guidance Essentials for enterprise IT, Essentials for OT, Essentials glossary

SERVICE OWNERSHIP

Make a record of what keeps you trading

Begin with the services that would stop you invoicing, taking bookings or serving customers. Record the business owner, technical administrator and recovery route for each one. Include the domain registrar and DNS, because losing the domain can affect more than the website.

Record important data separately from the app that stores it. A customer file, payroll export, API credential and automation account can need different access and recovery arrangements. Do not paste passwords, tokens or recovery codes into this record. Store those in an approved protected vault and record only the reference.

A useful service record contains the service name, the work it supports, owner, administrator, connected services, important data, sign in method, backup or export method and last review date. Note whether the account belongs to the business or a supplier.

For a cafe, this may include bookings and the roster alongside email. For a trade business it may include job management, quoting and the website enquiry route. Identify which service can wait and which one needs a usable fallback.

Source guidance [Asset scoping guide for cloud](#), [Asset scoping guide for enterprise IT](#)

PROTECT ACCESS

Close the obvious account and administration gaps

Review the list of current users against the people who should have access. Include contractors, supplier accounts, emergency accounts and apps that act without a person signing in. Remove or restrict access through an approved process, with recovery arrangements checked before a change.

Check who can grant permissions, create new administrators or alter sign in policies. Plan a dedicated, hardened administration environment separated from ordinary user work, with tightly limited privileges. Record any technical limitation and its agreed compensating controls. An ordinary browsing session should not become the place where all business accounts are administered.

Plan phishing resistant authentication where the service supports it. Check the chosen method, enforcement and alternative sign in routes. SMS or an approval prompt should not be described as equivalent to a phishing resistant method. Pilot changes with a recovery route available so that the owner is not locked out.

Keep evidence of the accounts reviewed, changes made and exceptions retained. An emergency access account needs a documented purpose, secure custody and monitoring. It should not quietly become the everyday administrator login.

Source guidance Implementing multi factor authentication, Assessment evidence guide for enterprise IT

KEEP THE RECORD

Keep the account review date and evidence of the changes made. Store recovery credentials in a protected vault.

CLOUD SERVICES

Review Microsoft 365 and Google Workspace as working systems

Start with the tenant owner and administrators, then examine how staff share information. Review public links, guest access and old project areas. Ask the data owner which external access is still needed before changing permissions across the business.

For Microsoft 365, include SharePoint and OneDrive locations, connected applications, Power Platform environments and automation owners where used. A Power Automate flow can be left without a valid owner when someone leaves, and connections tied to that person's account can fail. Review app ownership and connections before a person leaves. Teams Calling or other communications may need a fallback when internet access or the tenant is unavailable.

For Google Workspace, include shared drives, external sharing, connected applications and administrator access. Record devices that can hold business sessions or files. A personal phone can still be part of the access path even when the business does not manage it.

DLP can help detect or control sensitive information leaving through configured channels. Begin with the data types and routes you need to protect, test the policy and assign someone to investigate the alerts. A DLP subscription does not establish that coverage.

Check the current licence and service documentation before relying on audit logs, retention, authentication policies or a particular protection feature. Confirm what your agreement includes and where there are gaps. This guide does not assume every Microsoft 365 or Google Workspace plan supplies the same controls.

Source guidance Essentials for cloud, Asset scoping guide for cloud, Microsoft guidance on orphaned Power Automate flows, Microsoft guidance on data loss prevention, Google Workspace Drive log events

REPAIR AND MAINTAIN

Make vulnerability management a process that closes repairs

Keep an inventory of devices, applications and exposed services. Confirm their support status and who receives security advisories. A scanner report helps identify work, but the result you need is a repaired or deliberately mitigated problem.

Agree remediation times using exposure, exploitation, business criticality and the likely effect of a change. Existing mandatory or contractual times still apply. Track exceptions with an owner, compensating controls and a review date. Recheck the affected system after the repair.

For office equipment, automatic updates can be suitable when the expected operational impact is low. A line of business app may need a tested maintenance window and recovery plan. Do not transfer that routine directly to equipment controlling a physical process.

Useful evidence includes the assets covered, the findings, repair dates and verification results. If a device is unsupported, record the replacement plan and how it is protected in the meantime.

Source guidance Essentials for enterprise IT, Transitioning from the Essential Eight

KEEP THE RECORD

Close each repair with evidence. A finding that remains open needs an owner and a review date.

PROVE RECOVERY

Prove that you can recover important work

Choose one important service and describe the failure you need to recover from. Include accidental deletion, a compromised administrator and loss of access to the provider. Those scenarios can expose different weaknesses.

Agree how much work the business can afford to lose and how long it can be without the service. Those decisions become recovery point and recovery time objectives. Test a recovery method that can demonstrate those objectives for the service in question.

Check whether a compromised production account could alter or delete the backup. Use protected storage and an administration route that remains available when the primary identity environment is compromised. Include configuration and application settings when they are needed to restore the service.

A useful controlled test records what was restored, where it was restored, the date of the data and the time taken. Check the content and permissions, then record the gaps and repair them. Avoid overwriting live work just to prove that a backup exists.

Cloud availability, sync, retention and a backup can solve different problems. Ask the provider which deletion, account loss and recovery scenarios your arrangement covers. Record a gap instead of assuming the subscription handles it.

Source guidance Cloud computing security for tenants, Assessment evidence guide for enterprise IT

KEEP THE RECORD

Record the restore result and its gaps. Keep the evidence separate from the system you may need to recover.

WEBSITE AND INTEGRATIONS

Check the website and its connected services

Record who controls the domain, DNS, hosting, CMS and source code. Include the people who can deploy a change and the third party services used by forms, bookings or payments. Keep a current business controlled recovery route for each account.

Confirm which party patches the platform and which party maintains the application, theme, plugins or dependencies. Check unused administrators and integrations. A fully managed hosting invoice may still leave some of those jobs with your business.

Use a clearly labelled test enquiry to confirm the complete form route. Check validation, delivery and the handling of failed submissions. Confirm the enquiry does not end up only in a supplier's account. Test a restore in a safe environment when the website is important to trading.

Review access to preview sites and development tools when they can reach live data or deploy changes. Keep production credentials out of public code and ordinary project documents. Remove an exposed secret and rotate it through an approved process rather than assuming deletion is enough.

Source guidance Asset scoping guide for enterprise IT, Implementation planning guide

KEEP THE RECORD

Test the whole enquiry route and the recovery process. Record which party is responsible for each component.

AI AND AUTOMATION

Limit what AI agents and automations can do

Keep a register of approved AI tools and the business purpose for each one. Identify the information sent to the provider, who can retrieve it and the available retention and training settings. Obtain approval before using sensitive business data.

For an agent or automation, record its owner, connected systems, permissions and credentials. Start with the smallest access that supports the task. An agent that drafts a reply does not need permission to send it to every customer or change bank account details.

Test whether untrusted content can influence the agent's actions. Keep a human approval step for consequential changes and a way to stop the automation or revoke its access. Those limits should operate outside the prompt where possible.

Treat AI logs as potentially sensitive. Decide what must be recorded for investigation and how access and retention will be controlled. Avoid collecting full prompts and customer records into an unrestricted logging service. Recheck permissions and behaviour when a model, connector or workflow changes.

Source guidance AI considerations within the Essentials

KEEP THE RECORD

Keep consequential actions behind a permission or approval control that does not rely on the prompt.

DETECTION AND RESPONSE

Know who notices a problem and who responds

Choose the events that matter for the services in scope. Examples include an unexpected administrator, a new external connection or a suspicious sign in. Confirm those events can be recorded and that the alerts go to a monitored destination.

Ask who reviews them, during which hours and what happens when a serious alert arrives after hours. Keep the response promises realistic. An email alert in an unattended inbox does not provide a response service.

Write a short incident plan with the responsible person, supplier contacts and an alternative way to communicate if email is affected. Include the steps for preserving evidence and obtaining help. Identify applicable reporting duties and the person responsible for checking them rather than guessing a universal deadline.

Walk through an account takeover scenario with the people who would act. Can they reach the right support contact without the compromised inbox? Can they revoke sessions and preserve records? Record the missing access or information and arrange the repair.

Source guidance Assessment process guide, Security when engaging a managed service provider

KEEP THE RECORD

Practise reaching the support contact without the normal inbox. Record any access that would be missing during an incident.

AGREE THE WORK

Agree the work with your IT provider

Ask the provider to mark each responsibility as included, optional, held by your business or supplied by another party. Name the systems covered. Managed IT, managed security, monitoring and backup are service descriptions that need an agreed scope.

Request evidence relevant to your environment, such as account review records, patch coverage, restore results and the response process. Agree how supplier administrator access is granted, recorded and removed. Confirm what happens to accounts and information if you change providers.

If you are working towards SMB1001 or another standard, keep that assessment and its obligations explicit. A mapping can help reuse evidence, but it does not establish an automatic Essentials result or certification equivalence.

Finish with an action list that records the finding, affected service, proposed treatment, owner, due date and evidence needed to close it. Separate the assessment of the current outcome from the project status. A job marked underway has not necessarily reduced the risk yet.

Source guidance Security when engaging a managed service provider, Assessment process guide

KEEP THE RECORD

Agree the scope in writing and keep current evidence. Ask who is responsible for unfinished repairs.

A MANAGEABLE PLAN

An optional first 90 days

The following is an A Dark Cloud Creative planning example. It is not an ASD deadline or a substitute for responding to an urgent vulnerability. Set the pace around your risks and any existing obligations.

During the first month, establish ownership and recovery for critical accounts, record the important services and review exposed access and administrator privileges. Collect the available evidence and assign the urgent repairs.

During the next month, work through the agreed repairs and conduct a controlled restore test. Review sharing and application connections, then document the response arrangements with your provider.

During the third month, exercise the incident plan, check whether the repairs worked and review overdue exceptions. Agree the next scope and a recurring review date. Someone needs to own the work after the first project ends.

Source guidance Implementation planning guide

What this review should leave you with

You should have a service register, an access review, a tested recovery record and a prioritised action list. The record should say what was checked, what remains unknown and who will address each gap.

For a formal Essentials assessment, use ASD's assessment process and current evidence guidance with an appropriate assessor. Report unassessed work clearly and keep the detailed findings alongside any summary chart. This guide and its worksheets do not assign formal effectiveness ratings.

A Dark Cloud Creative can help scope the work in Perth or remotely across Australia. Send the service names and business impact through our contact form. Do not send passwords, recovery codes or API keys with an enquiry.

Source guidance Assessment process guide

WORKING RECORD

Service and responsibility record

Use this page in a private business record. Write references to protected evidence rather than passwords, API keys or recovery codes.

Service and business impact

Business owner and administrator

Provider and customer responsibilities

Recovery method and last test

Reviewed by _____ Date _____

WORKING RECORD

Remediation and exception record

Use this page in a private business record. Write references to protected evidence rather than passwords, API keys or recovery codes.

Finding and affected service

Treatment and evidence to close

Owner and due date

Exception approval and review date

Reviewed by _____ Date _____

WORKING RECORD

Recovery test record

Use this page in a private business record. Write references to protected evidence rather than passwords, API keys or recovery codes.

Service and failure scenario

Permitted data loss and downtime

Test result and evidence location

Gaps, owner and next test

Reviewed by _____ Date _____

[CHECK THE SOURCE](#)

ASD source publications

This guide uses the release published on 15 October 2026. ASD may correct or expand its advice. Use the current source when making an assessment or changing a security plan.

ASD frequently asked questions

cyber.gov.au/publication/frequently-asked-questions

The Essentials for senior executives

cyber.gov.au/publication/the-essentials-for-senior-executives

Which chapter should I start with

cyber.gov.au/publication/which-chapter-should-i-start-with

Asset scoping guide for enterprise IT

cyber.gov.au/publication/asset-scoping-guide-for-enterprise-it

Essentials for enterprise IT

cyber.gov.au/publication/essentials-for-enterprise-it

Essentials for OT

cyber.gov.au/publication/essentials-for-ot

Essentials glossary

cyber.gov.au/publication/essentials-glossary

Asset scoping guide for cloud

cyber.gov.au/publication/asset-scoping-guide-for-cloud

Implementing multi factor authentication

cyber.gov.au/publication/implementing-multi-factor-authentication

Assessment evidence guide for enterprise IT

cyber.gov.au/publication/assessment-evidence-guide-for-enterprise-it

[CHECK THE SOURCE](#)

ASD source publications continued

Essentials for cloud

cyber.gov.au/publication/essentials-for-cloud

Microsoft guidance on orphaned Power Automate flows

<https://learn.microsoft.com/en-us/troubleshoot/power-platform/power-automate/flow-management/manage-orphan-flow-when-owner-leaves-org>

Microsoft guidance on data loss prevention

<https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>

Google Workspace Drive log events

<https://support.google.com/a/answer/4579696?hl=en>

Transitioning from the Essential Eight

cyber.gov.au/publication/transitioning-from-the-essential-eight

Cloud computing security for tenants

cyber.gov.au/publication/cloud-computing-security-for-tenants

Implementation planning guide

cyber.gov.au/publication/implementation-planning-guide

AI considerations within the Essentials

cyber.gov.au/publication/ai-considerations-within-the-essentials

Assessment process guide

cyber.gov.au/publication/assessment-process-guide

Security when engaging a managed service provider

cyber.gov.au/publication/how-to-manage-your-security-when-engaging-a-managed-service-provider

GET A USEFUL SCOPE

Bring the service names, not the passwords

A Dark Cloud Creative helps small businesses in Perth and works remotely across Australia. We can review the systems you use and agree the work before changing them.

Useful information for the first conversation

How many people use the services and where they work.

The email, file, website and business applications in use.

The problem or obligation that prompted the review.

What would stop the business trading and how quickly it would need to recover.

What your current provider is responsible for, if you have one.

DISCUSS YOUR SETUP

adarkcloud.com.au/contact

Please keep passwords, recovery codes and API keys out of your enquiry.