



Australian Government
Australian Signals Directorate

cyber.gov.au

Transitioning from the Essential Eight

 Essentials

Contents

Purpose	3
Audience	3
The transition principle	4
Why existing controls may need to be strengthened	5
Key concepts translated	6
What is new	7
Considering existing maturity levels	8
Organisations at Maturity Level Two	9
Organisations at Maturity Level Three	9
Organisations undertaking an Essential Eight program	9
Strategy-by-strategy transition mapping	10
Application control	11
Patch applications and patch operating systems	12
Multi-factor authentication	13
Restrict administrative privileges	14
Restrict Microsoft Office macros	16
User application hardening	18
Regular backups	19
Event logging, detection and response	20
Reusing existing assessment evidence	21
Recommended transition pathway	22
Reporting during transition	23
Common transition pitfalls	24

Purpose

The Australian Signals Directorate (ASD) has evolved the Essential Eight into the *ASD Essentials for enterprise IT* to address contemporary cyber threats and modern enterprise environments.

Organisations that have implemented the Essential Eight have already made significant investments in improving their cyber security posture. That investment remains valuable. However, *ASD Essentials for enterprise IT* describes, scopes and assesses cyber security outcomes differently and, in many cases, applies existing controls more broadly.

This guidance helps organisations transition an existing Essential Eight implementation to *ASD Essentials for enterprise IT*. It explains:

- how each Essential Eight mitigation strategy maps to principles and actions in the enterprise IT chapter
- where existing controls and evidence can be reused
- where existing controls may need to be strengthened or expanded
- a recommended approach for planning the transition.

This guidance should be read alongside *ASD Essentials for enterprise IT*, *What is the Essentials series?*, the *Implementation planning guide* and the *Assessment process guide*.

Audience

This publication is for organisations that have implemented, or are currently implementing, the Essential Eight.

It will be particularly useful for:

- security architects
- cyber security program leads
- chief information security officers
- assessors
- executives and governing bodies seeking to understand how previous Essential Eight investments carry forward.

Organisations that have not implemented the Essential Eight can implement *ASD Essentials for enterprise IT* directly and do not need to use this transition guidance.

The transition principle

Existing investment carries forward, but it is assessed differently

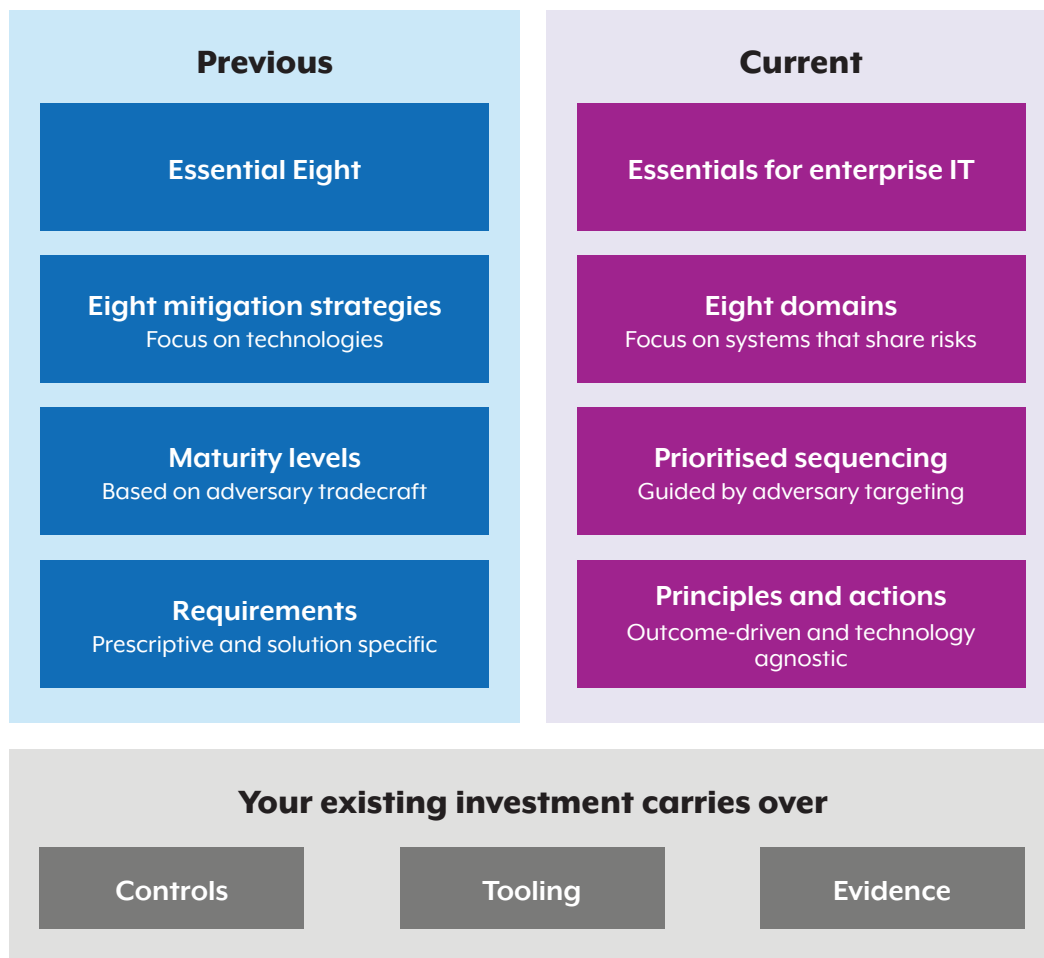


Figure 1. Transition from Essential Eight to ASD Essentials for enterprise IT

Every Essential Eight mitigation strategy maps to at least one **principle** in the *ASD Essentials for enterprise IT*. Existing controls will often directly satisfy, or contribute to, one or more **actions**.

The main differences are:

- the scope that controls need to cover
- the broader security outcomes that some controls now contribute to
- the evidence required to demonstrate that an action is effective.

Previous Essential Eight maturity level ratings do not automatically translate into effectiveness ratings under the *ASD Essentials for enterprise IT*. The two approaches assess different things.

Organisations should instead use their existing implementation and assessment evidence as the starting point for a gap analysis. Existing evidence can be reused where it remains current and relevant.

Why existing controls may need to be strengthened

A control that satisfied an Essential Eight requirement may need additional work under *ASD Essentials for enterprise IT*. This is generally because of differences in principle breadth, domain scope or assessment evidence.

Why a compliant control may need strengthening

Existing implementation remains valuable, but the required outcome may be broader than the original control

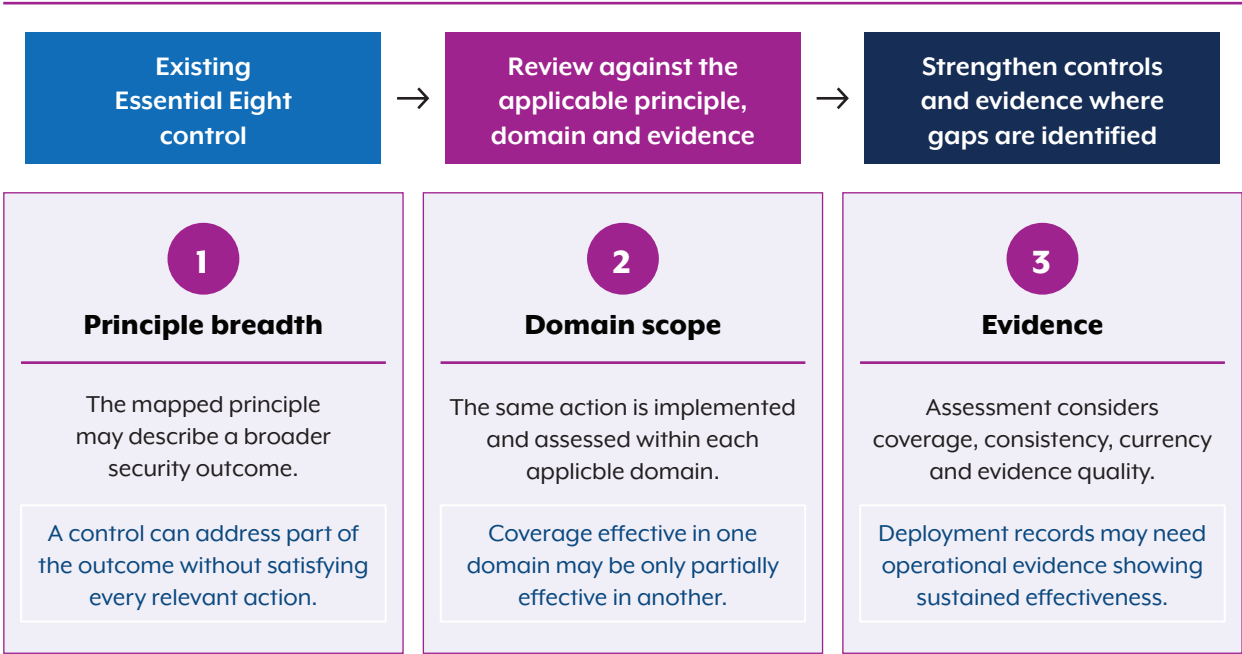


Figure 2. Why a compliant control may need strengthening

Principle breadth

Many Essential Eight mitigation strategies map to principles that have a broader security outcome.

For example, **Restrict Microsoft Office macros** contributes to the broader **Trustworthy software** principle. Existing macro controls therefore remain valuable, but they address only part of the broader requirement to control software execution.

A gap analysis helps identify what is already addressed and what additional work is required. Additional work represents an extension of existing investment rather than its replacement.

Domain scope

The Essential Eight maturity model applied requirements across an organisation’s IT environment. *ASD Essentials for enterprise IT* groups assets and functions into domains with similar risk characteristics.

The same action may therefore be implemented and assessed differently across domains.

For example, an organisation may have an enterprise-wide control that is **fully effective** in one domain but only **partially effective** in another because its coverage or implementation is not proportionate to the risks of that domain.

This means organisations need to consider existing controls in the context of each domain rather than assume an enterprise-wide implementation produces the same outcome everywhere.

Evidence

Existing Essential Eight evidence remains valuable. Configuration records, policies, control settings and deployment records can show how a control has been implemented.

However, an assessment under the Essentials series considers whether an action is achieving its intended security outcome. Assessors consider **coverage**, **consistency**, **currency** and **evidence quality** when determining an action rating.

Where existing evidence demonstrates deployment but not sustained effectiveness, organisations may need additional operational evidence. Depending on the action and environment, this could include control validation, testing, exercise results, monitoring records or other evidence showing that the control continues to operate as intended.

Key concepts translated

Table 1 summarises how key Essential Eight concepts relate to *ASD Essentials for enterprise IT*.

Table 1: Translating Essential Eight concepts

Essential Eight concept	ASD Essentials concept	What changes in practice
Mitigation strategies with requirements	Principles supported by actions	Principles describe the security outcome. Actions describe what organisations must do to achieve it. One Essential Eight mitigation strategy may contribute to several principles and actions.
Maturity levels	Priority phases	Priority phases sequence the technical domains. They are not maturity or assurance ratings.
Whole-of-environment implementation	Eight domains	Actions are applied and assessed in the domains to which they are mapped. Assets that support more than one domain are considered in each relevant domain.
Selecting a maturity level based on adversary tradecraft	Threat-informed implementation across the framework	Organisations no longer select a target maturity level. The framework is informed by current adversary tradecraft and cyber threat information, while priority phases provide the recommended implementation sequence.
Assessment against specific requirements	Four-tier, outcome-based assessment	Assessments consider whether each action achieves its intended security outcome for the assets in scope.
Essential Eight assessment process	Assessment process guide	Actions are assessed using the ratings not assessed, not effective, partially effective and fully effective. Indicators of good practice support consistent assessor judgement.

What is new

The Essential Eight remains an important foundation for many of the controls required by ASD Essentials for enterprise IT. However, the enterprise IT chapter also introduces security outcomes that were not directly addressed by the Essential Eight.

Governance and risk management

The **Governance and culture** domain includes principles covering areas such as:

- executive cyber security accountability
- cyber security resourcing
- security risk management assurance
- supplier cyber security assurance
- artificial intelligence accountability
- legacy system management.

Organisations may already have relevant governance arrangements through existing regulatory, risk management or assurance processes. However, these areas were not assessed as part of the Essential Eight maturity model.

Asset and risk identification

Asset identification extends beyond the asset discovery requirements of the Essential Eight.

Organisations need to continuously identify and document **infrastructure, operating systems, applications, identities, credentials and data** as distinct assets.

The framework also requires threat-informed risk assessment that considers relevant weaknesses, malicious actor techniques and cyber threat behaviours.

Expanded protect principles

Many Essential Eight controls continue to contribute directly to the **Protect** principles, but the required security outcomes are broader.

For example, the **Identity, credential and access management** principle includes MFA as well as requirements relating to accounts, credentials, authentication protocols and credential storage.

Similarly, **application control and macro restrictions** contribute to broader requirements for **Trustworthy software** and **Secure configuration management**.

New protect principles

ASD Essentials for enterprise IT also contains principles that do not have a direct Essential Eight equivalent.

Examples include:

- **Content filtering**
- **Cyber security awareness training**
- **Cyber supply chain security**

Visibility and response

The Essential Eight included logging, monitoring and incident response requirements within individual mitigation strategies.

ASD Essentials for enterprise IT brings these capabilities together through the **Visibility and response** domain and dedicated principles covering event logging, detection, incident identification, detection efficacy, incident coordination, incident response and post-incident insights.

The **Visibility and response** domain applies across all phases and expands as additional technical domains are implemented.

Considering existing maturity levels

Essential Eight maturity level ratings do not automatically convert into ratings under *ASD Essentials for enterprise IT*.

The Essential Eight maturity model assessed implementation against requirements associated with increasing levels of adversary tradecraft. The Essentials assessment model instead assesses whether individual actions achieve their intended security outcomes for the assets within each applicable domain.

Each action is assessed using a four-tier rating scale:

- **not assessed**
- **not effective**
- **partially effective**
- **fully effective.**

An action is rated **not assessed** if it has not yet been assessed against a domain or there is insufficient evidence to determine whether its intended security outcome is being achieved. This is a neutral rating and must remain distinct from **not effective**.

Previous Essential Eight implementation remains a useful indicator of where an organisation may start because many Essential Eight controls address assets and capabilities that remain important under ASD Essentials for enterprise IT.

Essential Eight maturity levels: starting posture

Previous maturity provides a useful baseline for transition,
not an automatic Essentials effectiveness rating.

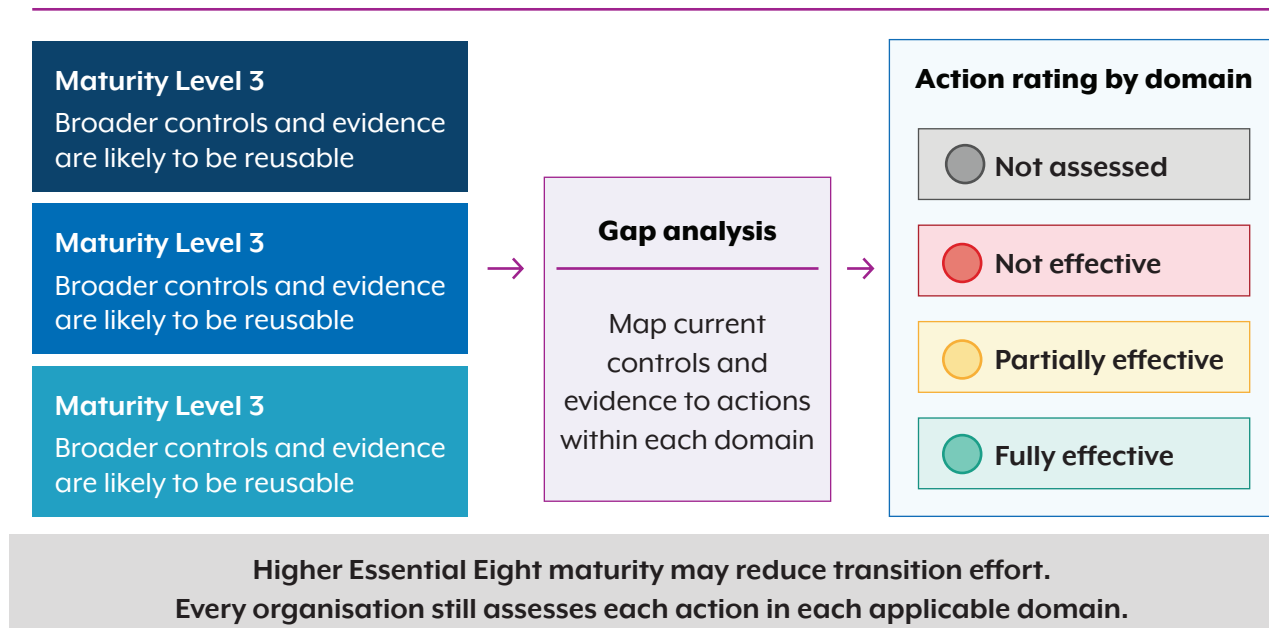


Figure 3. Essential Eight maturity levels starting posture

Organisations at Maturity Level Two

Maturity Level Two was the required baseline for Commonwealth entities and many Australian critical infrastructure operators. Organisations that achieved Maturity Level Two can expect many existing controls to contribute to actions in the early priority phases. Examples include controls relating to phishing-resistant MFA, patching internet-facing services, privileged access, application control and centralised logging of security-relevant events.

However, organisations should not assume that previous achievement of Maturity Level Two means an action will be **fully effective** in every applicable domain.

Common areas requiring additional work are likely to include:

- extending controls to assets or domains not previously covered
- addressing the **Governance and culture** principle
- expanding **Visibility and response** capabilities
- producing evidence that demonstrates sustained effectiveness rather than deployment alone.

Organisations at Maturity Level Three

Organisations that achieved and sustained Maturity Level Three are likely to be able to reuse a broader range of controls and evidence. This may include controls relating to vulnerability management, application control, privileged access, event logging and analysis, configuration hardening and restoration testing.

However, Maturity Level Three does not automatically produce **fully effective** ratings under *ASD Essentials for enterprise IT*.

The enterprise IT chapter includes actions with no direct Essential Eight equivalent, including requirements relating to credential exposure, supply chain security, domain-based implementation and the **Governance and culture** and **Visibility and response** capability domains.

A gap analysis therefore remains necessary.

Organisations previously implementing or assessed at Maturity Level One can use the same transition approach. However, they should expect a greater proportion of actions to require additional implementation.

Organisations undertaking an Essential Eight program

Organisations part-way through an Essential Eight uplift program can begin transitioning without discarding work already completed.

Existing controls, implementation evidence and assessment results should be mapped to the relevant actions in *ASD Essentials for enterprise IT*. Where planned Essential Eight work remains relevant, it can be incorporated into the broader implementation strategy.

The priority phases can help organisations focus remaining investment on the domains where ASD recommends effort be directed first.

Organisations should also continue to meet any regulatory, contractual or other obligations that require Essential Eight implementation or reporting.

Strategy-by-strategy transition mapping

The following sections consider each Essential Eight mitigation strategy.

For each strategy, they identify:

- the principles and actions it contributes to
- where existing investment can be reused
- where existing controls may need to be strengthened.

The mappings assume that the relevant Essential Eight requirements were implemented and sustained. Organisations should confirm that existing controls and evidence remain current before relying on them. The actions reproduced in this section should match the current wording in *ASD Essentials for enterprise IT*. The enterprise IT chapter remains the authoritative source for the requirements.

Table 2: Essential Eight mitigation strategies and mapped principles

Essential Eight mitigation strategy	Mapped principles
Application control	Trustworthy software Secure configuration management
Patch applications	Vulnerability management Asset identification Legacy system management
Patch operating systems	Vulnerability management Asset identification Legacy system management
Multi-factor authentication	Identity, credential and access management
Restrict administrative privileges	Identity, credential and access management Least privilege access Secure administration Network segmentation and segregation
Restrict Microsoft Office macros	Trustworthy software Secure configuration management
User application hardening	Secure configuration management
Regular backups	Regular and proven backups Least privilege access

Application control

Key mapped principles: Trustworthy software and Secure configuration management.

Action mapping

Table 3: Application control action mapping

Principle	Action	Domain coverage	Existing E8 contribution
Trustworthy software	Permit only supported, verified and organisation- authorised software to execute on systems, with exceptions minimised, formally risk accepted, time-bound, monitored and regularly reviewed.	• User devices (ML1) • Boundary services (ML2) • Business systems (ML3) • Critical processes and services (ML3)	Existing application control rulesets, approved software lists and blocklists can provide strong evidence of software execution controls.
Trustworthy software	Restrict administrative and management tooling to approved software sets and executed from only authorised, known locations.	• User devices (partial, ML1) • Boundary services (partial, ML2)	Existing application control may provide partial coverage. Administrative and management tooling may need to be identified and controlled separately.
Secure configuration management	Detect and respond to configuration drift using scheduled technical assessments and, where supported, automated monitoring, based on system criticality and change rate.	• User devices (partial, ML2) • Boundary services (partial, ML2)	Existing ruleset reviews and validation records may contribute evidence, but organisations may need broader mechanisms for identifying configuration drift.

Where existing investment is recognised

Existing investment may include:

- application control on workstations and servers
- approved software lists and block list configurations
- restrictions on executables, scripts, installers, software libraries and other executable content
- documented application control exceptions
- application control logging and monitoring.

These controls remain relevant to the **Trustworthy software** principle.

Existing application control events forwarded to central logging can also contribute evidence for the **Centralised event logging** principle.

Where investments will need to be strengthened

Broader software requirements. Application control is one part of the Trustworthy software outcome. Organisations also need to consider whether software is supported, verified and organisation-authorised.

Administrative tooling. Administrative and management tools must be restricted to approved software sets and authorised locations.

Exception management. Exceptions need to be minimised, formally risk accepted, time-bound, monitored and regularly reviewed.

Domain coverage. Trustworthy software applies across the technical domains. Organisations should confirm that existing controls provide appropriate coverage in each applicable domain.

Patch applications and patch operating systems

Key mapped principles: Vulnerability management, Asset identification and Legacy system management.

Action mapping

Table 4: Patching action mapping

Principle	Action	Domain coverage	Existing E8 contribution
Vulnerability management	Identify known software and configuration weaknesses of assets through continuous and repeatable assessment activities, including vulnerability scanning activities.	• Boundary services (ML1) • User devices (ML1) • Business systems (ML1) • Critical processes and services (ML2)	Existing scanner configurations, scan schedules and results can provide useful evidence.
Vulnerability management	Apply security patches or updates within defined risk-based timeframes or, where operational impact is low, automatically.	• Boundary services (ML1) • User devices (ML1) • Business systems (ML1) • Critical processes and services (ML2)	Patch deployment records and compliance reporting remain relevant.
Vulnerability management	Remediate or mitigate vulnerabilities exceeding defined risk thresholds within defined timeframes based on exploitation, exposure, criticality, impact and compensating controls and verify treatment effectiveness.	• All technology domains (partial, ML1)	Existing vulnerability treatment and mitigation records can contribute evidence.
Asset identification	Use an approved asset inventory mechanism that supports automated discovery to detect new and changed physical and non-physical assets.	• Visibility and response (ML1)	Existing automated discovery capabilities remain relevant.
Asset identification	Continuously identify and document infrastructure, operating systems, applications, identities, credentials and data as distinct assets.	• Boundary services (partial, ML1) • Identity services (partial, ML1) • Critical processes and services (partial, ML1) • Privileged environments (partial, ML1) • Business systems (partial, ML1) • User devices (partial, ML1)	Existing operating system and application inventories provide a starting point but may not cover every required asset type.

Where existing investment is recognised

Existing investment may include:

- automated asset discovery
- vulnerability scanning
- patch deployment processes
- patch compliance reporting
- processes for responding to vulnerabilities where a patch is unavailable
- processes for removing or replacing unsupported systems.

These capabilities can be reused where they remain current and provide appropriate coverage.

Where investment may need to be strengthened

Asset coverage. Asset identification includes infrastructure, operating systems, applications, identities, credentials and data as distinct assets. Existing inventories may need to be expanded.

Risk-based treatment. Existing Essential Eight patching arrangements remain relevant, but organisations need to consider the exploitation, exposure, criticality, impact and compensating controls associated with vulnerabilities. Applicable ISM, regulatory and other mandatory timeframes continue to apply.

Domain context. An appropriate treatment timeframe may differ between domains because their assets and risk contexts differ.

Legacy systems. Where legacy systems cannot be removed or replaced immediately, organisations need to identify and manage the associated cyber security risk until decommissioning or replacement.

Multi-factor authentication

Key mapped principles: Identity, credential and access management.

Action mapping

Table 5: Multi-factor authentication mapping

Principle	Action	Domain coverage	Existing E8 contribution
Identity, credential and access management	Use phishing-resistant MFA for users authenticating to systems, including from untrusted, external or high-risk locations.	• Boundary services (ML1) • Critical processes and services (ML1) • Privileged environments (ML2) • Business systems (ML2) • Identity services (partial, ML2) • User devices (partial, ML2)	Existing MFA configurations, authentication policies and coverage reporting can provide strong evidence.

Where existing investment is recognised

Existing phishing-resistant MFA controls remain directly relevant. This includes MFA used for privileged users, unprivileged users, organisational online services, third-party services or remote or external access. Logging of successful and unsuccessful authentication events can also contribute evidence for **Centralised event logging** and the detection of identity and credential misuse.

Where investment may need to be strengthened

MFA is one part of the broader **Identity, credential and access management** principle.

Organisations also need to consider actions requiring them to:

- identify and disable or remove default and unused accounts
- store authentication keys, secrets and tokens in approved secure repositories
- regularly scan codebases, configuration files, file shares and collaboration platforms for unsecured keys, secrets and credentials
- disable legacy authentication protocols or, where this is not feasible, restrict and monitor their use, apply compensating controls and establish a time-bound decommissioning plan
- ensure user, machine, system and service account credentials are unique per system or account, particularly in high-privilege contexts.

Existing MFA coverage should also be considered for each applicable domain rather than only for external or remote access.

Restrict administrative privileges

Key mapped principles: Identity, credential and access management, Least privilege access, Secure administration and Network segmentation and segregation.

Action mapping

Table 6: Administrative privilege action mapping

Principle	Action	Domain coverage	Existing E8 contribution
Secure administration	Ensure administrative activities can only be executed from dedicated and hardened environments that are isolated from unprivileged user workloads.	• Privileged environments (ML1) • Boundary services (partial, ML1) • Identity services (partial, ML1) • Critical processes and services (partial, ML1)	Existing privileged access workstations, restricted administrative environments and jump servers can provide strong evidence.
Secure administration	Enforce explicit session establishment controls before privileged actions are permitted, including the use of time-bound privilege grants.	• Privileged environments (partial, ML2)	Existing session controls may contribute, but time-bound privilege is likely to require additional consideration.

Principle	Action	Domain coverage	Existing E8 contribution
Secure administration	Record all administrative or management actions that modify systems, configurations or controls with the details of the user, timestamp and target.	- Privileged environments (partial, ML2) - Identity services (partial, ML2)	Existing privileged access and account management logging can contribute evidence.
Least privilege access	Periodically review and update access privileges in alignment with current roles, duties and business requirements.	- Privileged environments (ML2) - Identity services (partial, ML2)	Existing privileged access reviews and revalidation processes remain relevant.
Least privilege access	Restrict permissions to create, modify or delete accounts or roles, or to access privileged functions or applications, to authorised administrative roles.	Privileged environments (partial, ML1)	Existing privileged access approval processes can contribute.
Least privilege access	Provision user, administrative and non-person accounts with only the minimum access and privileges required to perform defined operational functions.	- Privileged environments (ML1) - Identity services (partial, ML1)	Existing account provisioning and privileged account controls provide a strong starting point.
Identity, credential and access management	Identify and disable or remove default and unused accounts on a regular basis.	- Privileged environments (partial, ML2) - Identity services (partial, ML2)	Existing inactivity and account management processes may partially satisfy this requirement.
Identity, credential and access management	Store authentication keys, secrets and tokens in approved secure repositories with access controls, including MFA.	Privileged environments (partial, ML2)	Existing management of privileged credentials may contribute.
Identity, credential and access management	Ensure that user, machine, system and service account credentials are unique per system or account, particularly in high-privilege contexts.	- Privileged environments (partial, ML2) - Identity services (partial, ML2)	Existing controls for administrator, service and break-glass credentials may contribute.
Network segmentation and segregation	Limit lateral movement between, and within, network segments to explicitly approved pathways and services, based on business requirements and trust levels.	Privileged environments (partial, ML1)	Existing separation of privileged environments may provide partial evidence.

Where existing investment is recognised

Existing controls that remain relevant include:

- separate privileged and unprivileged accounts
- privileged access workstations and restricted administrative environments
- restrictions on internet and email access from privileged environments
- privileged access approval and revalidation processes
- management of privileged and service account credentials
- logging of privileged access and account management events.

Where investment may need to be strengthened

Privileged environments. Organisations need to identify the assets and functions that make up the Privileged environments domain, including relevant management platforms and privileged access services.

Time-bound privilege. *ASD Essentials for enterprise IT* requires explicit session establishment controls, including time-bound privilege grants. Organisations with standing privileged access should determine whether existing controls achieve this outcome.

Administrative recording. Logging needs to capture administrative or management actions that modify systems, configurations or controls, including the user, timestamp and target.

Non-person accounts. Least privilege requirements apply to non-person and service accounts as well as user accounts.

Network segmentation. Organisations need to limit lateral movement using explicitly approved pathways and services based on business requirements and trust levels.

Restrict Microsoft Office macros

Key mapped principles: Trustworthy software and Secure configuration management.

Action mapping

Table 7: Microsoft Office macro action mapping

Principle	Action	Domain coverage	Existing E8 contribution
Secure configuration management	Define approved configuration baselines, informed by vendor and industry hardening guidance, that disable or remove unnecessary services, insecure settings and unsupported or weak communication protocols.	• User devices (ML1)	Existing macro policies and security configuration settings can contribute directly to user device baselines.

Principle	Action	Domain coverage	Existing E8 contribution
Secure configuration management	Deploy approved configuration baselines on systems, including infrastructure, operating systems and applications.	User devices (partial, ML1)	Existing enforced macro settings can provide evidence of baseline deployment.
Trustworthy software	Permit only supported, verified and organisation-authorised software to execute on systems, with exceptions minimised, formally risk accepted, time-bound, monitored and regularly reviewed.	- User devices (partial, ML1) - User devices (ML3)	Macro restrictions, trusted publisher arrangements and other execution controls can provide evidence.

Where existing investment is recognised

Existing controls may include:

- disabling macros where there is no demonstrated business requirement
- blocking macros in files originating from the internet
- scanning macros for malicious content
- preventing users from changing macro security settings
- Trusted Location and trusted publisher arrangements.

These controls remain useful for limiting unauthorised code execution and enforcing approved configurations.

Where investment may need to be strengthened

Beyond macros. Macro controls contribute to broader requirements covering software execution. Organisations should consider equivalent controls for other relevant execution mechanisms.

Configuration baselines. Macro settings should form part of approved configuration baselines that are deployed, maintained and reviewed.

Configuration drift. Organisations need processes for detecting and responding to configuration drift using scheduled technical assessments and, where supported, automated monitoring.

User application hardening

Key mapped principles: Secure configuration management and Content filtering.

Action mapping

Table 8: User application hardening action mapping

Principle	Action	Domain coverage	Existing E8 contribution
Secure configuration management	Define approved configuration baselines, informed by vendor and industry hardening guidance, that disable or remove unnecessary services, insecure settings and unsupported or weak communication protocols.	• User devices (ML1)	Existing browser, office productivity and PDF hardening can provide strong evidence for user devices.
Secure configuration management	Deploy approved configuration baselines on systems, including infrastructure, operating systems and applications.	• User devices (partial, ML1)	Existing enforced security settings can contribute evidence of baseline deployment.
Content filtering	Block outbound network connections to known malicious or untrusted destinations.	• User devices (partial, ML1)	Existing browser and application controls may provide partial evidence but do not necessarily address all outbound connections.

Where existing investment is recognised

Existing hardening controls remain relevant, including controls applied to:

- web browsers
- office productivity suites
- PDF software
- PowerShell and command-line activity
- application security settings.

Associated event logging can also contribute to Centralised event logging and detection activities.

Where investment may need to be strengthened

Approved and tailored baselines. Organisations should ensure configuration baselines are appropriate to their environment, formally approved and maintained.

Configuration drift. Organisations need to detect and respond to deviations from approved baselines.

Coverage. Configuration baselines should cover the relevant assets within each applicable domain.

Beyond user devices. Secure configuration management applies across the technical domains, not only endpoints.

Broader content filtering. Blocking advertisements or browser-based content may contribute to the Content filtering principle, but organisations need to consider outbound connections across relevant applications and services.

Regular backups

Key mapped principles: Regular and proven backups and Least privilege access.

Action mapping

Table 9: Backup action mapping

Principle	Action	Domain coverage	Existing E8 contribution
Regular and proven backups	Back up important data, applications and settings on a defined schedule to secure, resilient storage protected by encryption and immutable, offline, logically isolated or equivalent controls.	• Critical processes and services (ML1) • Business systems (ML1) • Boundary services (partial, ML1) • Identity services (partial, ML1) • Privileged environments (partial, ML1)	Existing backup schedules, retention arrangements and access controls provide a strong starting point.
Regular and proven backups	Isolate backup repositories from general user environments and production workloads, ensuring they are separated from primary systems to prevent unauthorised modification or deletion.	• Critical processes and services (partial, ML1) • Business systems (partial, ML1) • Privileged environments (partial, ML2)	Existing restrictions on backup access may provide partial or direct evidence depending on the architecture.
Regular and proven backups	Conduct regular testing of backup and restoration procedures to ensure that backups are reliable and capable of meeting defined recovery time objectives and recovery point objectives.	• Boundary services (ML1) • Identity services (ML1) • Critical processes and services (ML1) • Privileged environments (ML1) • Business systems (ML1)	Current restoration test results and disaster recovery exercises can provide strong evidence.

Where existing investment is recognised

Existing Essential Eight backup arrangements remain highly relevant, including:

- regular backups of important data, applications and settings
- backup retention arrangements
- restrictions on who can access, modify or delete backups
- restoration testing
- disaster recovery exercises.

Where investment may need to be strengthened

Storage protection. Organisations need secure and resilient backup storage protected through appropriate measures such as encryption and immutable, offline, logically isolated or equivalent controls.

Repository isolation. Backup repositories need to be separated from primary systems, general user environments and production workloads to reduce the likelihood that an adversary can affect both production data and backups.

Recovery objectives. Restoration testing should demonstrate that defined recovery time and recovery point objectives can be achieved.

Domain scope. Organisations should confirm that backup arrangements cover the important data, applications and settings associated with each applicable domain.

Event logging, detection and response

The Essential Eight included event logging, detection and incident response requirements across several mitigation strategies. As such, these requirements contribute to a broader set of principles in *ASD Essentials for enterprise IT*.

Key mapped principles: Centralised event logging, Baselined high-risk access activities, Cyber security event detection, Cyber security incident identification, Detection capability efficacy, Cyber security incident coordination, Cyber security incident response, Cyber security incident insights.

These capabilities are primarily implemented through the **Visibility and response** domain.

Where existing investment is recognised

Existing Essential Eight investment may include:

- centralised logging of MFA events
- privileged access and account management logs
- application control logs
- PowerShell and command-line event logging
- protection of event logs from unauthorised access, modification or deletion
- analysis of security-relevant events
- incident escalation and reporting processes
- cyber security incident response plans.

These capabilities provide a strong starting point for the **Visibility and response** requirements.

Where investment may need to be strengthened

Visibility and response across all phases. Visibility and response is a capability domain that applies across all phases and expands as implementation progresses.

Log management. High-value, security-relevant event logs and configuration changes need to be forwarded to a central logging capability. Event logs also need to support effective correlation across systems and environments.

Detection. Organisations need to consider detection of unauthorised change, anomalous authentication activity, suspicious software execution and other behaviours relevant to the domains in scope.

Detection efficacy. Detection coverage should be reviewed to identify gaps arising from new assets, services, cyber threats or architectural change.

Incident response. Organisations need documented, tested and approved procedures for responding to cyber security incidents.

Post-incident learning. Reviews should identify the security gaps that enabled an incident and consider whether monitoring and response procedures need to change.

Reusing existing assessment evidence

Organisations that have been assessed against the Essential Eight may already hold substantial evidence, including assessment reports, configuration extracts, ruleset exports, control test results, logging architecture documentation, exception registers, risk registers and remediation plans.

This evidence should be reused where it remains current and relevant.

Evidence that shows what has been deployed remains useful. It can demonstrate where and to what extent a control is implemented.

However, deployment alone does not demonstrate effectiveness.

Evidence showing how a control operates over time can provide stronger support for an action rating. This may include:

- validation results
- monitoring records
- configuration drift reports
- review records
- restoration tests
- exercises
- detection engineering artefacts.

The *Assessment process guide* explains how existing evidence can be reused and when additional evidence may be required. If existing evidence is current and reliable and demonstrates appropriate coverage and consistency, organisations do not need to generate new evidence simply because it was originally collected for another framework or assessment.

Existing exceptions, compensating controls and accepted risks should also be reviewed. An expired exception, degraded compensating control or risk acceptance based on an outdated threat environment should not be relied on without review.

Recommended transition pathway

The transition should follow the implementation approach described in the *Implementation planning guide*, while making use of existing Essential Eight investment.

ASD recommends the following sequence.

1. Establish the transition baseline

Record the organisation's current Essential Eight position, including:

- the most recent assessment results
- existing controls
- exception and risk registers
- remediation plans
- committed or planned uplift activities.

Do not initiate work solely to achieve a superseded Essential Eight target unless it remains required by a regulator or other obligation or continues to address material cyber security risk.

Map existing and planned work to *ASD Essentials for enterprise IT* before deciding whether it should continue unchanged.

2. Scope the priority phase 1 domains

Identify the assets and functions within:

- Governance and culture
- Visibility and response
- Boundary services
- Identity services.

Reuse existing asset inventories, architecture documentation, business impact assessments and other relevant information.

Where an asset supports more than one domain, include it in each relevant domain.

3. Conduct a gap analysis

For each applicable principle, review the associated actions against existing controls.

Classify each action as:

- already effectively addressed
- partially addressed
- not addressed.

These are gap analysis findings, not formal assessment ratings.

Document how existing controls address each action and identify what remains to be delivered.

This terminology is consistent with the *Implementation planning guide*, which deliberately separates initial gap analysis from the formal action ratings used during assessment.

4. Plan implementation

Use the identified gaps to develop an implementation strategy.

Where a gap is specific to one domain, organisations can use a domain-focused implementation approach.

Where the same requirement applies across several domains, organisations can design the capability once and progressively apply it in priority phase order.

5. Deliver and measure

Implement remediation and prepare for assessment as controls are delivered.

For each applicable action and domain, consider:

- coverage
- consistency
- currency
- evidence quality.

Where an action is rated partially effective during an assessment, document the specific gaps and establish remediation with defined actions and timeframes.

6. Progress through the priority phases

After addressing the priority phase 1 technical domains, progress through:

- **priority phase 2:** Critical processes and services, and Privileged environments
- **priority phase 3:** Business systems and User devices.
- **Governance and culture**, and **Visibility and response**, continue across all phases and expand as implementation progresses.

Establish an appropriate reassessment cadence to confirm that controls continue to achieve their intended outcomes.

Reporting during transition

During transition, organisations should use the reporting approach defined in the *Assessment process guide*.

Domains or actions that have not yet been assessed should be reported as **not assessed**.

The **not assessed** rating should not be used to imply that an action is ineffective. It records that the action has not yet been assessed, or that there is insufficient evidence to determine its effectiveness.

Organisations with regulatory or other reporting obligations that continue to require Essential Eight terminology should continue to meet those obligations as directed by the relevant authority.

Common transition pitfalls

Treating priority phases as maturity levels. Priority phases sequence implementation across domains. They are not maturity, compliance or assurance ratings.

Claiming equivalence instead of assessing. A control that previously satisfied an Essential Eight requirement provides evidence. It does not automatically produce a rating under ASD Essentials for enterprise IT.

Assessing the enterprise instead of the domain. Actions are assessed in the context of each applicable domain. Enterprise-wide implementation does not mean an action will receive the same rating in every domain.

Ignoring the capability domains. Governance and culture, and Visibility and response, apply across all phases and expand as implementation progresses. They should not be deferred until the technical domains are complete.

Attempting to transition every domain at once. Spreading implementation, evidence collection and stakeholder effort across the whole environment can dilute progress. Use the priority phases to focus effort while continuing to mature the two capability domains.

Reusing stale evidence. Existing evidence remains useful only where it continues to represent the current environment and operation of the control.

Overlooking new requirements. Some actions have no direct Essential Eight equivalent and require additional planning and resourcing.

**For more information, or to report a
cyber security incident, contact us:**

cyber.gov.au

1300 CYBER1 (1300 292 371)

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms, the entity's logo, third party content, and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license

<https://creativecommons.org/licenses/by/4.0/>

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license

<https://creativecommons.org/licenses/by/4.0/legalcode.en>

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website

<https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>

