principia ratio

BRIEFING · BASED ON AUSTRALIAN SIGNALS DIRECTORATE (ASD) PUBLICATIONS

ASD Essentials in practice

ASD's Essentials are a welcome turn: from proving controls exist to proving they work, across enterprise information technology (IT), cloud and operational technology (OT). This briefing covers what has changed, how to plan the work and how assessors will rate it.

A practitioner briefing for security architects, cyber security program leads, chief information security officers (CISOs) and assessors.

CONTENTS

02 From controls to outcomes
03 Three layers, one model
04 The order of work
05 What differs by environment
06 Carrying the Essential Eight forward
07 Planning the program
08 Effectiveness, not deployment
09 Weakest link, by domain
10 Seven traps to avoid
11 References



PARLIAMENT HOUSE, CANBERRA

WHAT HAS CHANGED

From controls to outcomes

Every Essential Eight strategy maps to at least one Essentials principle, so past investment carries forward. What changes is the scope each control must cover, the outcome it must reach and the evidence needed to prove it.

Essential Eight		ASD Essentials
Eight mitigation strategies	→	Eight domains: six technical and two capability
Focus on technologies	→	Focus on business functions and assets that share risks
Maturity Levels One to Three as targets	→	Three priority phases that set the order of work, not a level
Prescriptive, solution-specific requirements	→	Principles and actions that name no product or vendor
One implementation across the whole environment	→	Each action applied and rated within each domain
Assessment against set requirements	→	A four-tier rating of whether each action achieves its outcome

Why ASD changed course

- Capable state-sponsored and criminal actors now target organisations of every size, often through their suppliers and service providers.
- A fixed set of controls does not carry across enterprise IT, cloud and OT.
- Artificial intelligence (AI) makes existing attacks faster and cheaper, and AI systems are themselves new targets.

DESIGN AIMS

Threat-informed | Flexible

Aligned with the Information Security Manual (ISM)

Future-focused

THE FRAMEWORK

Three layers, one model

Every chapter shares one structure. A principle sets the outcome, an action says what to do and a domain says where. Actions are always implemented and rated within a domain, never in isolation.

Principle

What outcome am I trying to achieve?

Drawn from ISM principles and traced by identifier, such as GOV-01. The intent stays the same in every chapter.

→

Action

What needs to be done to achieve it?

Technology-agnostic requirements, tuned to each environment's threats, operating needs and cost. Most are mapped to known adversary techniques.

→

Domain

Where does it apply?

A logical group of business functions and assets with comparable exposure and consequence of compromise. It is neither a network segment nor a business unit.

Worked example	PRINCIPLE	ACTION	DOMAIN	TECHNIQUES DISRUPTED
	Identity, credential and access management	Use phishing-resistant multi-factor authentication (MFA) for users signing in to systems, including from untrusted, external or high-risk locations	All six technical domains	Valid Accounts (T1078), Account Manipulation (T1098), Brute Force (T1110) and Remote Services (T1021), from MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) catalogue

1 Scope the domains → **2** Identify the principles → **3** Implement the actions → **4** Measure the outcomes → **5** Report and sustain

DOMAINS AND PRIORITY PHASES

The order of work

Each chapter groups its six technical domains into three priority phases, starting where attackers most often get in. Phases set a sequence, not a rating: reaching phase 2 describes scope, not security.

	Enterprise IT	Cloud	OT
PHASE 1	Boundary services Identity services	Boundary services Identity services	Boundary services Critical processes and services
PHASE 2	Critical processes and services Privileged environments	Critical processes and services Privileged environments	Privileged environments Identity services
PHASE 3	Business systems User devices	Business systems User devices	Business systems *User devices excluded: every device in OT is treated as privileged*
ALL PHASES	**Governance and culture** and **Visibility and response**, the two capability domains. Start them early and widen them with each phase.		

Why this order

Phase 1 closes the most common ways in. Phase 2 protects the highest-value assets and the administrative paths to them. Phase 3 covers the rest.

OT puts safety first

Critical processes move into phase 1 because their compromise can have safety, environmental and service-delivery consequences.

Departures are allowed

Threat intelligence, regulation or a planned system refresh can justify another order. Record the risk-based reason. Later domains still have to be done.

Non-production counts

Development, test and staging systems that can change production need production-grade protection.

What differs by environment

The model holds across chapters but the actions change. Choose a starting chapter by weighing what you operate, what you must comply with, where the gap is widest and where risk is highest. Most organisations will need more than one.

Cloud

For software as a service (SaaS) and platform as a service (PaaS). On-premises, hybrid or infrastructure as a service (IaaS) estates start with the enterprise IT chapter.

C **Customer.** You build and run the control.

S **Supplied.** The provider offers the feature; you enable, configure and monitor it. An insecure default is not effective.

P **Provider.** The provider runs it; you verify it with current independent assurance scoped to the services you use.

Outsourcing never transfers accountability. Keep a register of inherited and retained responsibilities for each provider.

Operational technology

For operators of complex control, automation and safety systems in critical services.

- Identify vital OT: systems that cannot be offline for long without stopping safe delivery of a minimum service.
- Isolate OT behind demilitarised zones; make isolation reversible only from inside vital OT.
- Exercise isolation and prove the plant runs safely, cut off, for a defined period.
- End all remote access in the demilitarised zone, with time-bound sessions and no permanent connections.
- Keep the ability to recover vital systems without supplier support.

Artificial intelligence

AI is a threat, a defensive tool and an asset to be scoped like any other.

- Scope AI by role: agent identities sit in Identity services, AI with administrative rights in Privileged environments and public AI interfaces in Boundary services.
- A new governance principle makes the board accountable for secure, controllable and human-supervised AI.
- Prompt injection cannot be fully prevented, so limit what a manipulated model can reach.
- In the cloud, get executive approval before switching on material AI features.
- In OT, no AI platform may have a path to change safety systems.

TRANSITION

Carrying the Essential Eight forward

Maturity levels do not convert into Essentials ratings. Use existing controls and evidence as the starting point for a gap analysis in each domain, then strengthen them where the required outcome is broader.

ESSENTIAL EIGHT STRATEGY	NOW CONTRIBUTES TO	TYPICAL STRENGTHENING
Application control	Trustworthy software; Secure configuration management	Control administrative tools too; make exceptions time-bound and reviewed
Patch applications and operating systems	Vulnerability management; Asset identification; Legacy system management	Risk-based timeframes for each domain; inventories that include identities, credentials and data
Multi-factor authentication	Identity, credential and access management	Remove default accounts, vault secrets, scan for exposed credentials and retire legacy authentication
Restrict administrative privileges	Least privilege; Secure administration; Network segmentation	Time-bound privilege, logged administrative actions and least privilege for service accounts
Office macros and application hardening	Trustworthy software; Secure configuration management; Content filtering	Approved baselines with drift detection, extended beyond user devices
Regular backups	Regular and proven backups	Immutable or isolated storage; restore tests that meet recovery time and recovery point objectives

Genuinely new

- Governance and culture: executive accountability, resourcing, supplier assurance, AI accountability and legacy systems
- Visibility and response as a domain in its own right
- Content filtering, awareness training and cyber supply chain security

Starting position

- **Maturity Level Two.** Expect reuse in phase 1 areas such as MFA, patching, privileged access, application control and logging.
- **Maturity Level Three.** Broader reuse, but no automatic fully effective ratings.
- **Mid-program.** Map planned work first. Do not chase a superseded Essential Eight target unless a regulator still requires it.

IMPLEMENTATION

Planning the program

Cost priority phase 1 in full and treat later phases as forward plans. Design every control for assessment from day one, because rebuilding evidence later causes rework.

01 Executive commitment
02 Scope assets
03 Gap analysis
04 Plan implementation
05 Deliver and measure
06 Sustain and reuse

Scope by role, not owner

Place each asset by the job it does. Check six categories: infrastructure, operating systems, applications, identities, credentials and data. Domains split functions, not business units, so scope shared services once. Version the scope statement and record every exclusion.

A gap analysis is not an assessment

Mark each action addressed, partially addressed or not addressed, domain by domain. Treat stale reviews, expired exceptions and outdated baselines as findings. Poor asset visibility is a finding, not a reason to wait.

Pick a delivery approach

Domain-focus finishes one domain at a time and suits newer programs. Principle-focus rolls one capability across domains and gets more from enterprise tooling. Build MFA, baselines, logging, patching and backups once, as reusable patterns.

Fund it in three tranches

Mirror the phases. Cost capability build, operating uplift and assessment separately. Build costs fall as patterns are reused; running costs rise as more of the estate moves into sustainment.

Threat-informed ordering. Use the ATT&CK mapping to rank work within a phase, never across phases.

ASSESSMENT

Effectiveness, not deployment

Assessors rate every applicable action in every domain on a four-tier scale. A control that exists but cannot be shown to work across the domain will not be rated fully effective.

Not assessed	Not yet assessed, or too little evidence to judge. Neutral, and always reported apart from not effective.
Not effective	Absent, or present but delivering no real security benefit.
Partially effective	Achieves the outcome in part, limited by gaps in coverage, consistency or enforcement. Starting work does not count.
Fully effective	Demonstrably achieves the outcome across the domain, backed by sufficient evidence.

Indicators of good practice guide each judgement; a single not-effective indicator normally decides the rating. The method follows the Cyber Assessment Framework of Britain's National Cyber Security Centre.

FOUR TESTS FOR EVERY ACTION

Coverage
Does it reach every relevant asset in the domain?

Consistency
Is it applied the same way across them?

Currency
Is the evidence recent enough to reflect today's system?

Evidence quality
Is it reliable enough to show the outcome?

EVIDENCE QUALITY

Excellent	Directly proves the outcome in the live environment
Good	Shows coverage, consistency and currency
Fair	Suggests the action probably works
Poor	Asserts only that the control exists

The strongest evidence comes from testing: try to run an unsigned program and see whether it is blocked. Get approval before any active test.

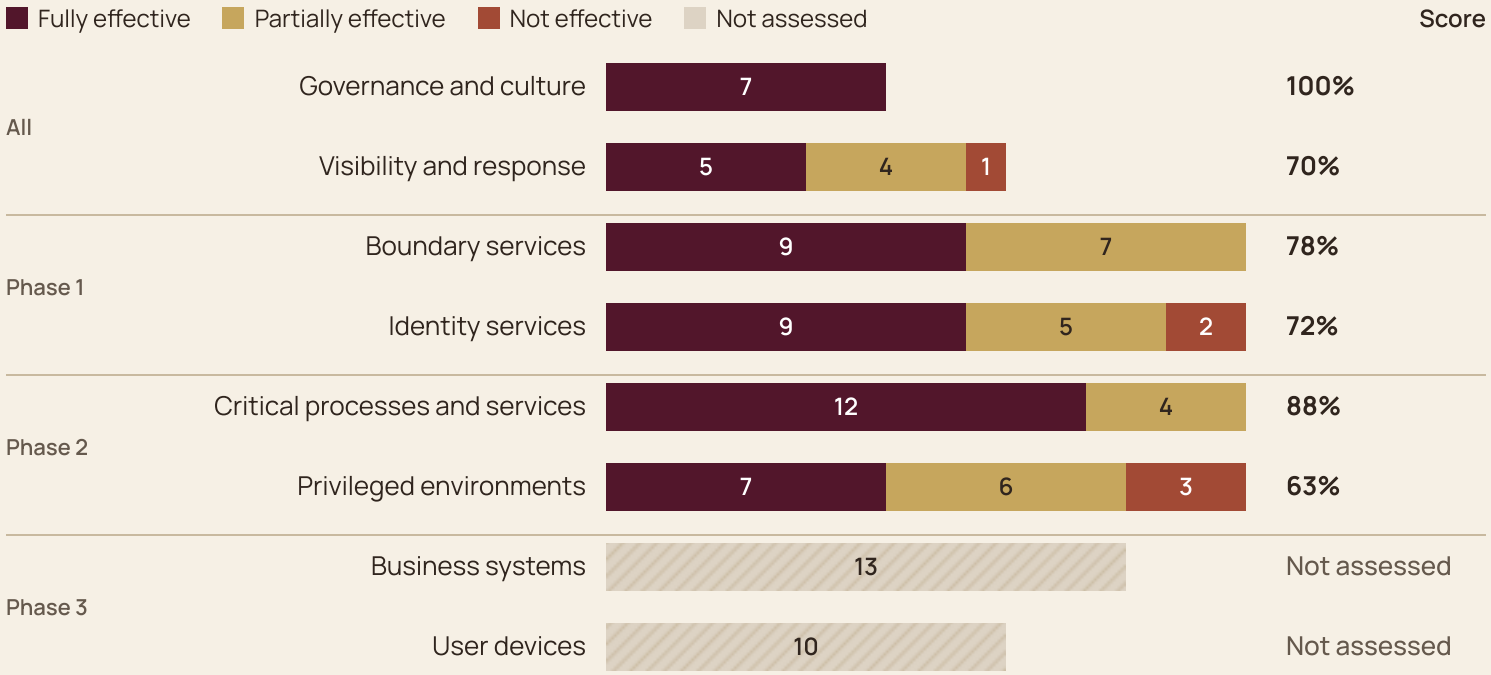
REPORTING

Weakest link, by domain

Within each domain a principle takes the rating of its weakest action. Domain scores turn those ratings into a percentage that boards can track across successive assessments.

Principles by rating and domain

Illustrative organisation part-way through phase 2; number of principles



Source: Assessment process guide [11], worked example for enterprise IT

How the score works

Each principle scores one if fully effective, a half if partially effective and zero if not effective. Divide the total by the number of applicable principles. In Visibility and response, five fully effective, four partially effective and one not-effective principle give seven out of ten, or 70%.

Reporting rules

- Pair the summary view with a detailed view of the principles and actions behind each score.
- Report unassessed domains as not assessed, never as failures.
- Agree format, frequency and audience with executives at the start.
- Radar charts suit boards, but never show one on its own.

PITFALLS AND FIRST STEPS

Seven traps to avoid

ASD's transition guidance lists the mistakes it expects most often. Most come from treating the Essentials as the Essential Eight with new labels.

1 **Treating phases as maturity levels**
Phases order the work. They are not ratings.

2 **Claiming equivalence**
A control that passed the Essential Eight is evidence, not a rating.

3 **Assessing the enterprise**
Rate each action in each domain it applies to.

4 **Deferring the capability domains**
Governance and culture, and Visibility and response, start in phase 1.

5 **Doing every domain at once**
Effort spread across the estate dilutes progress.

6 **Reusing stale evidence**
Evidence must reflect the system as it runs today.

7 **Overlooking new requirements**
Some actions have no Essential Eight equivalent and need fresh funding.

FIRST MOVES

01 Record the current Essential Eight position, exceptions and planned work.

02 Agree executive accountability, risk appetite and the reporting format.

03 Scope your chapter's phase 1 domains and both capability domains.

04 Run the gap analysis and open an evidence register.

05 Start an exception register with owners and expiry dates.

06 Set a risk-based reassessment cycle.

Effective cyber security has no completion date.

APPENDIX

References

This is a briefing by Principia Ratio. It summarises and adapts the ASD Essentials series, © Commonwealth of Australia 2026, used under a Creative Commons Attribution 4.0 licence. The selection, wording and charts are Principia Ratio's. ASD does not endorse this briefing or Principia Ratio.

OVERVIEW PUBLICATIONS

[1] What is the Essentials?

[2] The case for change

[3] The Essentials for senior executives

[4] Which chapter should I start with?

[5] AI considerations within the Essentials

ENVIRONMENT CHAPTERS

[6] ASD Essentials for enterprise IT

[7] ASD Essentials for cloud

[8] ASD Essentials for OT

SUPPLEMENTARY GUIDES

[9] Transitioning from the Essential Eight

[10] Implementation planning guide

[11] Assessment process guide

[12] Asset scoping guide for cloud

[13] ASD Essentials series reading guide

The Australian Signals Directorate published the first 13 references in Canberra in 2026. All are available at cyber.gov.au.

ALSO CITED IN THE SERIES

[14] Information Security Manual. Australian Signals Directorate; cyber.gov.au

[15] ATT&CK knowledge base of adversary tactics and techniques. MITRE; attack.mitre.org

[16] Cyber Assessment Framework. Britain's National Cyber Security Centre; ncsc.gov.uk