Australian Government

GUIDING PRINCIPLES TO EMBED ZERO TRUST CULTURE

Consultation Paper

November 2024

Purpose

The purpose of this consultation paper is to engage with interested stakeholders on the *"Guiding Principles to embed a Zero Trust Culture".* These Guiding Principles provide direction on the development of the policy uplift activities required to embed a zero trust culture across the Commonwealth.

The success of these initiatives, such as developing a whole-of-government zero trust culture, relies on an aligned, collaborative approach with all impacted stakeholders. As the Department considers the application of zero trust practices to Commonwealth entities through the PSPF 2025 update, we are eager to ensure a common understanding and closer engagement with industry.

These Guiding Principles are the first instalment of a coordinated consultation agenda facilitated by the Department of Home Affairs. As we move towards the adoption of practices such as zero trust, we also need to consider updates to existing publications, such as the Australian Government Gateway Policy, to support these changes. Additional consultation packages to support Commonwealth cyber security uplift initiatives, including the Hosting Certification Framework, will be released over the coming months.

The Guiding Principles have been developed alongside technical advice on zero trust by the Australian Signal Directorate's Australian Cyber Security Centre (ASD's ACSC).

Context

Shield 4 of **2023-2030 Australian Cyber Security Strategy**, highlights the importance of uplifting Commonwealth Government cyber security.

To achieve this, we are delivering a suite of policies for the Australia Government's cyber security capabilities to build resilient systems for the future. Commonwealth Cyber Security requires multiple lines of effort across business domains. Globally, we are seeing a growing focus for governments and industry to adopt zero trust practices, to provide a modern defensible architecture that offers a way to increase our systems cyber security resilience.

The concepts articulated in the Guiding Principles draw from the existing best practice and frameworks. They reflect areas that need to be strengthened to ensure our successful adoption of core paradigms, such zero trust practices.

The success of implementing zero trust practices cannot be achieved solely through a technology based approach. It requires organisational transformation to embed a 'zero trust culture' across an entity. Embedding zero trust culture does not mean we are promoting a lack of trust in our employees. An effective zero trust experience will empower employees through a clear understanding of roles and responsibilities, as well as providing a consistent experience across different IT platforms.

Embedding a zero trust culture allows opportunities to better combat the current and emergent risks stemming from a rapidly evolving cyber threat landscape and expansion of the digital attack surface, by shifting from a traditional strong perimeter protection focus to a zero trust architecture, rooted in the core principle of "never trust, always verify".

Through the Protective Security Policy Framework (PSPF) and the Hosting Certification Framework (HCF) and Systems of Government Significance (SoGS), we will consider how to strengthen the enabling concepts identified in the Guiding Principles, which will facilitate the secure adoption of contemporary technology and cyber security protections across the Australian Government's digital infrastructure.

Key Terminology

The following definitions and terms underpin the Commonwealth Government's *Guiding Principles to embed a Zero Trust Culture*:

Zero Trust:

Zero trust provides a collection of concepts and ideas designed to minimise uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. (United States National Institute of Standards and Technology - 800-207 | Nist.gov)

Zero Trust Architecture

Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilises zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan. (United States National Institute of Standards and Technology - 800-207 | Nist.gov)

Zero Trust Culture

A Zero Trust Culture is the term used to define the collective core enterprise level functions and activities required to underpin the application of Zero Trust.

Cyber resilience:

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. (Developing Cyber-Resilient Systems; A Systems Security Engineering Approach (nist.gov))

Cyber fluency:

Cyber fluency is the next step beyond cyber awareness – it is the ability to understand and apply knowledge of cybersecurity concepts, risks, and best practices across digital environments. It recognises that traditional cyber awareness is not enough to provide protection against the sophisticated threats of the modern age. Achieving cyber fluency requires an organisation's workforce to be sufficiently trained and has progress to a level of understand cyber security to the extent that it is automatically applied in their everyday work context. Cyber fluent individuals can apply this knowledge to safeguard systems and data, propagating a culture of cyber security understanding within organisations and communities.

Cyber resilience continuum:

The cyber resilience continuum terminology promotes the understanding that cyber security resilience is a continuous cycle that organisations are required to consider as a part of their broader business operations. It emphasises a proactive, adaptive approach, spanning readiness and response efforts to ensure systems can continue operating in an evolving cyber risk landscape.

Overview

The Commonwealth Government has five *Guiding Principles to embed a Zero Trust Culture.* The Guiding Principles are:

1. Identify and manage cyber security risk at an enterprise level.

Principle 1 increases the resiliency of the Australian Government's digital landscape by ensuring cyber security risk is considered at an enterprise level. In a world of digitalised services, managing cyber security risk should not be considered the responsibility of the CISO, but should be managed at the enterprise level.

Cyber risk **must** be treated as an enterprise level concern, integrated fully into the organisation's broader risk management framework and considered in critical business operation decisions. While eliminating cyber risk is impossible, effective foundational strategies can be used to mitigate this risk profile within the organisation's defined risk appetite.

To operationalise this principle, organisations will need to define cyber security risk at an enterprise level to ensure its integration and management throughout IT management and investment processes. This will ensure that cyber risks are continuously evaluated, dynamically treated and aligned with the enterprise's overall risk tolerance.

2. Understand accountabilities and responsibilities at all levels.

Principle 2 articulates that clear roles and responsibilities are both a fundamental requirement to establish a zero trust culture and a key to ensure Commonwealth increase their cyber security resilience.

Effective governance requires the establishment and maintenance of strong accountability mechanisms enforced from the highest levels, coupled with a commitment to cultural change, through both the designated technical senior executive roles and the entire senior executive suite, inclusive of the more traditional corporate facing roles.

To operationalise this principle, will understand and define roles and responsibilities further in order to effectively establish zero trust culture foundations. Secondly, entities must implement well defined reporting lines that ensure timely updates on emerging trends and regular assessments of organisational cyber security risk.

Clear definitions and understanding of roles and responsibilities at all levels ensures a consistent understanding of accountabilities and escalation pathways, enabling the organisation to respond and adapt swiftly to evolving challenges from the emerging threat environment.

3. Know and understand your most critical and sensitive technology assets.

Principle 3 requires entities to know and understand their most critical and sensitive technology assets. Embedding a zero trust culture not only requires an understanding of inventory, but also the context of business criticality. Business continuity and sensitivity need to be considered and aligned with the asset inventory, providing essential context to prioritise and implement appropriate risk mitigations.

To ensure an understanding of how to protect these critical assets, it's crucial to move our workforce beyond basic cyber literacy and towards cyber fluency, ensuring decision-makers at all levels can seamlessly navigate and respond to cyber threats in the moment. Identifying the critical functions and systems for business continuity, especially during cyber incidents, is just the start. Organisations must go further by embedding continuous cyber education and executive level training that emphasises fluency, empowering leaders to fully understand the risks and integrate cybersecurity into strategic planning. This shift enables a proactive, risk based approach, rather than reactive compliance.

4. Maintain resiliency through a comprehensive cyber strategy and uplift plans.

Principle 4 seeks to uplift the resiliency of the Commonwealth entities by requiring them to develop, maintain and foster a robust cyber strategy which is essential for enhancing cyber resilience. Central to this strategy is the identification of key digital assets and a thorough inventory, including critical systems and data.

To meet this principle, entities need a proactive approach that considers both current and predicted future threat trends to strengthen the organisation's cyber resilient posture. Cyber security requirements should be incorporated through entities digital investment plans, ensuring cyber security uplift activities are commensurate to planned digital investment and business operation changes.

Additionally, a comprehensive cyber resilience strategy and uplift plan must address the risks and dependencies tied to key third-party suppliers, ensuring a holistic approach to risk management.

5. Go beyond incident planning

Principle 5 seeks to shift entities to look beyond the traditional incident planning mechanisms such as standard incident response plans and consider that the incident has already occurred – they are just yet to discover it. To align with the zero trust paradigms —"assume breach" and "never trust, always verify"—cyber incident planning must be built on the premise that no system or user is inherently secure and that it should be initially treated as if it has already been breached.

Government entities must not only implement scenario based incident response plans with clear, predefined roles and responsibilities, but also continuously verify the integrity of all systems through established capabilities such as automated threat hunting and vulnerability scanning.

To meet the intent of this principle, incident management must go beyond the initial preparation, containment and eradication focus and should also drive continuous improvement in the entity's cyber posture. It should be ingrained in the organisation's entire operational framework, integrating cyber security response with business continuity and disaster recovery efforts.

Levers for change

The "*Guiding Principles to embed Zero Trust Culture"* will be applied through requirement changes released in the Protective Security Policy Framework 25 annual release; the Hosting Certification Framework; and the Resilient Digital Infrastructure framework.

1. The Protective Security Policy Framework provides updated guidelines and standards that reinforce security at every level, aligning organisational practices with Government security mandates. Integration of the Guiding Principles within the PSPF 25, in conjunction with the technical guidance provided by the Australian Signals Directorate, will provide organisations with the foundational requirements essential to progress on their zero trust journey.
2. Additionally, the Hosting Certification Framework reforms will consider how zero trust should be aligned with industry, through the assessment and validation of the security posture of cloud and hosting services provided to Commonwealth entities.
3. The Resilient Digital Infrastructure framework consolidates several key policies governing the security of IT infrastructure within the Australian Government, including

the Secure Cloud Strategy and Australian Government Gateway Policy, into a singular policy framework. The Department will reform and release the Australian Government Gateway Policy in 2025.

Together, these mechanisms act as powerful levers for change by setting consistent, high standards that encourage a culture of continuous verification, risk mitigation and further our journey on the cyber resilience continuum.

Submission Guidance

This consultation paper offers “Feedback Consideration” points at the end of the document. These are not mandatory questions. They have been designed to provide guidance to facilitate constructive feedback to help identify the activities and changes that will best facilitate embedding a zero trust culture across Commonwealth entities.

Response from entities will help the Department to develop requirements for the Hosting Certification Framework, Protective Security Policy Framework 25 and the Resilient Digital Infrastructure.

Feedback Considerations

1	In your experience, what key factors contribute to the successful identification of cyber risks across different business units? How should the Commonwealth foster and maintain collaboration among these groups?
2	Are there preferred frameworks or standards used by your organisation to identify and assesse cyber security risks across your organisation, including both internal systems and third party services?
3	How should the Commonwealth ensure that cyber security roles and responsibilities are defined and communicated across different levels of their organisation, from executive leadership to frontline staff?
4	How does your organisation ensure that all employees, regardless of their role, understand their responsibility in achieving cyber resilience? How often are training programs provided, and how is the effectiveness of the programs measured?
5	How do you ensure that roles and responsibilities related to cyber security are clearly defined and maintained across diverse client and supply chain portfolios?
6	What requirements and policies are most effective to ensure that all areas within an organisation (technical and non-technical) develop a necessary baseline understanding of cyber security concepts applicable to their role?
7	What modified or new requirements would you recommend for the PSPF, HCF or the Whole of Government Gateway policy to embed zero trust culture?
8	What requirements would you recommend to ensure that effective metrics and benchmarks are implemented?
9	What requirements or policy change would you recommend to ensure alignment between your broader cyber strategy and individual uplift plans? What governance or oversight mechanisms are in place to coordinate these efforts?

10	What Zero Trust capabilities have you already applied within your organisation? How long have you been implementing these? List the benefits and issues associated with these measures.
11	How do you manage distributed accountability, such as situations where multiple vendors or third-party providers are involved in delivering cyber security services for a government client? What mechanisms do you have in place to ensure coordination and clear responsibility?