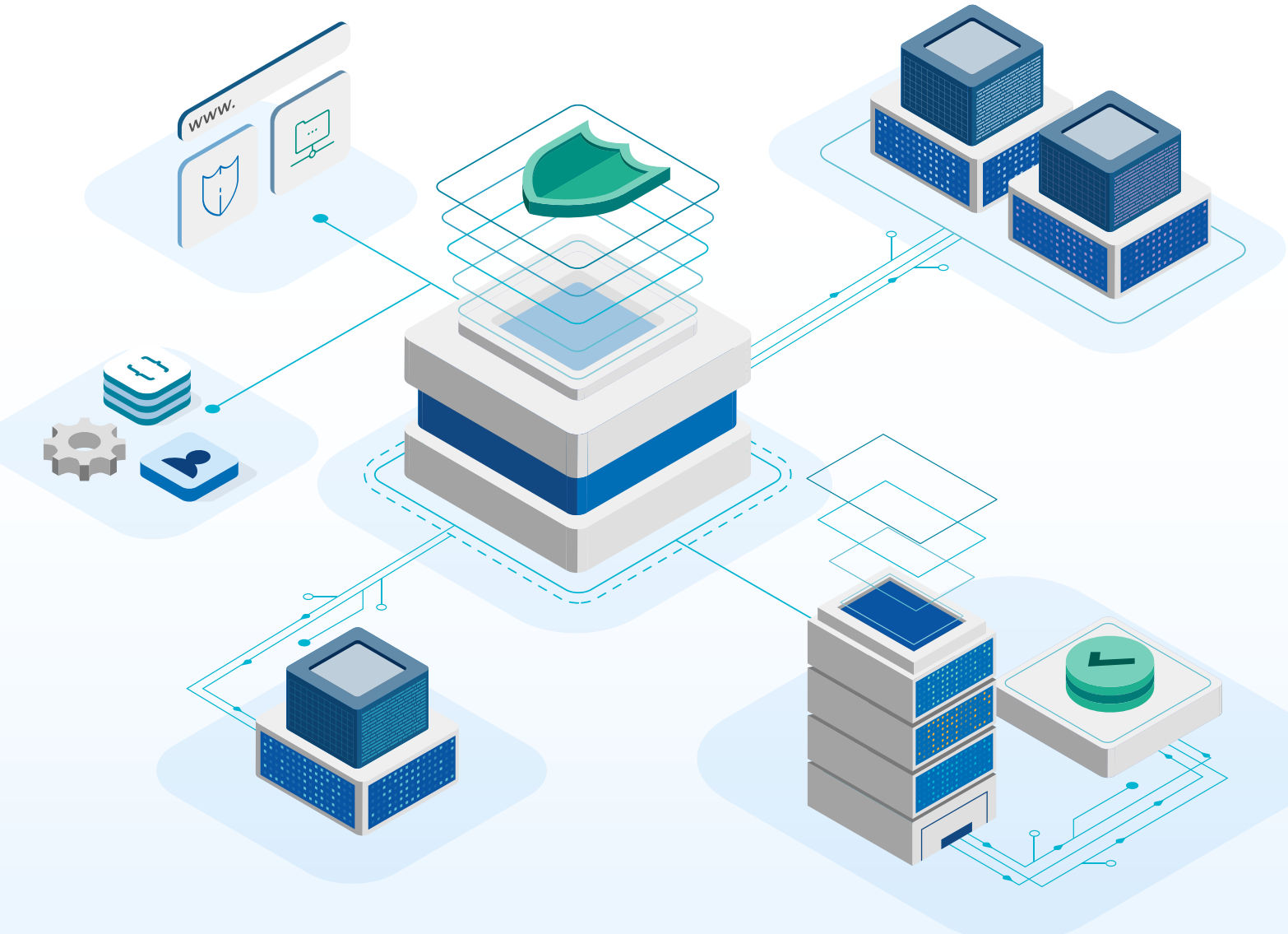
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Foundations for modern defensible architecture



Content complexity
MODERATE

Table of contents

Foundations for modern defensible architecture

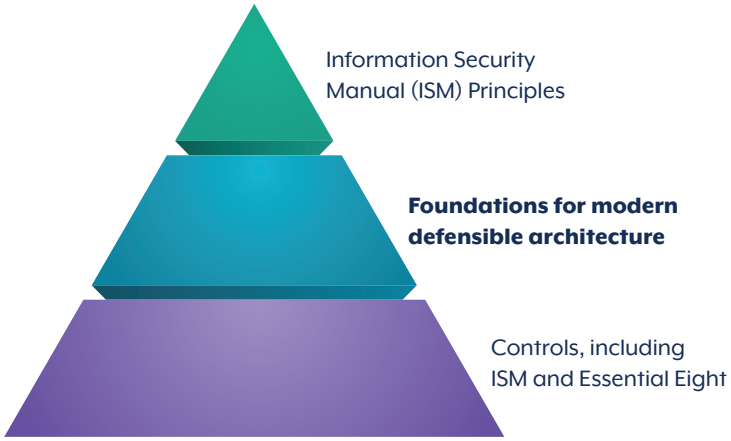
Australian organisations, industries and individuals continue to be the target of malicious cyber actors. Cyber security has become increasingly complex as organisations embrace flexible working, technologies rapidly develop, and the threat environment evolves. The nature and persistence of cybercriminals targeting Australian networks is such that organisations should adopt a stance of 'when' not 'if' a cyber security incident will occur. The threat has also made it increasingly difficult for network defenders to prevent cyber security incidents. However, steps can be taken in the design, architecture and build of networks to significantly minimise the risk and harm to a network's most critical assets and systems should an incident occur, while also increasing their resilience.

This publication introduces modern defensible architecture as an approach to assist organisations in applying consistent, foundational aspects to build, maintain, update and enhance their systems. The Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC) Foundations for Modern Defensible Architecture (the Foundations) provide a baseline of secure design and architecture activities that will best prepare organisations to adapt to current and emerging cyber threats and challenges.

This guidance is informed by ASD's experience in responding to cyber security incidents, and performing vulnerability assessments and penetration testing of Australia's critical networks. It is also informed by technical cyber security practices such as zero trust and secure-by-design, which have emerged as better-practice approaches to increase cyber resilience.

The Foundations offer additional secure design and architecture advice as a structural framework upon which to implement ASD's *Information Security Manual* (ISM) and ASD's *Essential Eight Maturity Model*. Properly implementing ISM controls and Essential Eight mitigation strategies remains important for mitigating targeted cyber intrusions and malware in information technology environments. However, no set of mitigation strategies guarantees the prevention of all cyber security incidents, and both controls and mitigations are dependent on changes to technology and the threat environment. Implementing mature security architecture will ensure a network is able to maintain its resilience over time and adapt as controls and mitigations evolve. This publication sets out how mitigation strategies and controls can be complemented by security architecture to increase network resilience.

The below diagram illustrates the relationship between ISM principles and strategic guidance; the Foundations; and controls – practical guidance offered in both the ISM and essential eight. All layers are important to protect from cyber threats and should be considered by organisations.



Audience and scope

This publication is written for technical security and enterprise architects who are responsible for designing and building information technology (IT) environments.

While this publication provides recommendations targeted at securing corporate IT systems that support a workforce consisting of internal users, at a high level, it is applicable to all types of environments.

This publication assumes an advanced level of computing and cyber security knowledge on the part of the reader.

What are the Foundations?

The Foundations have been developed to assist organisations to prepare and plan for the adoption of technologies based on:

1. Zero trust principles of "never trust, always verify", "assume breach" and "verify explicitly", implemented through zero trust architecture components and capabilities
2. Secure-by-design practices that institute a security-first mindset within organisations when it comes to procuring or developing software products and services.

Many of the individual architectural foundations covered in this guidance are not new concepts, but when combined they provide the ability to build a modern defensible architecture that is adaptable to emerging technologies and practices, and resilient to current and emerging cyber threats and challenges.

Organisations should regularly review their own architectural designs and decisions against each Foundation to ensure they remain resilient and improve their cyber security maturity over time.

How do the Foundations work?

Each Foundation represents an organisational goal or capability that will facilitate a more efficient adoption of zero trust technologies and architecture. Organisations should work towards each Foundation to improve their zero trust maturity and capabilities to achieve a modern defensible architecture. Implementing each Foundation contributes to a defence-in-depth approach which protects the most critical systems and data, first to prevent or limit the spread of cyber incident and impact to critical business operations.

The Foundations are designed to be technology agnostic. They allow organisations to make guided decisions on investment opportunities and design considerations, and to identify technologies that are consistent with their requirements and zero trust architectural advancements.

The Foundations recognise that every organisation is different, and the way they approach and prioritise implementation will be unique to their organisational strategy and business objectives. The Foundations do not represent any order of priority for implementation, and organisations are encouraged to plan for implementation of each Foundation as appropriate to their organisational context.

Designing and implementing architectural improvements to an enterprise environment will take significant time, resources and investment. Organisations should ensure that effort is applied to hardening and protecting existing systems by leveraging mature frameworks and prioritised mitigation strategies, such as ASD's *Essential Eight Maturity Model*. An organisation that works towards implementing a higher maturity level of ASD's Essential Eight will be well placed to adopt future guidance for achieving modern defensible architecture.

ASD's ACSC has considered international advice and guidance on zero trust architecture alongside existing Australian government frameworks including the *Protective Security Policy Framework* (PSPF), *Hosting Certification Framework*, cloud strategies, *Gateway Policy* and guidance, and technical advice, including ASD's ISM and Secure-by-Design publications.

Key terms

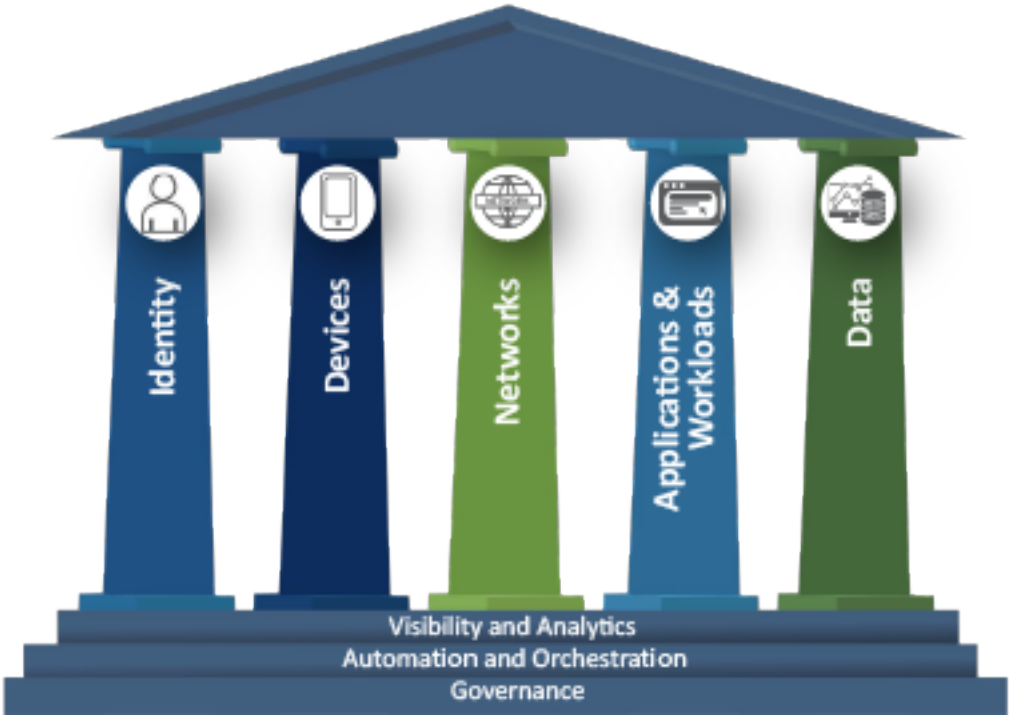
The following terms appear throughout the Foundations:

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 (NIST) 800-207)

Zero trust architecture is an enterprise's cyber security 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. (NIST-800-207)

This publication refers to the United States National Security Agency (NSA) **zero trust principles**: "Never trust, always verify", "Assume breach", and "Verify explicitly". These principles outline the objectives for operational capabilities that support a zero trust solution. More information on each of these principles is found at the end of this document.

This publication refers to the United States Cybersecurity and Infrastructure Security Agency's (CISA) **zero trust pillars**: Identity, Devices, Networks, Applications and Workloads, and Data. These pillars represent distinct technology areas in which organisations may advance their zero trust implementation over time. More information on each of these pillars is found at the end of this document.



Zero Trust Maturity Model Pillars. *Source: CISA Zero Trust Maturity Model v2.0*

Feedback

The Foundations are the first step in ASD's drive to champion modern defensible architecture as a key approach for building cyber resilience. The Foundations are intended to form the basis for future advice and guidance on modern defensible architecture, including more detailed guidance on each individual Foundation, architectural patterns, investment and measurement.

This publication is aimed at organisations across the private and public sectors looking to increase their cyber resilience, particularly those considering or adopting zero trust technologies and architecture and secure-by-design practices.

ASD would value hearing from you on:

- suggested improvements to the Foundations
- suggestions for alternative environments on which to develop further recommendations, including Critical Infrastructure and Operational Technology organisations
- further advice and guidance you would like to see developed via our future work program
- any case studies, experiences or lessons learned you wish to discuss or provide to inform our future work.

If you would like to provide written feedback, or have any questions regarding the Foundations, please email us at acsc.sda@asd.gov.au.

The Foundations are being released in parallel with the Department of Home Affairs' (Home Affairs) consultation publication, *Guiding Principles to Embed a Zero Trust Culture*, which seeks comments on proposed policy principles to inform government adoption of zero trust principles and technologies. We encourage government service providers and organisations to also consider the Home Affairs' consultation paper.

Foundation 1: Centrally managed enterprise identities

Zero trust pillars: All

Organisations need to reduce the number of authoritative sources for enterprise identities in their information environments by using centrally managed solutions. This approach provides organisations with a more holistic view of their users, including their roles and responsibilities, which assists in making risk-based decisions on user access requests and permissions. It additionally gives a greater ability to track users through organisational changes, including when staff change responsibilities or depart from their roles.

The following outline recommendations for implementing the centrally managed enterprise identities Foundation:

- Non-user identities should be captured and managed within centrally managed solutions, including service identities and device identities, such as those used by Internet-of-Things (IoT) devices and software.
- All user and non-user identities should be granted the minimum privileges required to perform their functions correctly.
- Centrally managed identity solutions should share data about identities with other enterprise systems, including authentication, authorisation and security monitoring software.
- Identity information should be sourced from external systems, such as those used by personnel security, human resources and contract management teams.
- Identity information, both sourced and centrally managed, should maintain its accuracy through change and release management processes.
- When procuring new hardware, software and services, the requirement for compatibility with an organisation's identity management system should be a high priority.
- A centrally managed solution should facilitate integration with external organisations and cloud services, especially when the organisation provides access to external or guest users.

Foundation 2: High assurance authentication

Zero trust pillars: Identity, Devices, Networks and Application & Workloads

Organisations require a trusted and strong authentication model, to protect user and device credentials from compromise by common attacks.

The following outline recommendations for implementing the high assurance authentication Foundation:

- Authentication requirements should be integrated at the application layer, rather than the network layer, to provide visibility and assurances of a user's particular activities.
- Organisations should align the choice of approved authentication solutions to the potential business impact of compromise, and to provide the necessary assurances that the claimant controls the authentication factors.
- The level of assurance can change between systems and roles based on what activities a user is able to perform. Organisations should standardise the level of assurance across the workforce to the most secure option that suits the organisation's requirements.
- Organisations must prioritise technology solutions that support cryptographically secure, phishing resistant multi-factor authentication, such as passkeys and smartcards.
- For non-user identities, authentication should be achieved through factors that are tightly bound to the service or hardware, such as trusted digital certificates.
- Device identities should be required to authenticate to the network before they are allowed to communicate with other resources.
- Mutual Authentication should be used to communicate between services to provide confidence that both services are genuine.
- Organisations should prioritise investment in technologies that support cryptographic credential binding to the device and the service being used. Cryptographic credential binding enhances the authenticated session security for unmanaged endpoints, such as bring-your-own-device (BYOD).

Foundation 3: Contextual authorisation

Zero trust pillars: All

Organisations need to ensure that access to enterprise resources is initially, and continuously, authorised based on defined levels of trust, using the context of the sessions and resources to gain confidence in the access request.

The following outline recommendations for implementing the contextual authorisation Foundation:

- To evaluate the level of trust, session context should be available to the authorisation model as signals and confidence indicators. This includes attributes such as time of request, location of endpoints, network source, user roles, credential type and endpoint health. Resource attributes, such as sensitivity labels and data type, are required to determine which access policies should be used by the authorisation model.
- The authorisation model should assume that no session has inherited trust, and that a minimum set of confidence indicators are essential to attain and retain the required level of trust for access.
- The authorisation model should be capable of managing sessions based on an organisation's access policies, including the use of multiple confidence indicators to evaluate whether the access remains in a trusted state.
- Access policies should identify the expected values of session attributes to provide indicators of confidence to the authorisation model.
- The policies that define the attributes and their expected values should be developed in a secure way, ensuring they maintain a high level of integrity and availability during storage and communication.
- To keep an ongoing session secure, user access needs to be continuously evaluated based on the activities taking place within a session, as well as other information that may indicate a drop in confidence, including changes in software state, security posture or behavioural analysis.
- Organisations should prioritise technology solutions that support dynamic authorisation policies, which can adjust the level of confidence required for access based on broader organisational context, such as an ongoing incident or known exploitable vulnerabilities being identified.
- Organisations should design and develop their information environments and software to be integrated with their chosen identity management solutions, and authorisation and access model. This includes defining system boundaries where authorisation model decisions can be enforced.
- Authorisation decision enforcement points should have the ability to generate and communicate ongoing environmental and session context for the continuous access evaluation.

Foundation 4: Reliable asset inventory

Zero trust pillars: All

Organisations need to have complete and comprehensive knowledge of all endpoints, networks, applications, identities and data stores that contain organisational information, including in services and environments not directly managed by the organisation. This is achieved through an accurate and reliable inventory solution which continuously identifies and records information on an organisation's assets and resources.

The following outline recommendations for implementing the reliable asset inventory Foundation:

- Information from the asset inventory should be accessible by security software for analysis, and authorisation solutions for evaluating and assessing access requests.
- The inventory should record information about the relationships between assets. This includes what endpoints, networks and applications interact with data and workloads, including whether they have the requirement to access, transmit, store or process sensitive data.
- The automatic discovery of assets should be supported to streamline the detection of components that exist in highly dynamic or short-lived environments, such as in systems that are designed to scale based on processing needs.
- Software that can automate the discovery of assets should be configured to detect and analyse the removal of assets from the environment and provide that information to the relevant teams and monitoring solutions.
- An asset's lifecycle changes should be recorded and analysed by the solution, ensuring that only approved assets are added, changed or removed, and unauthorised operations are blocked and reported.
- Organisations should prioritise technology solutions that support security alerting, to prevent unauthorised assets being connected to the organisation's information environment.

Foundation 5: Secure endpoints

Zero trust pillars: Devices and Applications & Workloads

Organisations need to harden and configure all endpoints to provide protection against cyber threats and mitigate weaknesses in software and hardware.

The following outline recommendations for implementing the secure endpoints Foundation:

- Information on an endpoint's current state of health should be continuously consumable by the authorisation model as an input to evaluate trust.
- Priority should be given to real-time attestations of an endpoint's conformance with a security baseline, with stored historical data being treated as lower confidence.
- All organisationally managed endpoints and endpoint software (including operating systems) should be hardened with ASD and vendor hardening guidance where possible.
- All hardened configuration baselines should be recorded in a secure way, ensuring they maintain a high level of integrity.
- Endpoints and software should be monitored for changes to configuration, or operational settings, and alerts should be generated when these drift from the recorded baselines.
- Endpoints and software that have drifted from recorded baselines should provide low confidence indicators to the authorisation model and have access to resources limited accordingly.
- Endpoints not owned or managed directly by an organisation, such as bring-your-own-devices (BYOD), should provide low confidence indicators to the authorisation model. Systems that are commonly accessed by these endpoints should be architected to mitigate attacks that are likely to come from compromised systems.
- Highly sensitive and privileged activities should require endpoints that are managed by the organisation, with continuously verified and high confidence indicators of the endpoint's security baseline.
- A comprehensive endpoint solution will include technologies that can respond to deviations by automatically restoring software back to the required secure configuration baseline.
- The systems that evaluate security baselines should communicate back to a centralised repository where endpoint status can be used by the authorisation model.

For more information on ASD hardening guidance, please visit Guidelines for System Hardening.

Foundation 6: Reduced attack surface

Zero trust pillars: Devices, Networks, Applications & Workloads, and Data

Organisations need to minimise exposure of their attack surface to cyber threats and malicious actors. This can be achieved by reducing the number of services that communicate with networks of lower trust, as well as limiting the exposure of resources to networks where there is no logical requirement or a significant security risk.

The following outline recommendations for implementing the reduced attack surface Foundation:

- Organisations should consider the exposure of systems they do not own or operate that contain organisational data, including cloud services and externally hosted source code repositories.
- Organisations should restrict access to unauthorised external services, specifically cloud applications, email services and file sharing applications.
- All applications and networks should be designed and configured to only be visible to networks and resources that are required for them to perform their operations.
- Organisations should have a capability to verify that applications and networks are not exposed to untrusted environments.
- Internally managed applications that are required to be accessed remotely should do so in a way consistent with the organisation's authorisation model and without relying solely on protections at the network layer.
- Organisation endpoints should have the minimum set of applications installed to meet business requirements and should be managed securely, including through the deployment of security patches and the removal of unnecessary features and functions.
- Organisations should develop a capability with vulnerability and attack surface management tools, to quickly and accurately respond to new potential cyber threats to reduce the attack surface of vulnerable systems.
- Endpoints that have vulnerable business-critical software that cannot be updated, patched or upgraded should be isolated from other resources when not being utilised, with the intent to replace the software as soon as possible.

Foundation 7: Resilient networks

Zero trust pillars: Devices & Networks

Organisations need to build resilient networks derived from an organisation's business requirements, noting these evolve organically over time. Organisations can take proactive steps to reduce the business impact of system testing and maintenance to improve network resiliency, and to identify architectural and operational flaws. Organisations need to ensure data being communicated over their network is safe from tampering, interception and exfiltration, while protecting service and system availability from impacts, such as network failures, system compromises and denial-of-service attacks. Networks should be designed to allow for only secure and authenticated identities to communicate with other resources, using the context of the request to dynamically determine confidence in the validity of the communication.

The following outline recommendations for implementing the resilient networks Foundation:

- Organisations should prioritise technologies that support high availability and automated failover in the event of a device or service failure.
- Organisations should test their networks through table-top exercises, penetration tests, threat modelling, redundant network path failure testing, load testing, and simulated device failure testing.
- Organisations should periodically evaluate network architecture to identify opportunities to improve network resiliency
- Organisational networks should be configured with secure protocols using ASD-approved cryptographic protocols and leveraging secure and verifiable technologies.
- All data that is communicated over enterprise networks should be encrypted and configured to meet contemporary security standards and established better practices.
- Organisations should actively deprecate weak or vulnerable network protocols as hardened and encrypted versions are standardised.
- Monitoring of network device configurations should be implemented to ensure that security policies are being enforced across segments and environments.
- Organisations should evaluate the threat of compromise in traffic capture and monitoring solutions, including the threat of data collection from capture devices that decrypt traffic for inspection.
- Organisations should design and define logical network boundaries that restrict lateral connections between resources based on the context of a request, to prevent compromised endpoints impacting other endpoints in the environment. Networks can be segmented in accordance with these boundaries.
- All network technologies that are introduced into an organisation's environment should be designed with modern approaches to security and privacy, including the customisation of chosen protocols and ciphers.
- Organisations should invest in secure networking technology solutions that support their users' operational behaviours, such as remote working and bring–your–own–device (BYOD), while considering how these behaviours may impact the security of software and data.

For more information on ASD-approved cryptographic protocols, please visit Guidelines for Cryptography.

Foundation 8: Secure-by-design software

Zero trust pillar: Applications & Workloads

Organisations need to procure and develop software that is built with a security-first approach. Secure-by-design principles and tactics should be applied to all software that is used by the organisation. Software that is built with secure-by-design principles and practices is less likely to have exploitable weaknesses, which can reduce the likelihood of incidents occurring.

The following outline recommendations for implementing the secure-by-design software Foundation:

- Software that enables an organisation to analyse and implement technical policies should be secure and verified before use. This includes the software used to develop, store and implement access policies, as well as any software that provides information as an input to the authorisation model.
- Organisations should prioritise software that is compatible with their identity management solutions and authorisation model.
- Procurement teams should work closely with technical teams to determine the technical features and business requirements for new software. Software needs to be evaluated to ensure it can operate within an organisation's environment, including automatic measurement against known secure baselines and security event logging to support incident response.
- Software that is used to deploy infrastructure and applications should be developed with the principles of immutability and idempotence. These characteristics will assist organisations in preventing weaknesses from being introduced to a system outside of approved change management decisions. The use of these principles will also assist in the recovery of systems after an incident has been recognised, by having the ability to quickly redeploy or reconfigure systems.
- Organisations should confirm that threat models are leveraged by manufacturers and have been utilised to mitigate the most likely cyber threats and weaknesses.
- Each application introduced into the organisation should be assessed prior to deployment to ensure it has been designed and built to be protected 'out of the box' against known prevalent cyber threats.
- Before procuring software, organisations should evaluate the manufacturer and/or vendor for risk associated with their security practices, their reputation and their ability to quickly and effectively secure their products.
- SecDevOps practices should be embedded in organisational processes. This includes ongoing training and upskilling of development and operations teams to keep up to date with software advancements and prevalent cyber threats.
- Development teams should be aware of risks within their software supply chains, including the generation and consumption of a software bill of materials (SBOM) to ensure third-party components have no known vulnerabilities.

For more information on choosing secure and verifiable technologies, please visit Choosing secure and verifiable technologies.

Foundation 9: Comprehensive assurance and governance

Zero trust pillars: All

Organisations need to perform assurance activities that enable decision makers in the governance structure to be able to make decisions on security actions and priorities.

The following outline recommendations for implementing the comprehensive assurance and governance Foundation:

- Organisational assurance activities should be developed and delivered in accordance with relevant industry and government regulations and standards, and the outcomes regularly reported to the appropriate level of senior management.
- Organisations should dedicate appropriately skilled resources and time to the initial and ongoing assurance and verification of the security and resilience of their systems.
- Systems should be regularly assessed for their resilience against current and emerging cyber threats and to quickly detect changes that impact the security posture of the organisation. Regular assessments include vulnerability scanning, penetration testing, control validation and user access reviews.
- Technical policies for access authorisation and security baseline requirements should be developed and stored on systems that are considered privileged, highly sensitive and hardened accordingly.
- Reviews and updates to policies based on cyber threat intelligence or changes in the environment should be regularly performed.
- Policies should be protected throughout their lifecycle, with monitoring applied to identify unauthorised changes, modifications or deletion actions.
- All new software and hardware should be assessed against approved and trusted assurance frameworks, including necessary technical governance and assurance testing.
- Assurance testing processes should be developed to be repeatable and automatable, to enable them to be run regularly with minimal human intervention.
- Outputs of assurance tests should be stored and protected from compromise and be consumable by an organisation's authentication and authorisation models.

Foundation 10: Continuous and actionable monitoring

Zero trust pillars: All

Organisations need to monitor and respond to all identified and suspected security incidents in a timely and efficient manner, including through the automation of time-critical response actions.

The following outline recommendations for implementing the continuous and actionable monitoring Foundation:

- Monitoring systems should be configured with organisational knowledge to recognise behaviours and indicators that identify potential compromise, or likelihood that compromise could occur. The data sources used must have a high assurance of integrity to reliably inform both alerting and monitoring activities.
- The organisation should ensure that the development and configuration of automated response actions are done in accordance with the organisational risk appetite and tolerances. All actions that are triggered by automated response systems should be monitored for further impacts, and reverted if unforeseen outcomes are detected.
- Monitoring activities should be informed by up-to-date and trusted threat intelligence sources, including from services that automatically deliver new data.
- Threat intelligence data that includes indicators of compromise should be analysed against existing systems as soon as practical.
- Systems where an indicator of compromise is detected should be automatically managed according to organisational risk tolerances, including removing the system from the network or restricting user access until the incident can be investigated and remediated.
- When an incident is discovered, the response activities should be automated where possible to reduce the impact, such as the spread of malicious code, lateral movement of malicious actors, and the misuse of access privileges. By quickly responding through automation, an organisation can increase the chances of a quick recovery and return to normal operations.
- All endpoints and software in an organisation should have the capability to generate and communicate quality and high-fidelity signals about security events, including in logs, state, and system telemetry and behaviour.
- Organisations should seek out vendor and manufacturer advice on events and patterns of behaviour in their software and services that could be an indicator of compromise. This information should be implemented in the organisation's security monitoring solutions and alerted on when detected.

For more information on monitoring and detection, please visit Guidelines for System Monitoring and Identifying and Mitigating Living Off the Land Techniques.

Zero trust principles and pillars

The following principles and pillars are applied throughout the Foundations:

Zero trust principles:

1. **Never trust, always verify** – Treat every user, device, application/workload and data flow as untrusted. Authenticate and explicitly authorise each to the least privilege required using dynamic security policies.
2. **Assume breach** – Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinise all users, devices, data flows and requests for access. Log, inspect and continuously monitor all configuration changes, resource accesses and network traffic for suspicious activity.
3. **Verify explicitly** – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources. (NSA – Embracing a Zero Trust Security Model)

Zero trust pillars:

1. **Identity:** An identity refers to an attribute or set of attributes that uniquely describes an organisation user or entity, including non-person entities.
2. **Devices:** A device refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, IoT devices, networking equipment, and more.
3. **Networks:** A network refers to an open communications medium, including typical channels such as organisational internal networks, wireless networks, and the Internet, as well as other potential channels, such as cellular and application-level channels used to transport messages.
4. **Applications and workloads:** Applications and workloads include organisational systems, computer programs, and services that execute on-premises, on mobile devices and in cloud environments.
5. **Data:** Data includes all structured and unstructured files and fragments that reside or have resided in systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata. (CISA – Zero Trust Maturity Model 2.0)

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the Essential Eight Maturity Model prioritises the implementation of controls to mitigate different levels of malicious actors' tradecraft and targeting.

Reference material:

- United Kingdom's National Cyber Security Centre (NCSC-UK) Zero Trust Architecture Design Principles: Outlines zero trust principles for organisations looking to design and implement a zero trust architecture in an enterprise environment.
- Canadian Centre for Cyber Security (CCCS) A Zero Trust Approach to Security Architecture – ITSM.10.008: Provides a description of zero trust security concepts and how organisations can benefit from implementing a zero trust architecture to safeguard their assets.
- NIST SP 800-207, Zero Trust Architecture: NIST's foundational technical publication that gives a conceptual framework for zero trust. While not comprehensive to all information technology, it can be used as a tool to understand and develop a zero trust architecture for an enterprise.
- NIST SP 1800-35, Implementing a Zero Trust Architecture: A series of guides that summarises how the United States government and identified vendors are using commercially available technology to build interoperable, open standards-based zero trust architecture.
- CISA's Zero Trust Maturity Model V2: Designed to provide United States Federal agencies with a roadmap and resources to achieve an optimal zero trust environment.
- CISA's Cloud Security Technical Reference Architecture: Provides strategic and tactical guidance for the adoption of cloud services.
- National Security Agency, Advancing Zero Trust Maturity Series guidance on zero trust pillars: User, Device, Network and Environment, Data, Application and Workload, and Visibility and Analytics.
- National Security Agency, Embracing a Zero Trust Security Model: Explains the zero trust security model and its benefits, as well as challenges for implementation.
- United States DoD Zero Trust Reference Architecture: Describes DoD's end-state vision, strategy, and framework to strengthen cyber security. It provides technical guidance to evolve existing capabilities to focus on a data centric security strategy.

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

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 Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

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

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre