A GATHID LABS SERIES: EPISODE 1

Government Compliance and The Essential Eight

The Role of Identity and Access in the Essential Eight

The Essential Eight, developed by the Australian Signals Directorate (ASD), is widely regarded as a gold standard for mitigating cybersecurity threats. By implementing the eight prioritised security controls, organisations can dramatically reduce the risk of cyber incidents.

While the Essential Eight covers a broad range of security strategies, identity and access governance is at the heart of its effectiveness. Identity-related weaknesses—such as poor access controls, excessive privileges, and weak authentication—are the most common vulnerabilities exploited by attackers. Without strong identity governance and evidence of governance processes and procedures, achieving Essential Eight compliance is nearly impossible.

In this article, we'll examine the Essential Eight's maturity model, the critical role of identity and access governance within it, and how organisations can effectively implement identity controls to strengthen their security posture.

Understanding the Essential Eight and Its Maturity Model

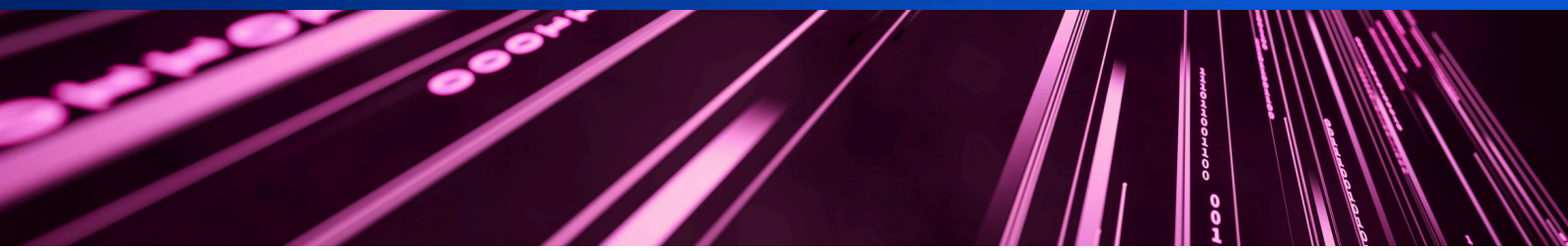
The Essential Eight consists of eight mitigation strategies designed to protect IT environments from cyber threats. These strategies are:

1. Application Control
2. Patch Applications
3. Configure Microsoft Office Macros
4. User Application Hardening
5. Restrict Administrative Privileges
6. Patch Operating Systems
7. Multi-Factor Authentication (MFA)
8. Regular Backups

The Essential Eight Maturity Model defines four levels of security maturity:

- **Maturity Level Zero**: No controls are effectively implemented, leaving the organisation vulnerable to basic attacks.
- **Maturity Level One**: Protects against attackers using widely available tools and exploits.
- **Maturity Level Two**: Defends against attackers who invest time in crafting more effective phishing campaigns or technical exploits.
- **Maturity Level Three**: Protects against adversaries who actively seek to bypass security controls and maintain persistent access.

While these strategies address various security layers, identity and access governance underpins several of them—especially Restricting Administrative Privileges and Multi-Factor Authentication (MFA). Without effective identity controls, an organisation cannot reliably achieve or maintain Essential Eight maturity.



Identity and Access: A Foundation of Essential Eight Compliance

A significant proportion of cyber incidents stem from identity-related failures. Credential theft, privilege misuse, and inadequate access management are among the most common attack vectors. By strengthening identity and access governance, organisations can dramatically improve their security posture across multiple Essential Eight controls.

1. Restrict Administrative Privileges: The First Line of Defence

Why it matters: Administrative accounts hold the keys to the kingdom—if compromised, attackers can move laterally across networks, install malware, and exfiltrate data. Understanding, reviewing and restricting administrative privileges limits the damage an attacker can do even if they gain access.

Key identity governance controls:

- **Least Privilege Enforcement**: Users should have the minimum permissions required to perform their job.
- **Dedicated Privileged Accounts**: Admins must use separate privileged accounts for administrative tasks, rather than everyday access.
- **Internet Access Restrictions**: Privileged accounts should be blocked from accessing the internet, email, or general web browsing to prevent credential theft via phishing.
- **Privileged Access Review**: Access to privileged accounts must be reviewed regularly to ensure users only retain necessary permissions.
- **Break-Glass Accounts**: Emergency admin accounts should be tightly controlled, with long, unique credentials and strict access logging.

At Maturity Level Three, administrative activities should be conducted through jump servers, and privileged account events should be centrally logged and analysed for suspicious behaviour.

2. Multi-Factor Authentication (MFA): Strengthening Identity Security

Why it matters: Passwords alone are no longer sufficient—attackers frequently steal credentials through phishing, brute force attacks, or database breaches. MFA adds an additional layer of protection, ensuring that even if credentials are compromised, attackers cannot gain access without a second authentication factor.

Key identity governance controls:

- **Mandatory MFA for All Users**: MFA should be enforced for all accounts, not just privileged users. Attackers often target regular user accounts to gain an initial foothold.
- **Adaptive MFA Policies**: Implement context-aware MFA that enforces stricter authentication based on risk (like unusual login locations or untrusted devices).
- **FIDO2 or Passwordless Authentication**: To further enhance security, organisations can move toward passwordless authentication methods that reduce the risk of stolen credentials.

At Maturity Level Three, MFA should be strictly monitored and enforced across all remote access systems, privileged accounts, and high-risk applications. Additionally, organisations should monitor and audit failed authentication attempts to detect potential compromise attempts.

3. Identity Management and Access Control: Beyond the Essential Eight

Although not explicitly called out as a separate control in the Essential Eight, strong identity governance with context is crucial to ensuring these controls are implemented appropriately.

Key identity management considerations:

- **Role-Based Access Control (RBAC)**: Ensures users are granted only the permissions necessary for their job function.
- **Joiners, Movers, and Leavers (JML) Processes**: Access rights must be managed throughout the employee lifecycle, ensuring:
  - New employees are granted appropriate access immediately.
  - Employees changing roles have permissions updated accordingly.
  - Departing employees have access revoked immediately upon termination.
- **Continuous Identity Monitoring**: Identity environments should be continuously mapped and monitored to detect:
  - Stale or orphaned accounts
  - Privilege creep
  - Anomalous login behaviours

How to Strengthen Identity and Access Governance for Essential Eight Compliance

To achieve a high Essential Eight Maturity Level, organisations must implement proactive identity governance strategies. Below are three steps to strengthen access controls.

Step 1: Map and Model Identity Risks

Before making changes, organisations must first gain visibility into their identity environment. This includes:

- Mapping all identities, access permissions, and entitlements across on-premises and cloud systems.
- Identifying unowned accounts, excessive privileges, and unused admin accounts.
- Conducting an access risk assessment to understand where the biggest security gaps exist.

Step 2: Implement Role-Based Access and Least Privilege Controls

Once identity risks are understood, organisations should:

- Define clear role-based access control (RBAC) policies for all users.
- Apply the principle of least privilege across all accounts, especially privileged users.
- Automate privileged access requests and approvals to ensure access is granted only when necessary.

Step 3: Automate Continuous Monitoring of Identities and Access

Identity and access governance is not a one-time project—it requires continuous oversight to keep access secure. Organisations should:

- Implement daily identity policy checks to detect and respond to potential non-compliance.
- Use automated identity lifecycle management to enforce consistent access controls.
- Centrally log and audit privileged access events for compliance and security reviews.

Identity Governance is Critical to Essential Eight Success

The Essential Eight provides a structured approach to cybersecurity, with identity and access governance serving as the linchpin of its effectiveness. Without strong access controls, privileged account management, and multi-factor authentication, organisations will struggle to reach higher maturity levels.

By adopting a modern, data-driven approach to identity governance—one that includes continuous access mapping, automated privilege management, and proactive monitoring—organisations can:

- Reduce the risk of credential-based attacks.
- Achieve compliance with Essential Eight maturity requirements.
- Strengthen overall cybersecurity resilience.

The Essential Eight isn't just about compliance—it's about building a security-first culture where access is managed with precision, identities are protected by design, and cyber threats are neutralised before they can cause harm.

Schedule a Demo | **Learn More** | **Read Online**