A GATHID LABS SERIES: EPISODE 3

Government Compliance and The Essential Eight

Case Study: How Gathid Transformed Essential Eight Compliance for a Government Agency

A government agency facing increasing cybersecurity risks and regulatory pressure sought to improve its Essential Eight compliance. Initially at Maturity Level Zero, the agency needed immediate visibility into its user access landscape, efficient identity governance, and continuous monitoring to progress towards Maturity Level 2 and beyond.

However, the government agency struggled with siloed identity data, manual access reviews, and enforcing least privilege access—all of which created compliance gaps and security vulnerabilities.

By leveraging Gathid as an identity and access strategy coach, the agency successfully automated compliance maturity, reduced excess privileges, and strengthened its cybersecurity posture.

The Challenge

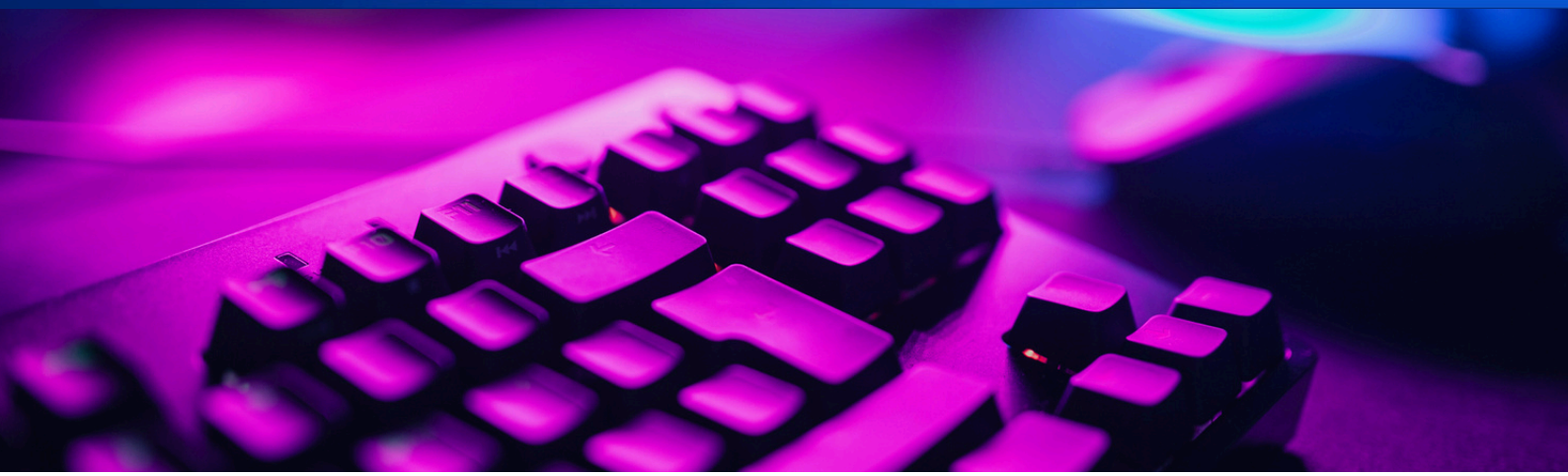
Like many public sector organisations, the government agency faced several identity and access governance (IAG) roadblocks that hindered its Essential Eight compliance journey.

Limited Visibility into User Access: Multiple systems lacked a centralised view of identity data, making it difficult to track who had access to what across departments.

Manual Access Reviews Were Inefficient and Inconsistent: Access reviews were conducted infrequently, often only before audits, leaving long periods where inappropriate access could go unnoticed. The agency struggled to quickly identify and revoke stale accounts.

C**hallenges in Enforcing Least Privilege and Administrative Restrictions**: Excessive administrative access created security risks. The agency lacked a structured way to link privileged accounts to real people and determine if permissions were justified.

Inconsistent Monitoring and Lack of Risk Insights: Without daily monitoring, the agency had no proactive way to detect compliance gaps. Moving towards Maturity Level 3 required a continuous, adaptive approach to identity governance.



Multiple Sources of People Data Increased Risk Exposure: Employees, contractors, and third-party personnel data were spread across different departments with no unified oversight. Dormant accounts from former employees or role changes were not being revoked, leaving security vulnerabilities.

Without an automated, data-driven identity and access solution, the government agency risked non-compliance, security breaches, and operational inefficiencies.

The Solution: A Data-Driven Approach to Identity and Access

To bridge the compliance gap and progress towards Essential Maturity Level Two, the government agency implemented Gathid. This provided a range of benefits.

Immediate Access Visibility
Gathid mapped and modelled relationships between user accounts, permissions, and associated systems in one centralised platform. This allowed the agency to quickly identify high-risk access issues and understand their impact.

Automated Access Reviews and Continuous Monitoring
The agency replaced infrequent, manual access reviews with continuous, policy-driven access assessments. Initially, reviews focused on accounts belonging to former employees or users who had changed roles or projects. Over time, the agency expanded automated role-based access mapping to include privileged users. Today, the agency receives daily notifications when a user's actual access differs from expected access, enabling governance improvements.

Enforcement of Least Privilege and Privileged Access Management
Administrative accounts were reviewed and restructured to follow least privilege principles. Gathid helped link privileged accounts to real users and ensured that service and non-human accounts had appropriate ownership and monitoring.

Daily Risk Insights and Actionable Reporting
Instead of relying on yearly audits, the government agency now receives daily updates on security risks related to identity and access. High-risk accounts are flagged immediately, allowing for timely corrective actions.

Automated Revocation of Dormant and Stale Accounts
Gathid detected and flagged inactive accounts across systems. Notifications were sent to revoke access for former employees, expired contractors, and third-party personnel. Stale accounts were systematically deactivated, ensuring no unnecessary access remained.

Strategic Coaching for Long-Term Compliance Maturity
Gathid partnered with the agency's IT team, providing expert guidance on best practices for policy enforcement, role management, and access control governance. The agency now has a structured roadmap to achieve Maturity Level Three in the future.

The Results: Stronger Compliance and Cyber Resilience

By implementing Gathid, the government agency achieved measurable improvements in compliance maturity, security posture, and operational efficiency.

Achieved Essential Eight Maturity Level Two
The agency matured from Level Zero to Level Two by enforcing stricter access control policies and ensuring continuous, daily monitoring. A clear roadmap to Level Three compliance is now in place.

95% Reduction in Excess Privileges
Automated insights allowed the agency to confidently remove unnecessary administrative access and reduce privilege creep.

Dormant and Stale Accounts Eliminated
Former employees, expired contractors, and inactive third-party users no longer have lingering access to critical systems. The agency eliminated a significant attack vector by ensuring all access is tied to active, authorised personnel.

Audit-Ready Compliance with Minimal Effort
Daily compliance reports provided auditors with immediate evidence of security controls and policy enforcement. Instead of spending months gathering identity governance data, the agency now provides daily compliance validation.

Enhanced Security Posture and Proactive Risk Mitigation
Continuous monitoring and identity mapping allowed the agency to detect and remediate threats before they became security incidents. The shift from reactive compliance to proactive identity governance strengthened long-term cybersecurity resilience.

Why This Matters: Identity Governance as the Key to Essential Eight Success

For government agencies facing increased cyber threats and regulatory scrutiny, Essential Eight compliance is no longer optional.

- **Before Gathid**: The agency struggled with siloed identity data, excessive access privileges, and inefficient compliance audits.
- **After Gathid**: The agency gained full visibility, automated governance, and continuous assurance—dramatically improving compliance maturity.

With daily insights, automated controls, and a strategic roadmap to Maturity Level 3, the agency is now better equipped to protect critical systems and sensitive data from cyber threats.

Final Thoughts: Transforming Essential Eight Compliance with Gathid

This case study demonstrates that Essential Eight compliance is not just about implementing security controls, it's about proving and maintaining them continuously with the required context.

With Gathid, government agencies can:

- Gain rapid visibility into identity and access risks.
- Automate access compliance reporting and access reviews.
- Eliminate excess privileges and more efficiently define and enforce least privilege policies.
- Achieve continuous compliance with reduced risk and minimal manual effort.
- Confidently progress towards Maturity Level 3 and beyond.

Want to Enhance Your Essential Eight Compliance?

Contact Gathid today to see how we can help your organisation achieve faster, easier, and more effective compliance maturity.

Schedule a Demo | Learn More | Read Online