TANIUM

The Power Of Certainty™

THE ESSENTIAL EIGHT

The voice of the customer insights report

Insights from the Public Sector on reducing risk and achieving Essential Eight compliance

DECEMBER 2024

The Voice of the Customer

In October 2024, Tanium held a roundtable discussion with 14 key IT and security leaders from six federal agencies featuring guest speaker Sean Hugo, the Assistant Secretary of Cyber Risk Services at Home Affairs. The purpose was to create an opportunity for government agencies to share the challenges they are facing when it comes to addressing security risk and Essential Eight compliance and to foster a productive discussion on how to overcome them.

The Voice of the Customer report shares valuable insights and key takeaways from some of the leading security voices in the Australian Federal Government shared during the roundtable.

What is the Essential Eight?

The Essential Eight is a set of mitigation strategies recommended by the Australian Signals Directorate to help reduce cybersecurity risk. Essential Eight compliance is mandated across all Federal Government agencies, requiring each agency to self-assess their compliance annually. Beyond being a regulatory requirement, the Essential 8 is an effective baseline to measure an organisation's Cyber Hygiene.

With the Australian National Audit Office (ANAO) providing reports to the Parliament and, in turn, the Minister for Cyber Security, non-compliance can no longer be swept under the rug.

Balancing Compliance and Risk

> “Agencies can’t risk-accept their way to compliance.”

Sean Hugo, Assistant Secretary Cyber Risk Services at Home Affairs

In 2023, only 25 per cent of organisations reached overall Maturity Level 2 when factoring in compensating controls. Although this signals progress in security postures, it means the vast majority of agencies are still falling short of meeting the Essential Eight’s compliance guidance.

One of the key traps that agencies fall into is simply to accept the risk and move on.

> Risk acceptance is great for measuring compliance, but not for actually protecting the business.”

Ian Fisher, Director, of Banking, Finance, and Government, A/NZ at Tanium

Whilst it might help improve your security posture in the short term, this is not a sustainable path towards compliance. If alternative controls are implemented, they must meet or exceed established guidance, and agencies that have not achieved Maturity Level 2, must still develop a plan to achieve the minimum requirements.

Rather than seeking ways to make frameworks fit outdated applications, agencies need to address the root issues.

> “Bad actors aren’t concerned with budget constraints or legacy system challenges.”

Matt Waite, Technical Account Manager at Tanium

Sean Hugo, Assistant Secretary of Cyber Risk Services at Home Affairs, explained this problem using this analogy during the discussion:

“The regulator says we need a lock on the door, but we can’t put one on because the one we have is not compatible with the door. The next best thing is an alternative control such as hiring a security guard to stand in front of the door, but we can’t afford one. So we put in a CCTV camera and now we only know the door has been opened after the fact. This could all have been avoided if you invested the time and money to replace the door”

Unfortunately, many senior leaders are forced to wait for a disaster before committing resources to fix problems. This approach is risky; we shouldn’t wait until we’ve already hit the iceberg.

Another issue is tooling. Some agencies rely heavily on a multitude of tools, yet simply piling on more technology won’t guarantee compliance or security. One example of this is deploying audit sampling tools.

“It’s easy to lose sight of the ultimate goal by focusing on box-ticking for compliance but sampling a few compliant endpoints doesn’t secure the overall environment and still leaves agencies vulnerable to the ANAO or ACSC,” added Matt Waite, Technical Account Manager at Tanium.

Essential Eight challenges facing government agencies

Understanding compliance vs. risk

Agencies need to differentiate between compliance—a regulatory obligation—and actual risk management, which involves proactively identifying and addressing vulnerabilities. Achieving compliance doesn't necessarily equate to reduced risk, yet agencies struggle to go beyond box-ticking to materially improve their security maturity.

Overcoming legacy systems

Many agencies still rely on legacy systems that are difficult to secure in line with the regulations, presenting significant roadblocks towards compliance. With budget constraints making it difficult to replace entire systems, agencies often face the challenge of finding workarounds that don't necessarily improve overall security.

A siloed approach

Many agencies tackle cybersecurity challenges independently, missing out on valuable lessons that could be learned from their peers. Greater collaboration and sharing of best practices could enhance resilience across the sector, helping everyone strengthen the government's defences as a whole.

Keeping up with shifting regulation

The regulatory requirements around the Essential Eight changes as we adapt to new threats. Agencies face the challenge of continuously adapting to these new requirements, requiring agility and constant monitoring of the standards to ensure ongoing compliance.

Raising awareness amongst staff

Communicating the importance of cybersecurity across large agencies with thousands of employees can be hard, particularly as processes and tools regularly shift to meet new compliance requirements.

Getting buy-in from senior execs

Securing support from senior executives, particularly those without technical backgrounds, can be challenging but is essential for successful cybersecurity initiatives.

Recommendations for meeting compliance

Don't accept risk acceptance as a solution: Risk acceptance should be a last resort, not a substitute for effective risk mitigation strategies.

See non-compliance as an opportunity for more funding: When non-compliance is identified, it highlights areas needing investment to avoid disaster, which can justify additional budget allocation.

Introduce data stewards working together with system and business owners: Data stewards can provide a governance role to ensure that an organisation's data is accessible and secure, and collaborate with system and business owners to better understand the business needs and improve risk management.

Identify and gain visibility across all endpoints: Full visibility of all endpoints in your environment means any risk can be identified and remediated quickly.

Replace sampling with real-time, continuous compliance: Real-time, continuous compliance means you know exactly what's happening in your environment at any given moment, rather than relying on point-in-time sampling which provides outdated, often inaccurate data.

Reduce compliance tooling: Save money, time, and resources by using one platform for detecting and remediating risks.

Tanium's new E8+

Fast-track your maturity level uplift with the only platform that:

Provides continuous monitoring across all IT Assets

Identifies and remediates risks in real time

Provides visibility and reporting across all Essential Eight controls

Learn more about Tanium's game-changing E8+ solution.

https://site.tanium.com/ANZ-E8plus.html

TANIUM

The Power of Certainty.™

Visit us at www.tanium.com and follow us on LinkedIn and X.