POINT OF VIEW

# Navigating Australia's cybersecurity obligations: SOCI, PSPF and the Essential Eight

## A strategic guide for government and critical infrastructure organisations

*By Chandrakant Kamble, Shane Silva, Hirun Tantirigama and Peter Bokor*

As Australia confronts an evolving and intensifying cyber threat landscape, public and private sector entities are under increasing pressure to fortify their cyber resilience. Central to this effort are three frameworks that define the country's cybersecurity foundation: **the Security of Critical Infrastructure (SOCI) Act, the Protective Security Policy Framework (PSPF) and the Australian Cyber Security Centre's (ACSC) Essential Eight.**

The most recent updates to the PSPF (July 2025) and the Essential Eight (September 2025) was only recently released, these frameworks remain highly relevant and foundational. They directly support implementation of the **Australian Cyber Security Strategy 2023–2030**, reinforcing national objectives around sovereign cyber resilience, uplift of critical infrastructure and consistency in minimum baseline security controls. In parallel, they align with the direction of Australia's ongoing cybersecurity legislative reform agenda, including proposed updates to cyber incident reporting, governance and accountability requirements.

protiviti®
Global Business Consulting

By mapping obligations, identifying common implementation gaps and proposing prioritised remediation strategies, this paper serves as a timely and actionable resource for organisations seeking to align with current regulatory expectations, enhance cyber maturity and operationalise national cyber priorities in 2025 and beyond.

For government departments, agencies and critical infrastructure operators, these frameworks are not only regulatory requirements but also enablers of national trust, economic continuity and operational integrity. However, despite their strategic importance, many organisations face complex challenges in understanding, implementing and sustaining compliance.

This article offers a detailed view into the significance of these frameworks, the challenges faced by organisations, and pragmatic approaches to implementing and maintaining compliance. It also outlines the role of consulting firms in supporting these efforts, ensuring entities can operationalise compliance while maintaining mission-critical outcomes.

## Key frameworks supporting Australia's cyber security strategy

### Security of Critical Infrastructure (SOCI) Act

SOCI ensures national-level visibility and response to infrastructure threats.

### Protective Security Policy Framework (PSPF)

PSPF provides a holistic approach to security for government agencies.

### Australian Cyber Security Centre's (ACSC) Essential Eight

Essential Eight offers a technical baseline for cyber defence across environments.

> *For government departments, agencies and critical infrastructure operators, these frameworks are not only regulatory requirements but also enablers of national trust, economic continuity and operational integrity.*

## 01 Understanding the frameworks: SOCI, PSPF and the Essential Eight

The increasing digitalisation of Australia's critical sectors continues to expose them to heightened cyber risk. While the Optus (2022) and Latitude Financial (2023) breaches brought national attention to the fragility of customer data protection, their impact remains active and highly relevant due to ongoing regulatory reviews and public scrutiny. In 2024, both incidents were examined in Senate committee hearings (Parliament of Australia, 2024), leading to policy discussions on mandatory breach disclosure, third-party accountability and reforms to the Privacy Act 1988. Additionally, the Office of the Australian Information Commissioner (OAIC) issued enforcement outcomes and undertakings in response to these breaches, reinforcing expectations for baseline cyber hygiene and regulatory compliance (OAIC, 2024).

The Australian Cyber Security Strategy 2023–2030, released in late 2023, entered its implementation phase in 2024. This included the launch of sovereign cyber hubs, new sector-specific risk management obligations and increased resourcing for the Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC). In February 2025, the ACSC released updated guidance on ransomware readiness and Essential Eight maturity self-assessments, providing clearer expectations and benchmarking tools for organisations across sectors (ACSC, 2025).

In this context, the three serve complementary and ongoing strategic roles:

- SOCI provides national-level oversight and mandates proactive security measures for critical infrastructure entities.
- PSPF, updated in July 2025, ensures a coordinated and holistic approach to protective security across Commonwealth agencies and entities.
- The Essential Eight, updated in November 2023, continues to serve as a scalable technical control baseline still undergoing widespread implementation and uplift throughout 2025–2026.

For government agencies, regulated infrastructure providers and private entities engaged with government, these frameworks are critical for:

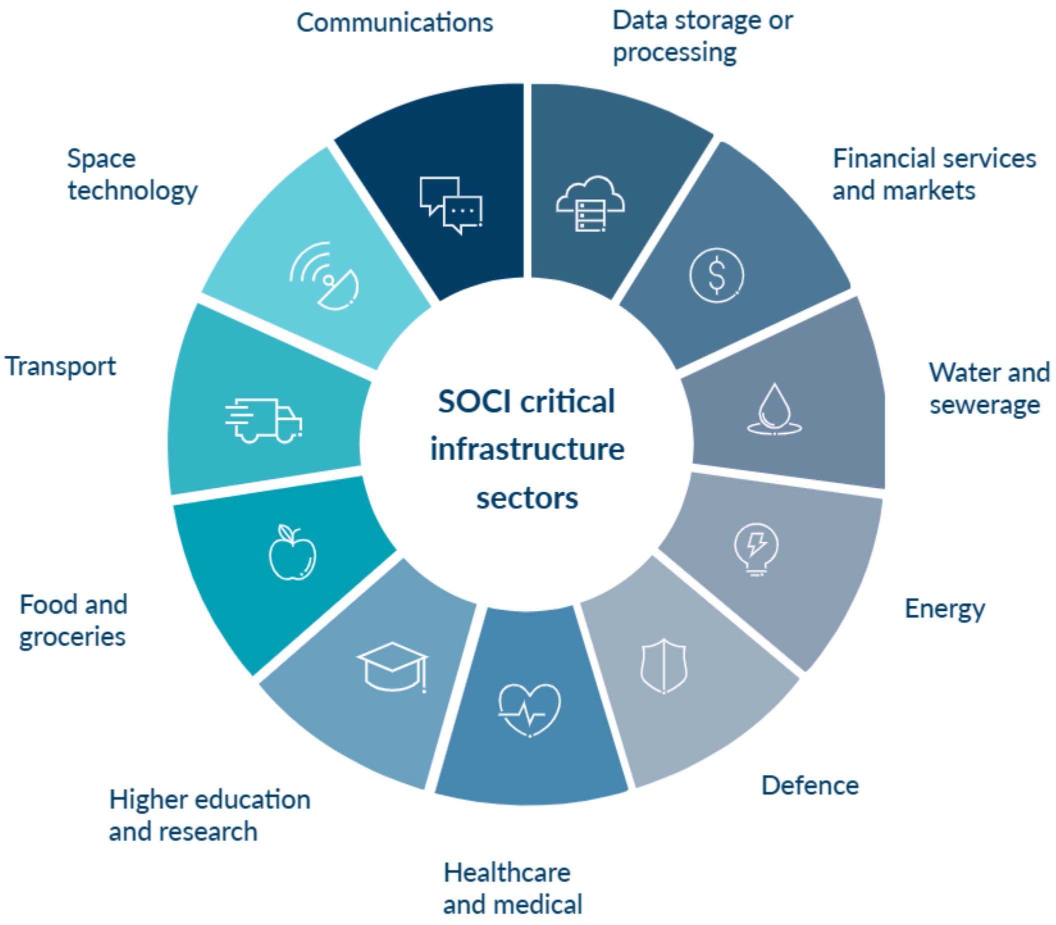
- Upholding public trust in digital services and systems
- Meeting ongoing regulatory compliance expectations under SOCI and Privacy Act reforms
- Resisting evolving threats from ransomware actors, insider threats, and nation-state APTs

As the 2025 threat environment grows more complex and regulated, these frameworks remain essential for operationalising national cyber priorities, achieving uplift targets, and building systemic resilience across Australia's digital economy.

*As the 2025 threat environment grows more complex and regulated, these frameworks remain essential for operationalising national cyber priorities and building systemic resilience across Australia's digital economy.*

## 1.1 The Security of Critical Infrastructure (SOCI) Act

Originally enacted in 2018 and significantly amended in 2021, the SOCI Act aims to protect Australia's critical infrastructure from both physical and cyber threats. The act applies to sectors deemed vital to the country's economy and safety, including energy, water, health, communications, and ports.


SOCI critical infrastructure sectors
Communications
Data storage or processing
Financial services and markets
Water and sewerage
Energy
Defence
Healthcare and medical
Higher education and research
Food and groceries
Transport
Space technology

The amendments introduced obligations such as:

- Mandatory cyber incident reporting within 12 or 72 hours depending on impact.
- Risk Management Program (RMP) requirements for regulated entities.
- Government assistance provisions in the event of a nationally significant cyber threat.

The SOCI Act introduces a tiered approach to regulatory oversight, with specific entities designated as Systems of National Significance (SoNS), requiring enhanced obligations such as vulnerability assessments and annual reporting.

## 1.2 Protective Security Policy Framework (PSPF)

The PSPF is the primary security compliance framework for Australian Government entities, having been developed by the Attorney-General's Department, and now overseen and managed by the Department of Home Affairs. The Protective Security Policy Framework (PSPF), first established in 2010 by the Directive on the Security of Government Business and most recently updated in July 2025, outlines minimum security requirements for government agencies and forms a core pillar of Australia's cyber resilience approach (Attorney-General's Department, 2024). Aligned with the Australian Cyber Security Strategy 2023–2030, the July 2025 update to the PSPF reinforces expectations around supply chain assurance, personnel vetting and protective information security (Attorney-General's Department, 2024).

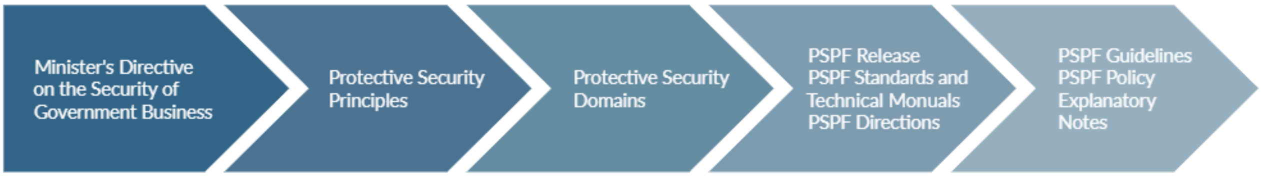
The PSPF underwent a structural improvement in the November 2024 release, with the adjustment of domains based on the current threat landscape and business operations. Changes made to the PSPF included the introduction of a 'risk' and 'technology' domain. The PSPF now comprises of 218 individual control elements, grouped within 25 thematic areas (previously 16), which sit across six security domains (previously four):

- Governance security (GOV)
- Information security (INFO)
- Personnel security (PERS)
- Physical security (PHYS)
- Risk (RISK)
- Technology (TECH)

It is mandatory for non-corporate Commonwealth entities that are subject to the Public Governance, Performance and Accountability Act 2013 to implement the PSPF in compliance with the law. In accordance with the PGPA Act, the PSPF is a more suitable practice for corporate Commonwealth entities and wholly-owned Commonwealth corporations. Non-governmental organisations that are granted access to security classified information may be required to execute a deed or agreement in order to enforce the relevant provisions of the PSPF (Applying the Protective Security Policy Framework, n.d.).

Entities must attest to their PSPF compliance annually and demonstrate continuous improvement to the Department of Home Affairs. The framework is risk-based and requires alignment of security controls with business functions and threat environments. PSPF compliance across the private sector may be encouraged by Commonwealth entities to seek compliance under vendor commercial obligations to provide services – an example being the Department of Defence DISP obligations.

Protective security policy framework structure



Minister's Directive on the Security of Government Business

Protective Security Principles

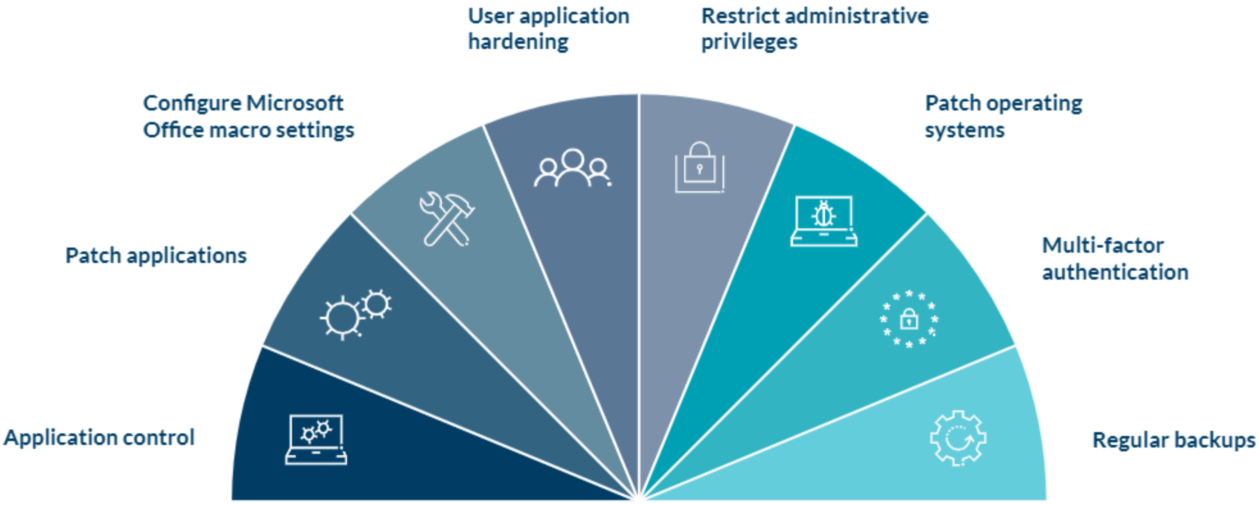
Protective Security Domains

PSPF Release
PSPF Standards and Technical Monuals
PSPF Directions

PSPF Guidelines
PSPF Policy Explanatory Notes

## 1.3 The Essential Eight

The Essential Eight is a prioritised set of mitigation strategies developed by the ACSC to help organisations defend against cyber threats. These include:


User application hardening
Restrict administrative privileges
Configure Microsoft Office macro settings
Patch operating systems
Patch applications
Multi-factor authentication
Application control
Regular backups

Although the Essential Eight Maturity Model was first introduced by the Australian Cyber Security Centre (ACSC) in 2017, it remains highly relevant and timely in today's cybersecurity landscape. This is due to its continuous evolution—most recently updated in September 2025—and its explicit endorsement in the Australian Cyber Security Strategy 2023–2030 as the foundational baseline for improving national cyber resilience (ACSC, 2023; Department of Home Affairs, 2023).

The Essential Eight provides a practical, implementation-focused framework that is scalable to organisations of varying size and complexity. It also serves as the benchmark for compliance with numerous regulatory requirements, including the SOCI Act's risk management obligations and security uplift expectations under the Protective Security Policy Framework (PSPF). As threat actors increasingly exploit known but unpatched vulnerabilities, the Essential Eight's emphasis on proactive control maturity and measurable uplift makes it an indispensable guide for both public and private sector organisations navigating complex cybersecurity obligations.

These controls are measured using the Essential Eight Maturity Model (E8MM), which ranges from Maturity Level 0 (unmitigated risk) to Level 3 (fully aligned with recommended practices). While the Australian Cyber Security Centre's (ACSC) Essential Eight provides a highly effective baseline for mitigating cyber threats, non-government entities particularly small to medium enterprises (SMEs) and organisations outside the public sector often face significant barriers to full compliance.

Unlike federal government agencies that are mandated to adopt these controls under frameworks like the Protective Security Policy Framework (PSPF), many private and not-for-profit organisations operate with limited resources, legacy systems or competing operational priorities. Full maturity across all eight strategies, especially those requiring application control, patch automation or centralised administrative privilege management, can involve substantial investment in technology, skilled personnel and governance processes.

However, this does not diminish the importance or relevance of the Essential Eight. In fact, several of these controls should be considered foundational cybersecurity hygiene for all sectors, regardless of size or regulation.

> *Unlike federal government agencies that are mandated to adopt these controls under frameworks like the Protective Security Policy Framework (PSPF), many private and not-for-profit organisations operate with limited resources, legacy systems or competing operational priorities.*

## 1.4 Priority controls every organisation should implement

While many organisations are aware of baseline security controls, inconsistent implementation and limited resourcing often leave critical gaps. The following control domains remain the most frequently exploited by adversaries and offer high return on investment when effectively applied. Their prioritisation is endorsed by both the Essential Eight and international threat intelligence bodies (e.g., MITRE, ENISA):

- **Multi-Factor Authentication (MFA):** Despite its broad availability, MFA is still inconsistently applied—particularly for third-party access, cloud admin portals and legacy applications. Mandating MFA for privileged and remote accounts significantly reduces credential-based compromise, which remains one of the most common initial access vectors.
- **Regular patching (Operating systems and applications):** Many ransomware incidents and APT campaigns still rely on exploiting known but unpatched vulnerabilities (e.g., Citrix Bleed, Log4Shell). Implementing automated patch deployment with risk-based prioritisation (e.g., critical CVEs within 14–30 days) mitigates common attack paths.
- **Restricting administrative privileges:** Default administrator access is often over-provisioned across workstations, servers and cloud resources. Implementing role-based access controls, just-in-time privilege elevation and audit logging reduces the likelihood of privilege escalation and limits lateral movement.
- **Daily backups:** Backups remain one of the most effective ransomware mitigations—but only if they are tested, immutable and isolated. Organisations should prioritise automated backup integrity checks and ensure recovery procedures are regularly exercised under pressure.

These controls are not just foundational—they continue to represent break points in real-world intrusions when neglected. They are also scalable and defensible in board-level discussions, making them an ideal starting point for organisations aiming to uplift cyber resilience in a phased or risk-informed manner.

It is important to view the Essential Eight not as a rigid compliance checklist, but as a dynamic maturity journey. By starting with the controls that address the most probable attack vectors and are operationally achievable, even small or non-government organisations can realise meaningful security improvements while building toward long-term maturity.

# 02 Common challenges in achieving compliance

While Australia's cybersecurity frameworks SOCI, PSPF, and the Essential Eight — set clear expectations, organisations continue to face persistent barriers in achieving meaningful and sustainable compliance. These challenges are not just technical — they are governance, cultural, and systemic in nature. Lessons from the **Optus** and **Latitude Financial** data breaches, as well as ACSC's own audit findings, underscore how even well-resourced entities may falter in translating compliance intent into operational execution (ACSC, 2023; Parliament of Australia, 2024; OAIC, 2024).

## 2.1 Framework overlap and interpretation

The coexistence of multiple frameworks leads to duplication and misalignment without clear mapping or regulatory consolidation. For example, the **SOCI Act's Risk Management Program Rules** require entities to implement appropriate security measures but do not define "appropriate" in maturity terms — leaving it to interpretation. Meanwhile, the **PSPF's policies** and the **Essential Eight's maturity model** overlap in intent but diverge in format and audit readiness. In the absence of unified guidance, many organisations struggle to establish a single defensible compliance narrative.

## 2.2 Resource and capability gaps

According to the **Australian Cyber Security Strategy 2023–2030**, workforce shortages are one of the biggest national risks to cyber resilience. Many regional agencies and smaller critical infrastructure providers lack internal cyber expertise to keep pace with evolving SOCI obligations or implement technical controls such as **application control** or **privilege restriction** at scale. Without a dedicated governance lead or GRC tooling, compliance becomes reactive and fragmented — posing audit and regulatory risks.

## 2.3 Legacy and complex environments

Legacy and hybrid environments often fall short of Essential Eight technical prerequisites — e.g., unsupported operating systems or embedded devices that cannot be patched regularly. During post-breach investigations (such as Latitude Financial's), regulators highlighted control breakdowns tied to legacy complexity and insufficient network segmentation. These same constraints limit compliance with **PSPF's policies**, which require secure configuration and monitoring of ICT systems.

## 2.4 Unclear third-party accountability

Both **SOCI and PSPF (through supply chain risk management)** expect regulated entities to manage third-party cyber risk. However, due to complex outsourcing arrangements, control performance (e.g., MFA enforcement, daily backups, patch SLAs) is often assumed rather than assured. Contracts may lack measurable security clauses, and few entities perform end-to-end due diligence. As a result, organisations face residual exposure that may not be defensible in audits or breach response scenarios.

## 2.5 Reporting and governance burden

Regulatory obligations such as SOCI's annual compliance report to the **Cyber and Infrastructure Security Centre (CISC)**, PSPF's self-assessment to portfolio agencies, and internal Essential Eight maturity reporting are often conducted manually. Without automation or centralised mapping, teams duplicate effort and introduce inconsistencies. This increases operational burden and reduces accuracy — especially for federated agencies operating across jurisdictions or subsidiaries.

These challenges highlight the importance of adopting a **risk-based compliance strategy**. As emphasised by the ACSC (2025), organisations should focus on the controls most likely to reduce risk exposure — prioritising implementation of the Essential Eight controls based on threat likelihood, business criticality, and resource availability. Moreover, agencies should integrate compliance workflows into **governance, risk, and compliance (GRC)** platforms and continuously align to updated guidance from ACSC, OAIC, and CISC.

# 03 How to meet compliance in a pragmatic way

Compliance with cybersecurity frameworks such as **SOCI**, **PSPF**, and the **Essential Eight** should not be viewed as a tick-box task but as a structured opportunity to embed security into operational resilience. The following recommendations offer a **phased**, **regulation-aware roadmap** to uplift compliance maturity in line with government expectations:

## 3.1 Harmonise cybersecurity control frameworks

Develop a unified cybersecurity control framework that consolidates PSPF mandatory controls (e.g., INFOSEC, GOV), Essential Eight maturity requirements, and SOCI Act obligations — including those related to the Risk Management Program (RMP) and incident reporting. Leverage crosswalks and control libraries to reduce duplication across self-assessments, audits, and third-party assurance.

## 3.2 Prioritise crown jewels and Systems of National Significance (SoNS)

Use a risk-based asset classification to prioritise Essential Eight implementation starting with Crown Jewels and SoNS designated under SOCI. This aligns with PSPF's TECH and INFOSEC policies and ensures that high-impact systems meet baseline maturity (e.g., Maturity Level Two or higher).

> Compliance with cybersecurity frameworks such as SOCI, PSPF, and the Essential Eight should not be viewed as a tick-box task but as a structured opportunity to embed security into operational resilience.

## 3.3 Establish cybersecurity governance for regulatory alignment

Form a multi-disciplinary Cyber Risk and Compliance Committee accountable for tracking alignment with SOCI reporting requirements, PSPF attestations, and Essential Eight maturity progression. Governance bodies should be empowered to approve funding, prioritise control remediation, and oversee third-party security obligations.

## 3.4 Automate control monitoring and assurance reporting

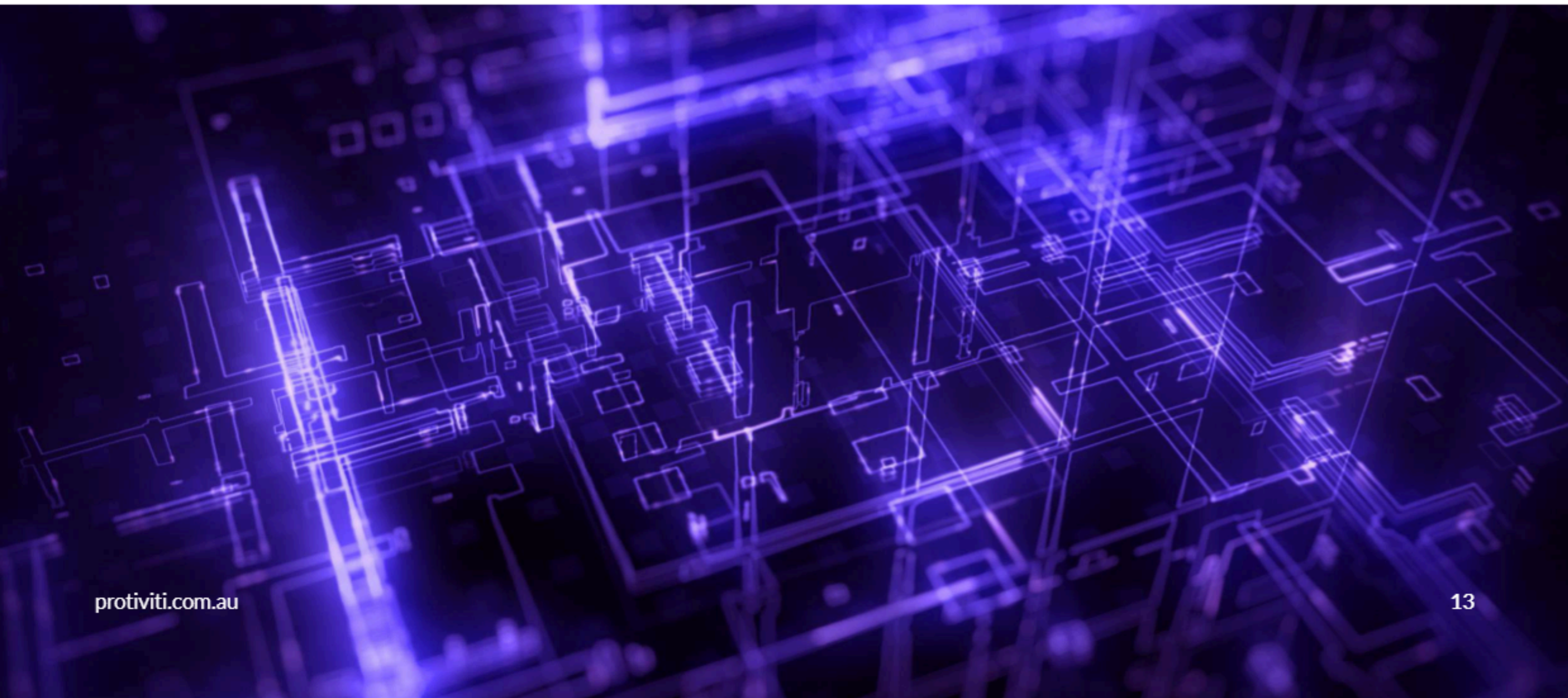
Deploy technical tools that generate evidence for compliance with specific regulatory requirements — e.g., vulnerability scanning for PSPF, MFA logs for Essential Eight Maturity Level One, and incident detection aligned with SOCI's 12-hour reporting requirement. Integrate this into a GRC platform with dashboard views mapped to each framework.

## 3.5 Targeted training and operational readiness

Move beyond generic awareness campaigns by delivering role-specific training aligned to regulatory duties. For example, provide incident reporting workflows to operations teams (per SOCI), policy mapping exercises for auditors (per PSPF), and Essential Eight implementation sessions for IT administrators.

## 3.6 Conduct cyber resilience drills with regulatory scenarios

Run tabletop exercises that simulate ransomware, insider threats, or third-party breaches, explicitly incorporating compliance decision points — e.g., whether an event meets SOCI's "material cyber incident" criteria, or how recovery aligns to Essential Eight backup integrity requirements. Use outcomes to refine response plans and regulatory reporting processes.



## 04 Conclusion

Australia's national cybersecurity resilience hinges not just on policy intent, but on the practical implementation of SOCI, PSPF, and the Essential Eight across critical infrastructure sectors and government agencies. These frameworks are no longer theoretical or optional — they are now reinforced by active regulatory enforcement, mandatory reporting, and alignment with the Australian Cyber Security Strategy 2023–2030.

While full compliance may appear complex, particularly across legacy environments and federated governance structures, organisations can succeed by adopting a phased, risk-informed approach. This includes prioritising systems of national significance (SoNS), leveraging maturity-aligned implementation of the Essential Eight, and aligning governance processes to PSPF and SOCI reporting obligations.

As highlighted throughout this paper, the most effective compliance strategies are those that embed security controls into daily operations, automate evidence collection, and translate requirements into actionable, risk-reducing activities. Regulatory alignment should be seen not as a burden, but as an opportunity to strengthen mission delivery, build public trust, and uplift sector-wide resilience.

With strategic investment, skilled resources, and guidance from experienced cybersecurity practitioners, government and regulated industries can confidently navigate overlapping obligations, minimise regulatory exposure, and help safeguard Australia's digital infrastructure and national interest well into the future.

## How Protiviti can support

Partnering with Protiviti accelerates compliance and avoids common pitfalls.
Key value-added services include:

- **Framework mapping:** Translating compliance requirements into unified control libraries.
- **Gap assessments:** Baseline assessments against Essential Eight Maturity Model, PSPF, and SOCI RMP obligations.
- **Program governance:** Establishing oversight committees, project charters, and reporting mechanisms.
- **Policy and process design:** Creating policies that reflect best practices in identity, access, patching, and incident management.
- **Tool implementation:** Advising on and deploying GRC, asset management, SIEM, and SOAR platforms.
- **Training and culture change:** Delivering tailored training programs and communication strategies.

Consultants also act as external facilitators, helping depoliticise control ownership, resolve ambiguity, and engage board-level stakeholders with the right language and reporting insights.

## References

- Applying the protective security policy framework. (N.D.-B). Protective security policy framework. https://www.protectivesecurity.gov.au/about/applying-protective-security-policy-framework
- Attorney-general's department. (2024). Protective security policy framework. https://www.protectivesecurity.gov.au
- Attorney-general's department. (2024, October). Protective security policy framework: securing government business. Australian government. https://www.protectivesecurity.gov.au/
- Australian cyber security centre (acsc). (2023, November). Essential eight maturity model (version: november 2023). Australian signals directorate. https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- Australian cyber security centre. (2023). Essential eight strategies to mitigate cyber security incidents. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight
- Australian cyber security centre. (2023, November). Essential eight maturity model (version: november 2023). Australian signals directorate. https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- Australian cyber security centre. (2025, February). Ransomware readiness and essential eight maturity self-assessment guidance. Australian signals directorate. https://www.cyber.gov.au/acsc/view-all-content/publications
- Australian signals directorate. (2022). Essential eight maturity model. https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- Department of home affairs. (2023). Australia's cyber security strategy 2023–2030: resilience in a cyber world. Australian government. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2023-2030.pdf
- Department of home affairs. (2023). Security of critical infrastructure act 2018. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-of-critical-infrastructure
- ISACA. (2022). The state of cybersecurity 2022 report. https://www.isaca.org/go/state-of-cybersecurity-2022
- Office of the Australian information commissioner. (2024, August). Enforcement outcomes: latitude financial and optus data breaches. Australian government. https://www.oaic.gov.au/privacy/privacy-enforcement
- Parliament of Australia. (2022). Amendments to the SOCI act — a regulatory guide. https://www.aph.gov.au
- Parliament of Australia. (2024, June). Inquiry into the implications of the optus and latitude data breaches. Senate standing committee on legal and constitutional affairs. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/CyberBreachInquiry2024

## About the authors

**Shane Silva**
Managing Director, Protiviti Australia

Shane Silva is an accomplished managing director, leading the data governance and technology assurance practices for Protiviti Australia. With a career spanning more than 18 years in the professional services industry and a strong focus on government consulting, Shane is recognised for his exceptional expertise and proficiency. His areas of specialisation encompass data governance, technology assurance, cybersecurity and project assurance. His in-depth knowledge of industry best practices, including CoBIT, NIST, ISO, DAMA DMBoK, and ITIL, adds to his exceptional capabilities.

Outside his professional role, Shane actively contributes to the ISACA.He is highly sought after as a speaker and frequently shares his invaluable insights at prestigious conferences and webinars. Additionally, Shane plays a pivotal role as an independent advisor and esteemed board member for data governance committees.

**Hirun Tantirigama**
Managing Director, Protiviti Australia

Hirun Tantirigama is Protiviti Australia's technology consulting lead with extensive experience in providing risk and regulatory advisory services across a variety of clients and industries from financial services to federal and state government. He has led complex, transformational programs across areas such as operational risk, regulatory remediation, operational and cyber resilience.

Hirun's technical and project management skills is further complemented by his deep understanding of good practice frameworks such as PRINCE2, COBIT, ITIL and NIST. Hirun is part of Protiviti's global operational resilience team and he's also the regional lead subject matter expert for Asia-Pacific Region. He also has experience servicing clients across New Zealand, Australia and the UK.

As a managing director, Hirun manages a portfolio of complex and risk-based engagements in high demanding environments, while developing and sustaining trusted-advisor and peer relationships with clients at senior and C-suite levels. As part of his role he is also involved in resource planning and headcount management, strategy setting, project commercials, staff training and performance management.

## About the authors

### Chandrakant Kamble

Associate Director, Protiviti Australia

Chandrakant Kamble is a highly respected cybersecurity strategist and technologyleader with more than 20 years of experience in IT, including over 15 years dedicated to cybersecurity. His global career spans across critical industries — such as energy, utilities, transport, health, financial services, telecommunications, and public sector organisations — where he has delivered high-impact security programs, advisory services, and resilience frameworks.

A keyarea of Chandrakant's work involves helping organisations translate regulatory and policy mandates into operational outcomes. He has played a pivotal role in guiding enterprises through alignment with Australia's Security of Critical Infrastructure (SOCI) Act, Privacy Act reforms, ISO 27001, NIST CSF, Essential Eight, and other internationally recognised frameworks.

Chandrakant is a regular contributor to national cybersecurity forums, industry working groups, and cyber maturity initiatives. He is passionate about enabling organisations — especially those operating critical infrastructure — torespond effectivelyto today's complex threat landscape while remaining aligned with evolving government policyandsector-specificregulations.

### Peter Bokor

SeniorManager, ProtivitiAustralia

Peter Bokor is a cyber security professional with experience working across Protiviti's technology consulting, and internal audit and financial assurance practices. Honing his skills from his time working in the consulting industry, Peter provides governance, risk and compliance (GRC) support, and ICT management assurance to Federal Government and privatesectorclients. Peter delivers independent program Line-3 assurance services, internal audit and assurance functions, and consults on technology risks within the APS sector.

Peter's focus is towards organisational framework compliance and assurance, leveraging national standards like the Information Security Manual (ISM), Essential Eight, and most importantly, the Protective Security Policy Framework (PSPF). Peter is determine to support his clients with practical and efficient services that are tailored based on individual capabilities and strategic direction.

## Contacts

**Shane Silva**
Managing Director, Protiviti Australia
0402.496.669
Shane.Silva@protiviti.com.au

**Hirun Tantirigama**
Managing Director, Protiviti Australia
0423.853.453
Hirun.Tantirigama@protiviti.com.au

**Chandrakant Kamble**
Associate Director, Protiviti Australia
0435.795.457
Chandrakant.Kamble@protiviti.com.au

**Peter Bokor**
Senior Manager, Protiviti Australia
0405.339.633
Peter.Bokor@protiviti.com.au

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 10th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

© 2025 Protiviti Inc. Protiviti is not licensed or registered as a public accounting firm and
does not issue opinions on financial statements or offer attestation services. 1125-AUS-EN

protiviti®