Compliance Brief

Complying with the SOCI Act in Australia

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

On 25 November 2024, the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (SOCI Act), which was included in the Cyber Security Legislative Package was passed into law. The SOCI Act gives the Government broader powers to deliver on Shield 4 of the Cyber Security Strategy 2023-2030 (protecting critical infrastructure) and to address gaps and issues of the evolving cyber threat landscape.

The key features of the SOCI Act include:

1. **Data storage systems that hold business critical data** would be regulated as critical infrastructure assets under the amendments.
2. **New government consequence management powers** under which the government may direct an entity to take action to respond to incidents more broadly than just cyber incidents.
3. **New definition of 'protected information'** that includes a harms-based assessment and a non-exhaustive list of relevant information plus clarifications as to when protected information can be shared or used for other purposes.
4. **New power for the regulator to issue directions** to a responsible entity to address any serious deficiencies that are identified in a critical infrastructure risk management program.

How Thales Helps with SOCI Act (Amendments) Compliance

The SOCI Act amendments in Schedule 1 strengthen the protection of data storage systems and business-critical data; Thales' solutions can help organizations comply with the SOCI Act by simplifying compliance and automating security reducing the burden on security and compliance teams.

Cyber Security Legislative Package referred to the Cyber Security Bill 2024 (**Cyber Security Act**), the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (SOCI Act), and the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 (IS Act). It grants additional protections to people and businesses and improves the Government's visibility of the current cyber threat environment.

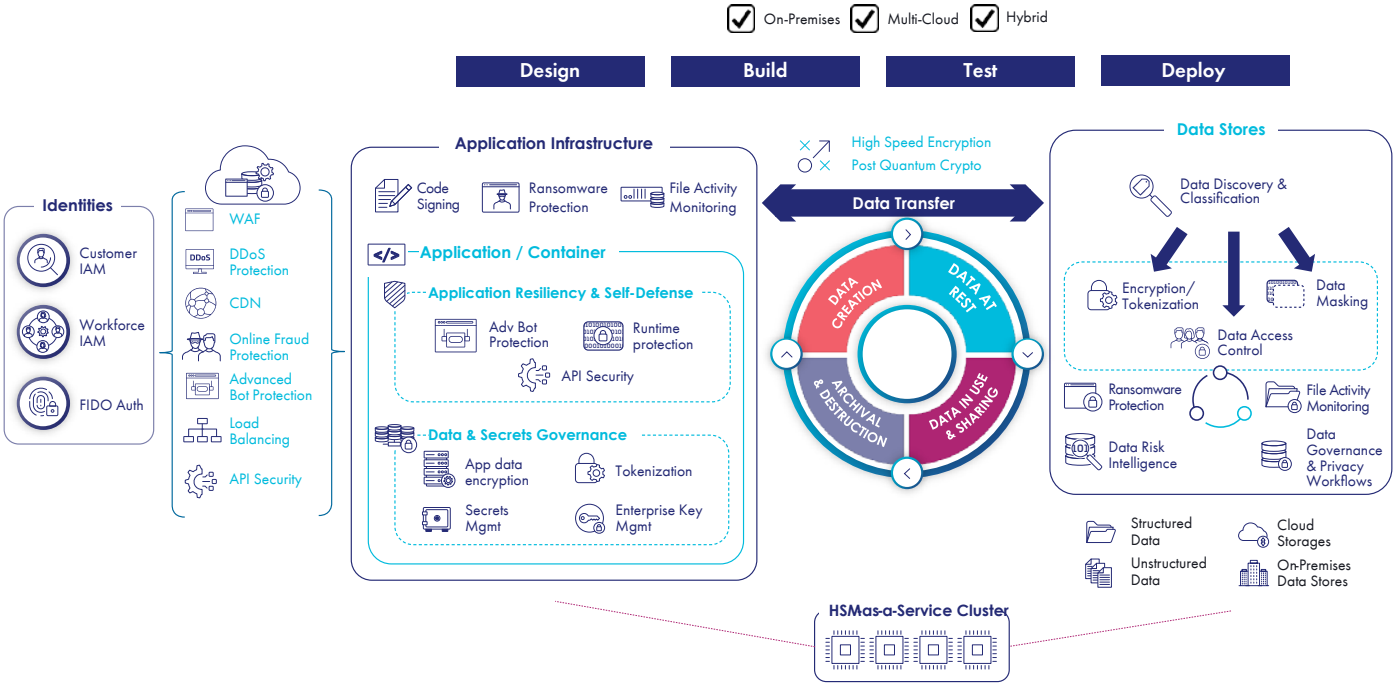
- The new Act strengthens safeguards for individuals, businesses, and critical infrastructure, enhancing Australia's resilience to cyber threats.
- Businesses must report significant cyber incidents, including ransomware demands and payments, ensuring improved visibility and coordinated responses.
- The Act updates standards for IoT devices, expands critical infrastructure definitions, and introduces a new Cyber Incident Review Board to prepare Australia for emerging challenges in a rapidly evolving threat landscape.

SOCI Act (Amendments) – SCHEDULE 1

Data storage systems that hold business critical data

- **#16:** "...strengthen the protection of data storage systems and business critical data."
- **#19:** "Schedule is not to capture all non-operational systems that hold business critical data, only those where vulnerabilities could have **a relevant impact on critical infrastructure. Examples of the types of systems** this could capture include: data storage systems that hold business critical data where there is **inadequate network segregation** between information and operational technology systems, or data storage systems that hold operational data such as network blueprints, **encryption keys**, algorithms, operational system code, and tactics,
- **#20:** "...Where the responsible **entity outsources to a third party**, then the third party becomes responsible for the data storage system."
- **#31:** The various criteria being proposed make clear the intent that not all non-operational systems that hold business critical data should be captured, only those where **vulnerabilities could have a relevant impact on critical infrastructure**. They also clarify that the responsible entity for the main critical infrastructure asset is responsible for data storage systems that they own or operate.

The Imperva-Thales Secured Digital Ecosystem

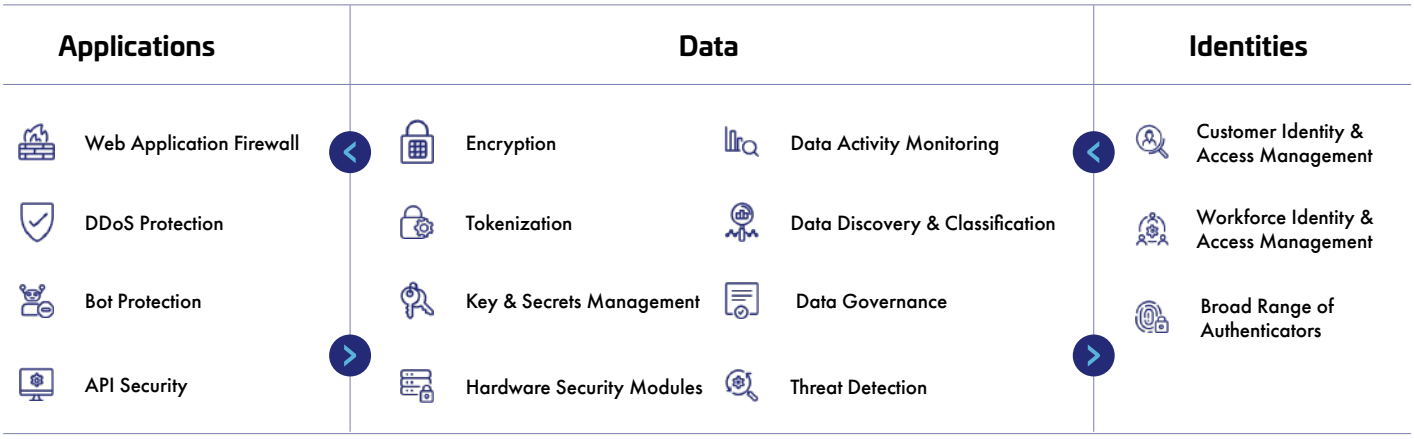


SOCI Act (Amendments)	How Thales helps	Solution Areas
Discovery Business Critical Data (Data Store & Application Data)	• Discover and classify potential risks for all public, private, and shadow **API**s. • Identify structured and unstructured **sensitive data** at risk on-premises and in the cloud. • Identify the current state of compliance, documenting gaps, and providing a path to full compliance.	**Application Security** API Security **Data Security** Data Discovery & Classification Data Risk Analytics Vulnerability Management
Monitor User Activity	• **Data activity monitoring** for structured and unstructured data across cloud and on-prem systems. • Produce **audit trail and reports** of all access events to all systems, and stream logs to external SIEM systems.	**Data Security** Data Activity Monitoring **Identity & Access Management** Workforce Access Management
Protecting Business Critical Data	• Encrypt data at rest on-premises, across clouds, and in **big data or container environments.** • Protect **data in motion** with high-speed encryption. • Gain full **visibility of sensitive data** activity, track who has access, audit what they are doing, and document.	**Data Security** Transparent Encryption Tokenization Key & Secrets Management High Speed Encryption Data Governance Data Activity Monitoring
Access Control	• **Limit the access** of internal and external users to systems and data based on roles and context with policies. • Apply **contextual security** measures based on risk scoring. • Leverage **smart cards** for implementing physical access to sensitive facilities of critical infrastructure	**Identity & Access Management** Workforce Access Management **Data Security** Transparent Encryption Data Risk Analytics

SOCI Act (Amendments)	How Thales helps	Solution Areas
Strong Authentication Mechanisms	• Build and deploy **adaptive authentication policies** based on the sensitivity of the data/application. • Protect against **phishing and man-in-the-middle** attacks	**Identity & Access Management** Multi-Factor Authentication Risk-Based Authentication PKI and FIDO Authenticators
Protecting secrets and cryptographic keys	• Protect **cryptographic keys** in a FIPS 140-2 Level 3 environment. • Streamline **key management** in cloud and on-premises environments. • Manage and protect all **secrets and sensitive credentials**.	**Data Security** Hardware Security Modules Key Management Secrets Management

Thales provides comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

THALES
Building a future we can all trust
+
imperva
a Thales company



Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, a secure Content Delivery Network (CDN), and Runtime Application Self-Protection (RASP).

Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

Organizations can leverage Thales' suite of identity, application and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.