Silverfort

Comply with the Security of Critical Infrastructure (SOCI) Act Requirements with Silverfort

Whitepaper

Executive summary

The Security of Critical Infrastructure (SOCI) act is a federal law first introduced by the Australian Government's Cyber and Infrastructure Security Centre (CISC) in 2018 to guide organisations in identifying, protecting and reporting on critical infrastructure assets that could harm Australia's economy, security or public safety if disrupted.

Originally created for four asset classes (electricity, gas, water and ports), SOCI has since been implemented across 11 critical infrastructure sectors, including communications, data, financial services, health, food, and space. SOCI was amended in 2021, 2022, and most recently with the Enhanced Response & Prevention Act 2024, which went into effect on 4 April 2025.

SOCI defines what constitutes a critical infrastructure asset, their responsible entity and direct-interest holders, and the four Positive Security Obligations (PSOs): asset registration, Critical Infrastructure Risk Management Program (CIRMP), mandatory cyber-incident reporting, and annual board attestation, with additional enhanced obligations for Systems of National Significance.

The main goal of SOCI is to give both government and operators clear, enforceable requirements to prevent, detect and rapidly respond to cyber, supply chain, personnel and physical threats before they cause national-level harm.

To meet the cyber and information security threats requirements, organisations may implement one of five frameworks (or an equivalent standard): ISO/IEC 27001, ACSC Essential Eight Maturity Model, NIST CSF, U.S. Department of Energy C2M2, and the Australian Energy Sector AESCSF.

By aligning with these frameworks, SOCI helps organisations strengthen identity security controls, enforce least privilege, reduce their identity attack surface, and increase their operational resilience across modern, legacy and hybrid environments.

Addressing the identity security aspects of SOCI

SOCI identifies three foundational pillars for enforcing strong access controls and reducing the identity attack surface: identity inventory, multi-factor authentication (MFA), and least privilege, which operators of critical infrastructure assets must comply with

Failure to comply carries heavy civil penalties. Currently, the civil penalty for not adopting and maintaining a CIRMP is up to 1,000 penalty units (AUD 275,000) for individuals, and up to five times that amount (AUD 1.38 million) for corporations.

Other identity-related breaches (for example, missing the 72-hour incident reporting deadline) can result in between 50 and 250 penalty units (AUD 13,750-68,750 for an individual and five times that amount for a corporation).

By following SOCI requirements, organisations can enhance visibility and identity governance while applying dynamic access policies automatically triggered by risk. This strengthens their identity posture against credential compromise, lateral movement, and privilege escalation, while helping them avoid heavy civil penalties.

The Silverfort Identity Security Platform

Silverfort enables organisations to implement the SOCI principles across hybrid environments by enforcing strong authentication and dynamic access controls. The platform extends security controls like MFA, risk-based authentication, PAS (Privileged Access Security) and continuous identity verification to all users, NHIs, devices, and services across on-prem, cloud, and hybrid systems.

By integrating with existing Identity and Access Management (IAM) infrastructure, Silverfort unifies access visibility and control. It helps organisations comply with SOCI by preventing credential compromise, lateral movement, and unauthorised application access, supporting least privilege Just-In-Time (JIT) access, and secure application workflows at scale.

Multi-factor authentication

Extend MFA protection to command-line access, legacy apps, IT infrastructure, and other critical resources that couldn't be protected before.

Securing privileged users

Discover, classify, and enforce least privilege and JIT access policies for all your privileged users.

Continuous monitoring

Gain comprehensive visibility into all authentication and access attempts, monitor and review them continuously to detect anomalies and prevent malicious access in real time.

Detect and respond to identity threats

Detect common credential access, privilege escalation and lateral movement attacks, and respond automatically with real-time blocking.

Compliance table: Silverfort alignment to SOCI's requirements

SOCI Clause	Essential Eight	Information security manual (ISM) Controls	ISO/IEC 27001	NIST CSF	Silverfort Security Controls
s 23 The responsible entity must give the Secretary interest and control information within 6 months.	—	ISM-0407 (Account register); ISM-1171 (Quarterly review)	5.9 Inventory of information & other associated assets – identify, record and assign ownership to every information asset.	ID.AM-02: Inventories of software, services and systems managed by the organisation are maintained.	Silverfort provides a comprehensive identity inventory that includes human and non-human identities (NHIs) across hybrid environments. Silverfort offers visibility into which users and systems exist in the environment, who is accessing what, and with what authentication method or protocol. This supports the maintenance of an accurate identity asset inventory aligned with access governance requirements, helping ensure entities can identify and document relevant ownership and control relationships.
s 24 A reporting entity must notify a notifiable event within 30 days after becoming aware of it.	—	ISM-0123 (Incident Escalation); ISM-1650 (Central log)	5.24 Information-security incident management – planning & preparation.	RS.CO-02: Internal and external stakeholders are notified of incidents.	Silverfort supports incident response planning and escalation by enabling organisations to detect, contain, and respond to identity threats in real time. Silverfort assists with incident analysis by providing detailed logs of all authentication and access activities. Silverfort's real-time monitoring capabilities enable it to detect anomalies and suspicious activities, providing insights into the course of an incident. Upon detection of a suspicious activity, Silverfort can trigger automated enforcement policies, such as requiring MFA, blocking access, or isolating affected accounts. Silverfort integrates with SIEM platforms to escalate alerts through defined workflows and notify internal and external stakeholders based on policy. This ensures that security events involving compromised accounts or unauthorised access are immediately surfaced and routed to the appropriate teams, supporting compliance with the 30-day notification requirement.

SOCI Clause	Essential Eight	Information security manual (ISM) Controls	ISO/IEC 27001	NIST CSF	Silverfort Security Controls
s 30AC The entity must adopt and maintain a Critical Infrastructure Risk Management Program (CIRMP).	Multi-factor authentication is used to authenticate privileged users of systems.	ISM-0974 (MFA for unprivileged accounts); ISM-1173 (MFA for privileged accounts)	5.17 Authentication information – govern creation & use of credentials.	PR.AA-03: Users, services and hardware are authenticated.	Silverfort provides MFA protection for both privileged and unprivileged users across all environments, including legacy systems. Silverfort enforces adaptive, risk-based MFA policies that evaluate authentication requests based on context such as device integrity, user location, and protocol used. When anomalies or elevated risks are identified, Silverfort dynamically prompts users with additional MFA challenges or restricts access to prevent unauthorised entry.
CIRMP r⊠8 The program must identify and mitigate hazards relating to (a) cyber and information security; (b) personnel; (c) supply chain; (d) physical; (e) natural hazards.	Requests for privileged access to systems, applications and data repositories are validated when first requested.	ISM-0974 (MFA for unprivileged accounts); ISM-1173 (MFA for privileged accounts)	8.2 Privileged access rights – restrict & review all elevated privileges.	PR.AA-05: Access permissions, entitlements and authorisations are defined, managed, enforced and reviewed, incorporating least-privilege and separation of duties.	Silverfort's Privileged Access Security (PAS) continuously monitors and restricts access by privileged and service accounts. It provides fully automated visibility and monitoring of system/service accounts and includes classification of pure machine-to-machine accounts, accounts that are used interactively, and accounts that access a significantly large number of destinations. Additionally, each account's sources, destinations, privilege level, and risk score are aggregated and displayed, enabling organisations to assess and respond to potential misuse. PAS policies can block any access attempt that deviates from the service account's normal behaviour, enforcing access controls that align with least-privilege and separation of duties principles.

SOCI Clause	Essential Eight	Information security manual (ISM) Controls	ISO/IEC 27001	NIST CSF	Silverfort Security Controls
s 30AG / CIRMP r⊠15 The responsible entity must give an annual report in the approved form signed by the board.	—	ISM-0718 (Board cyber-posture report)	5.4 Management responsibilities – top management demonstrates leadership and reviews cyber performance.	GV.OV-01: Cyber-risk-management strategy outcomes are reviewed to inform and adjust strategy and direction.	Silverfort helps leadership meet their obligations for annual board-level reporting on cyber risk posture. Risk reports generated by Silverfort offer centralised visibility into identity-related threats, authentication activity, access trends, and anomalous behaviour across the environment. These reports are used to support audits and provide reliable evidence for legal, operational, and compliance purposes, and can be exported or integrated into existing executive dashboards.
s 30BC Notify a critical cyber security incident within 12 hours.	Following the identification of a cyber-security incident, the cyber-security incident response plan is enacted.	ISM-0140 (ASD notification ≤ 12 h)	5.24 Incident management – plan covers rapid escalation.	RS.MA-01: The incident-response plan is executed, in coordination with relevant third parties, once an incident is declared.	Silverfort enables organisations to begin the incident response process with a complete malicious access lockdown. Depending on the intensity and scope of the ongoing attack, organisations can determine the level of lockdown and the balance between MFA and block access policies. Most often, MFA would achieve the same level of containment as block access, while allowing legitimate users to continue to access resources. MFA is especially effective since it provides a clear indication of which accounts have been compromised, achieving both containment and discovery simultaneously. Silverfort's response capabilities provide a clear indication of compromised accounts, enabling immediate containment and supporting investigation. By denying access in real time based on behavioural anomalies, Silverfort supports rapid execution of the CIRMP requirements. These actions can be triggered automatically or escalated through SIEM workflows to ensure timely coordination with internal and external stakeholders.

SOCI Clause	Essential Eight	Information security manual (ISM) Controls	ISO/IEC 27001	NIST CSF	Silverfort Security Controls
s 30BD Notify any other cyber security incident within 72 hours.	Cyber-security incidents are reported to ASD as soon as possible after they occur or are discovered.	ISM-0123 (Internal escalation)	5.24 (as above)	RS.MA-01 (as above)	Silverfort continuously monitors identity behaviour across all access attempts to detect suspicious activity. All events, including failed MFA, policy violations, and service account activity, are logged with full metadata and can be exported to support investigation, triage, and reporting workflows aligned with 72-hour incident notification requirements.
CIRMP r 22 The entity must keep incident records for 7 years.	Event logs are protected from unauthorised modification and deletion.	ISM-0125; ISM-1803 (7-year retention)	5.33 Protection of records – prevent loss or unauthorised alteration.	PR.DS-11: Back-ups of data are created, protected, maintained and tested.	Silverfort securely logs all authentication events, access attempts, and policy decisions. Logs can be exported to external SIEM platforms in CEF format for long-term retention and evidentiary support, ensuring traceability of identity-related incident records over a multi-year retention period.
s 30ED The entity must consider measures to eliminate or reduce the risk specified in a risk notice.	—	ISM-0726 (CISO coordination)	5.4 (as above)	GV.RM-04: Strategic direction describing appropriate risk-response options is established and communicated.	Silverfort enforces granular identity access controls that can be configured and updated in real time. Policies may require MFA, block specific access paths, or isolate high-risk users based on behavioural or contextual risk indicators. These adaptive controls can be aligned with security measures recommended in a formal risk notice and activated across hybrid and legacy environments without infrastructure changes.

SOCI Clause	Essential Eight	Information security manual (ISM) Controls	ISO/IEC 27001	NIST CSF	Silverfort Security Controls
s 35AB The entity must comply with an information request, action or intervention direction.	Following the identification of a cyber-security incident, the cyber-security incident-response plan is enacted.	ISM-0733 (CISO oversight)	5.24 (as above)	RC.RP-01: The recovery portion of the incident-response plan is executed once initiated from the incident-response process.	Silverfort helps organisations implement concrete post-incident response controls that reduce the likelihood of recurrence and improve preparedness for future events. Silverfort automatically creates an access policy to each system/service account that, when enabled, blocks any access attempt that deviates from the service account's normal behaviour. This enables a persistent safeguard for accounts previously abused or compromised. Silverfort also provides continuous access monitoring and identity risk analysis that helps organisations revalidate entitlements, identify overprivileged accounts, and enforce updated MFA and access policies. These capabilities allow teams to implement durable technical controls immediately after an incident.
s 30CD (SoNS) The responsible entity must have an incident response plan for the asset.	Following the identification of a cyber-security incident, the cyber-security incident-response plan is enacted.	ISM-0576 (Plan developed); ISM-1819 (Plan exercised)	5.24 (as above)	RS.MA-01 (as above)	Silverfort provides identity-first incident response within hours of deploying our platform, even in the most complex multi-domain environments with hundreds of Domain Controllers. Silverfort continuously monitors authentication behaviour across all users and protocols and alerts in real time when risky activity is detected. These alerts can trigger automated policy responses, such as access denial or MFA enforcement. All incidents are logged centrally and can be integrated with broader incident response playbooks for rapid containment and forensic investigation.

SOCI Clause	Essential Eight	Information security manual (ISM) Controls	ISO/IEC 27001	NIST CSF	Silverfort Security Controls
s 45 Unauthorised disclosure of protected information is an offence.	—	ISM-1535 (Export/control of sensitive data)	5.31 Legal, statutory, regulatory & contractual requirements identify and comply with information-security obligations.	PR.DS-02 (as above)	Silverfort enforces end-to-end encryption for all data in transit between Silverfort and the identity infrastructure, and all authentication logs and identity telemetry data, as well as role-based access controls to prevent unauthorised access to stored identity-related data, and all logs are tamper-resistant. These protections ensure secure handling of identity metadata and authentication records, supporting confidentiality obligations for protected information.
Privacy Act s 6(1) Personal information means information or an opinion about an identified individual.	—	ISM-1535 (Export control of personal data)	5.34 Privacy & protection of PII – implement measures to safeguard personal information.	PR.DS-02 (as above)	Silverfort applies strong encryption, access restrictions, and privacy-respecting audit controls to all identity-related telemetry, including data that may contain personally identifiable information (PII). Logs are encrypted and access is governed by RBAC. The Silverfort platform aligns with ISO/IEC 27001:2022 and major privacy frameworks including GDPR, CCPA, and the EU-U.S. Data Privacy Framework.

About Silverfort

Silverfort secures every dimension of identity. We are the first to deliver end-to-end identity security across the entire IAM infrastructure, eliminating gaps and blind spots, giving organisations visibility into their identity fabric and extending protection to resources that previously could not be protected. This is all done via a patented technology that natively integrates with the entire IAM infrastructure, Runtime Access Protection™(RAP). It is lightweight, easy to use and deploy, and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyse exposures to reduce your attack surface, and enforce security controls inline to stop lateral movement, ransomware propagation, and other identity threats.

Learn more