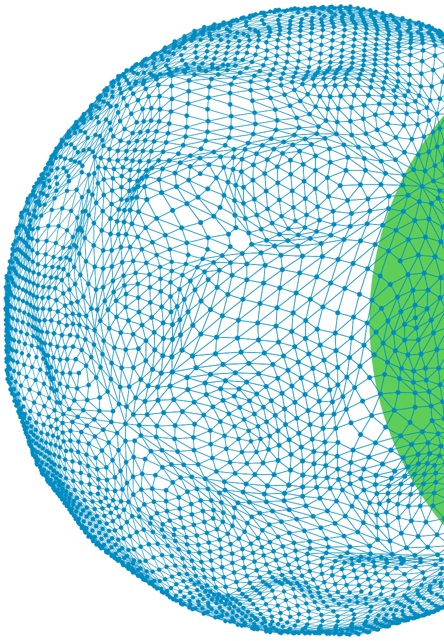
Australian Critical Infrastructure Act requires increased cybersecurity maturity

Minimize risk, prioritize remediation efforts, reduce cybersecurity compliance and reporting costs, and increase reporting speed



The Australian Security of Critical Infrastructure Act (the Act) provides a framework for managing the complex and evolving national security risks relating to critical infrastructure – including sabotage, espionage, and coercion posed by foreign interference. Many organisations are experiencing a substantial compliance gap due to the Security Critical Infrastructure Act of 2018 and its recent amendments.

In December 2021, amendments to the Act expanded coverage from four to eleven critical infrastructure sectors and 22 asset classes. Not surprisingly, organizations in the newly nominated sectors have the most significant gap. Those covered previously, however, may also need to take steps to comply with new provisions.

The amended Act includes a Register of Critical Infrastructure Assets and mandatory cyber incident reporting. It contains new Government Assistance measures to intervene when entities fail to respond effectively to serious cyber-attacks, increasing the potential cost of non-compliance. Changes also give the responsible Minister broad powers to declare services as Systems of National Significance. This new asset class extends the legislation's requirements to suppliers to the 11 nominated critical infrastructure sectors.

The legislation has also been greatly expanded to cover new sectors, creating a large compliance gap for many organizations. A new asset class, Systems of National Significance, means that the Act also covers suppliers to the 11 nominated critical infrastructure sectors. And new Government Assistance measures have increased the potential cost of non-compliance.

Critical infrastructure act lacks prescriptive guidance

Unlike the Essential Eight cybersecurity framework published by the Australian Signals Directorate (ASD), the Act is not prescriptive. Rather than specifying particular security controls to manage risk, the emphasis is on cybersecurity processes to ensure that organizations:

- **Identify risks and apply appropriate security controls**
- **Report incidents and address them effectively**
- **Take measures to prevent the reoccurrence of incidents**

Under the Act, the Australian government can also intervene directly in how business is conducted during severe cyber-attacks. Potential interventions include assigning government personnel to an organization and requiring it to install systems information software of the government's choice.

High-profile ransomware attacks on healthcare, higher education, and transport organizations underscore the need for continued cybersecurity investments in these sectors. Suppliers to the 11 nominated sectors should also assess their compliance with the Act and adopt an appropriate level of cybersecurity – or risk consequences that include losing business or incurring a costly government intervention during a serious cyber-attack.

Act's 11
critical infrastructure expansion sectors

- communications
- data storage or processing
- defense
- energy
- financial services and markets
- food and grocery
- healthcare and medical
- higher education and research
- space technology
- transport
- water and sewerage

Structural challenges lower the entry barrier for attackers

Historically, SCADA and industrial control systems that serve sectors including energy, transport, and water and sewage were comprised of highly specialized proprietary devices with long life spans. Such equipment was often ruggedized with strict uptime and latency requirements. Device longevity and deployment in remote locations increased the likelihood of software obsolescence and unpatched vulnerabilities. A simple patching procedure, for instance, may require complex change management processes due to the risk of equipment downtime or unforeseen hazards. To minimize their exposure, industrial automation equipment and critical infrastructure were traditionally "air-gapped" – or not connected to the public internet.

Over recent years, the tangible benefits of IT/OT convergence have catalyzed a new hyperconnected Industrial Internet of Things (IIoT) realm. Increasingly, OT sensing devices are connected to the network and thus exposed to a broad array of cyber-attacks, proving the existence of an IT/OT attack continuum. The cybersecurity talent gap and lack of specialized expertise around converged IT/OT architectures also compounds the challenges.

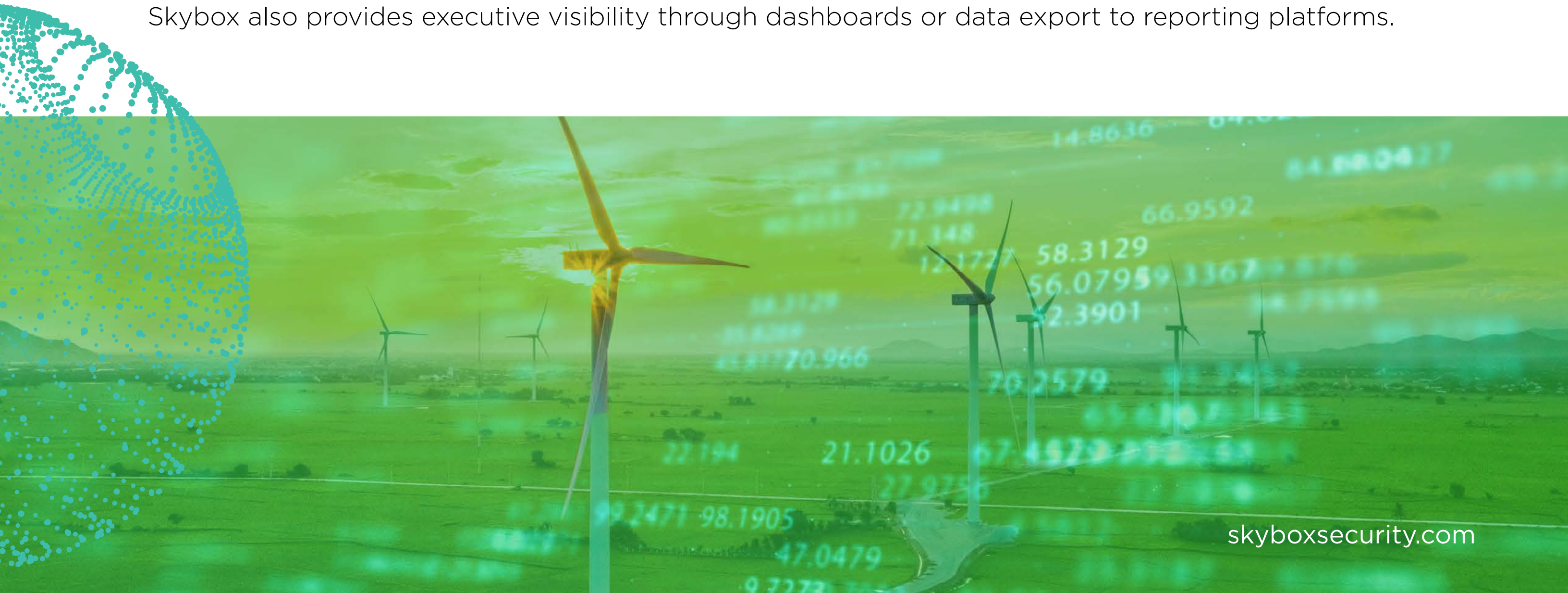
Forge a new approach to cybersecurity compliance

Organizations need a new proactive approach to risk mitigation that will significantly simplify and reduce the cost of complying with the Act. Skybox Security helps organizations strengthen overall security efficacy and limit exposure to cyber-attacks. In particular, the Skybox Security Posture Management Platform enables organizations to address their obligations under the Critical Infrastructure Act as and when required. It is the only security platform that allows organizations to collectively visualize and analyze hybrid, multi-cloud, and OT networks – providing full context and understanding of their attack surface.

Skybox identifies and centralizes data from systems and IT assets subject to the Act. It enables security teams to analyze these data sets to identify and remediate exposure risk and compliance violations. Such device-independent analytic capabilities allow small teams to manage compliance initiatives in large, heterogeneous IT, OT, and converged estates. When combined with actionable insights from Skybox Threat Intelligence, context from the hybrid infrastructure allows security leaders to balance connectivity needs with exposure risks. To minimize the cost of compliance, Skybox automates the following key areas:

- Essential compliance workflows such as access and segmentation analysis
- Compliance checks across corporate and regulatory policies for firewall and network device configuration
- Vulnerability discovery, prioritization, remediation, and reporting
- Context and risk-aware change management processes for connectivity
- Audit and compliance reporting tasks

Skybox also provides executive visibility through dashboards or data export to reporting platforms.



How Skybox helps you comply with the Act

The following table summarizes obligations under the Act and how Skybox helps customers meet those requirements:

Obligations	How the Skybox Security Posture Management Platform helps customers address Act requirements
Critical infrastructure assets	
Adopt and maintain a risk management program for specified assets:	Skybox provides comprehensive visibility of IT assets and hybrid network infrastructure. It integrates with other cybersecurity solutions, identifies and prioritizes risks, assures security controls, and automates compliance workflows.
+ Provide ownership and operator information for specified assets	Skybox consolidates datasets across security, cloud, network, and endpoint technologies. It integrates and augments CMDB information with data from scores of network devices and security solutions to create a comprehensive repository of IT assets.
+ Identify each hazard where there is a material risk of a relevant impact	With essential data from a wide range of security, cloud, and network technologies, Skybox creates a network model that visualizes all security controls and network configurations. Leveraging intelligence from the Skybox Research Lab, Skybox identifies exploitable vulnerabilities and correlates them with the network model to determine where cyber attacks pose the highest risk to the organization.
+ As far as reasonably possible, minimize or eliminate the risk of each hazard	Skybox supports a systematic, targeted approach to improve vulnerability management and continuously reduce the attack surface. The platform aggregates asset and vulnerability information from active scanning based on VA scanners, passive scanning based on specialized OT security solutions, and its own unique scanless vulnerability detection technology that fills in blind spots between active scan events. Combining context and visibility from the converged infrastructure with insights from Skybox Threat Intelligence, Skybox prioritizes the riskiest vulnerabilities for immediate remediation. The Skybox multifactor risk scoring framework incorporates CVSS severity ratings, asset importance, exploitability, and network-based exposure analysis to identify the vulnerabilities that could cause the most harm. Skybox can recommend effective, less disruptive alternatives to measures, such as patching or updates, which can cause downtime. The Skybox platform can identify risks from misconfigurations in network and firewall infrastructure when compared with customized or OOB policy templates.
+ Mitigate the relevant impact due to the hazard occurring	Skybox can model interdependencies and potential leverage between IT and operational technology (OT) assets. Organizations can readily understand the impact of potential cybersecurity incidents and identify mitigating controls.
Mandatory reporting of serious cyber incidents for specified assets:	Skybox supports customizable risk and compliance reporting in a singular view, enabling organizations to simplify and automate compliance assessment across their infrastructure.
+ Annually, report whether the risk management program is up to date and how it varied through the year	Skybox integrates with other cybersecurity solutions for complete visibility across the security stack. Organizations can see if their risk management program is up to date and track any changes.

Obligations	How the Skybox Security Posture Management Platform helps customers address Act requirements
+ Annually, identify hazards that have had a significant impact and evaluate the effectiveness of the program	With Skybox, organizations can consolidate information about cyber threats and their impacts and analyze the in-place security controls to provide a report card of their effectiveness.
+ Report incidents with a significant impact within 12 hours	Information in Skybox is continually updated, so reporting is an automatic exercise rather than a manual process that takes days or weeks of work.
Services of National Significance (SoNS)	
Adopt and maintain an incident response plan for cybersecurity incidents:	Skybox provides system and security information, including vulnerability assessments, as and when required. With in-depth network modeling and sophisticated attack simulation, organizations can visualize potential cyber incidents and define effective strategies to respond to or prevent them.
+ Engage in a cybersecurity exercise	Skybox attack simulations attempt to exploit all vulnerabilities on all assets from all threat origins since one security gap is all an attacker needs to infiltrate a network. The simulated attack attempts to move data past existing security controls, as in an actual attack, and assigns context-based risk. If a simulated attack results in the complete compromise of a host, another simulation is run using the compromised host as a threat origin to understand the risk of stair-step or pivot attacks. Attack simulation data enables vulnerabilities to be prioritized by actual risk. To understand how best to move forward with targeted, efficient remediation, security teams can view simulation results from multiple perspectives, such as threat origin, network segment, business unit, or asset.
+ Undertake a vulnerability assessment	The Skybox platform enables organizations to produce assessments within minutes, not days or weeks, by leveraging its asset repository, passive scanning capabilities, and threat intelligence service.
+ Provide periodical or event-based reporting of system information	Skybox consolidates datasets across security, cloud, network, and endpoint technologies. It integrates and augments CMDB information with data from scores of other network and security solutions to create a comprehensive security-centric repository for reporting on information assets.
+ Require installation of system information software	Providing systems and security information on demand reduces the risk and potential cost of government interventions.

Reduce the cost of reporting and compliance

The Act requires comprehensive reporting capabilities. Regulatory authorities need to understand the risks that assets are exposed to and whether they are effectively mitigated. Maintaining a single platform that satisfies the Act's multiple reporting requirements is far less costly than maintaining a patchwork of siloed solutions.

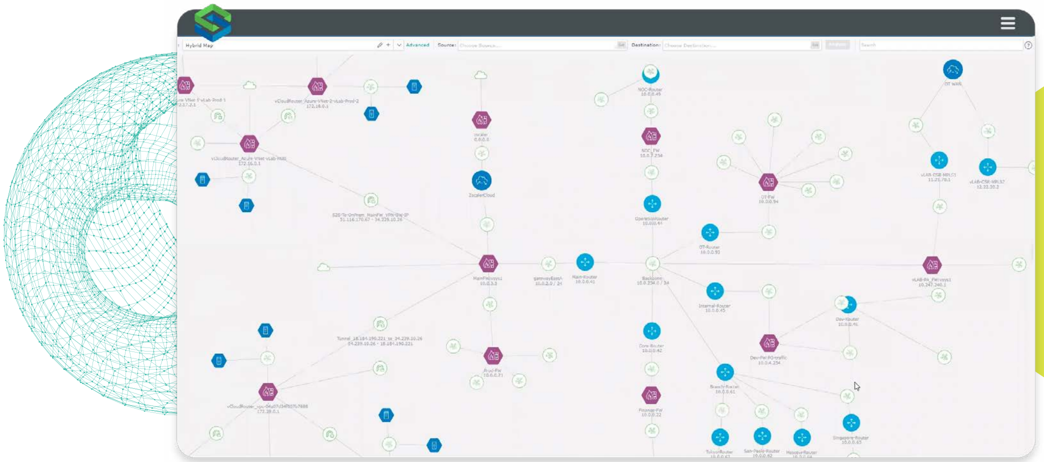
Skybox integrations with multiple vendors' toolsets enable information to be consolidated in a single place in a standardized format. Organizations can simplify and automate compliance with a singular view of the entire hybrid infrastructure and customizable risk and compliance reporting. Information is continually updated, making reporting an automatic exercise rather than a manual process that takes days or weeks of work.

Quickly identify and report cyber risks

Skybox is the only platform that comprehensively analyzes and validates network, cloud, and security configurations in order to understand an organization's attack surface. These capabilities allow Skybox to classify information assets by criticality and risk, unlike a CMDB, and map vulnerabilities and exposures to individual assets.

The platform integrates with an organization's other cybersecurity solutions to provide complete visibility across the security stack. Organizations can evaluate security policies and controls and provide a report card of their effectiveness.

Skybox can also provide an overall risk score based on business attributes rather than technical ones, allowing regulatory authorities and other entities in critical infrastructure supply chains to clearly understand risk exposure. The risk score allows organizations to report in minutes, not weeks, if required.



Searchable, customizable view of an organization's network topology

Minimize or eliminate risks

With the ability to model cyber risks and threat vectors across an organization's entire infrastructure, Skybox can prioritize and reduce the cost of mitigation efforts.

Skybox can analyze how each element in an organization's security stack functions. This single vantage point enables security teams to be significantly more productive than managing the pieces individually.

Skybox can recommend a range of actions to minimize or eliminate each risk. For example:

- For endpoint systems, Skybox can understand whether all the controls specified in the ASD's Essential Eight have been implemented and are operational.
- Skybox can monitor the vulnerabilities that exist in Internet-exposed systems and the steps, such as patching, to eliminate them.
- Skybox can act as a central management point for traditional and next-generation firewall policies to understand how an asset can be ring-fenced from potential Internet exposure.

Dynamically prioritize threat mitigation

Due to an ever-changing, complex attack surface, many organizations struggle to deal with expanding cybersecurity risks. With Skybox, organizations can visualize their information assets, attack surfaces, and vulnerabilities across their entire infrastructure to dynamically prioritize mitigation efforts.

An organization may have hundreds or thousands of vulnerabilities, which presents a seemingly impossible remediation task. With Skybox, organizations can see that the number of exposed vulnerabilities may be an order of magnitude smaller, and the exploitable subset could be smaller again.

Skybox also provides oversight of the remediation process, tracking remediation efforts and verifying measures to eliminate or mitigate vulnerabilities. This information is also available for any subsequent reports.

Gain a better understanding of cybersecurity impacts

Skybox models the interdependencies and potential leverage among assets. If element A is compromised, for example, Skybox understands the possible lateral movement to element B and can quantify the risk. This modeling is particularly important in Operational Technology (OT) environments commonly deployed in critical infrastructure.

While information assets in IT environments can be taken offline relatively quickly and updated or patched, this is not usually the case in OT environments. And with some cyber incidents, such patches or updates may not yet exist.

Skybox, however, can quickly identify alternative controls by understanding the interdependencies among assets. If a system cannot be taken offline for immediate remediation, for instance, a network security rule, such as blocking the attack path, might effectively mitigate the cybersecurity impacts – and allow the organization to patch or update the affected system at a later time.

Immediately respond to requests

Under the Act, vulnerability assessments may be required for organizations that provide Systems of National Significance. Skybox's comprehensive exposure analysis capabilities enable organizations to produce these assessments within minutes, not days or weeks. Skybox enables this via its passive scanning capabilities and threat intelligence service, which generate daily updates about the dynamically changing risk environment.

With passive scanning, Skybox does not need to actively scan information assets to understand that they have become vulnerable. Instead, Skybox compares its repository of an organization's information assets and security controls with the latest threat intelligence. This comparison flags exposed vulnerabilities that have moved from proof of concept to exploitable. Skybox escalates their remediation through a customized dashboard.

On the other hand, organizations that conduct weekly or monthly vulnerability scans or penetration tests cannot provide up-to-date vulnerability assessments on demand. Skybox's approach increases the productivity of security teams and enables them to respond immediately to requests.

Close critical infrastructure compliance gaps with Skybox Security

The extended coverage and new provisions included in the recent amendments to the Act have created significant compliance gaps for many organizations. Skybox Security can help organizations get ahead of these gaps by taking a proactive approach to mature their cybersecurity programs. This requires the creation of mature, consistent, and organization-wide security posture management programs. A joint approach across the IT and OT organizations enables leaders to optimize security planning, deployment, and remediation processes to reduce exposure risk.

Want to learn more? Get a demo or talk to an expert:

skyboxsecurity.com/request-demo

ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization.