TIER SIXTEEN

ASTRA
SECURING CRITICAL INFRASTRUCTURE

ENABLING & DEFENDING

AUSTRALIA'S CRITICAL INFRASTRUCTURE

Our comprehensive approach, goes beyond assessment, design, implementation and support. **We take a holistic approach to cyber security and resilience** covering aspects around people, process and technology.

The functioning of Australia's economy and society is underpinned by our critical infrastructure assets and essential services. However, geopolitical tensions and heightened cyber threats mean Australia's critical infrastructure is increasingly under threat.

The **Security of Critical Infrastructure Act (SOCI Act)** and the **Australian Energy Sector Cyber Security Framework (AESCSF)** are both pivotal regulatory structures aimed at bolstering the resilience and security of Australia's critical infrastructure sectors.

While the **SOCI Act** provides a broad regulatory framework addressing various risks, including cyber-attacks, the **AESCSF** specifically targets cyber security threats within the energy sector.

WHY IS THIS IMPORTANT

VITALITY | Society is largely dependent on the services provided by critical infrastructure organisations. The continuity of these services are vital for society to function, but often taken for granted in a modern society.

PHYSICAL IMPACT | Malfunction of components of critical infrastructure can have potential physical impact on human safety, the natural environment, and other critical infrastructure.

SYSTEM OF SYSTEMS | Critical Infrastructure sectors are highly interconnected and mutually dependent in complex ways, both physically and through a host of communications technology.

EASY TARGETS | The complexity, age and lack of security by design make these sectors easy targets for malicious actors to create wide-spread disruption and damage.

OPERATIONAL RESILIENCE | To manage operational risks, system resilience play a key part in sustainable operation and recovery of assets when affected by internal or external factors.

We provide more than regulatory compliance support; we build resilience, ensuring your business thrives, adapts quickly, and consistently delivers value for long-term success.

12

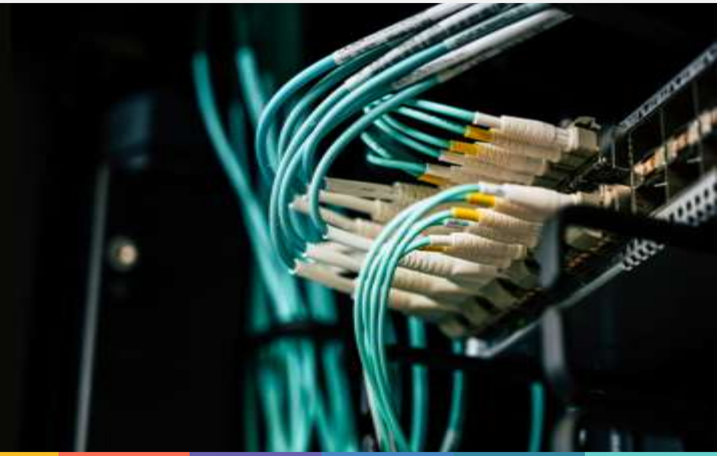
REMAIN COMPLIANT

CIRMP MAINTENANCE

At a minimum, a CIRMP must be reviewed once every 12 months.

Addressing Regulatory Compliance

NAVIGATE COMPLIANCE



AESCSF ASSESEMENTS

Evaluate the maturity of your industrial cybersecurity practices, identifying areas for improvement and strengthening your resilience to cyber threats.

REGULATORY GAP ANALYSIS

Conduct regulatory gap analysis for SOCI Act obligations, using our expertise to identify gaps and provide actionable recommendations for improvement.

OT CYBER PROGRAM MANAGEMENT & EXECUTION

Design and implement a comprehensive OT Cyber and Resilience Program tailored to the regulatory landscape of the industrial sector, ensuring adherence to SOCI Act requirements.

INCIDENT RESPONSE READINESS

Develop and implement response strategies specific to industrial environments, ensuring that actions taken do not disrupt critical operational processes or cause additional harm.

OPERATIONAL RESILIENCE

Enable organisations to deliver critical services and maintain plant operations, even through disruptive events.

PROTECT YOUR INVESTMENT

Analyse physical loss of asset impact through failure or potential cyber attack scenarios and provide advice to reduce the likelihood of such events.

CROWN JEWEL ANALYSIS TECHNOLOGY DEPENDENCIES

Pinpoint your most critical industrial assets and analyse their technological dependencies to strengthen vital systems and safeguard operational continuity.

ACTIONABLE INSIGHTS FROM ASSET MANAGEMENT AND MONITORING

Obtain actionable insights with comprehensive asset management and monitoring, optimising the performance and security of critical industrial systems to maintain operational continuity.

TIER SIXTEEN

ASTRA
SECURING CRITICAL INFRASTRUCTURE

01

02

03

04

Assess | Secure | Reinforce

DOMAIN FOCUS

We help strengthen the security and resilience of critical infrastructure assets across three crucial domains.

Each domain and its sub-components play a crucial role in securing your interconnected environments, and by strengthening each component, we **reinforce the entire system.**

GOVERNANCE AND POLICY

OT Security Program Management

CIRMP Management

Risk Assessment and Management

OT Governance Framework

OT Policies and Standards

CIRMP Reporting

SECURITY AND ARCHITECTURE

Access and Identity Management

OT **Architecture**

Security Logging and Monitoring

Vulnerability Management and Monitoring

Third Party Security

Incident Response

ASSET MANAGEMENT

Asset **Inventories**

Asset **Relationships**

Asset **Lifecycles**

Change Management

Configuration Management

Disaster **Recovery**

01

02

03

04

GOVERNANCE AND POLICY

OT SECURITY PROGRAM MANAGEMENT

Many OT Cyber Programs **Fall Short** of Ensuring Resilience

A comprehensive OT security program is crucial for unifying security efforts, addressing vulnerabilities, and safeguarding industrial control systems against cyber threats.

RISK ASSESSMENT & MANAGEMENT

Misunderstood Risks Undermine the Resilience of Industrial Operations

Regular risk assessments and proactive risk management strategies are vital to identify and address potential threats before they disrupt your industrial processes and cause costly downtime.

OT POLICIES AND STANDARDS

Misaligned Policies and Standards Leave Industrial Systems Vulnerable

IT-centric standards often push controls that don't work or make sense for OT environments. Tailored policies aligned with industry best practices are crucial for effective protection.

CIRMP MANAGEMENT

Ineffective CIRMPs Fail to Address Actual Risks to Critical Infrastructure Assets

A fit-for-purpose and regularly updated CIRMP is essential for effectively managing cyber program elements, accurately identifying risks, and ensuring the protection of critical infrastructure assets.

OT GOVERNANCE FRAMEWORK

Weak OT Governance Hinders Cybersecurity Decision-Making

A robust OT governance framework establishes clear roles, responsibilities and processes, empowering your organisation to make informed decisions and respond effectively to cybersecurity challenges.

CIRMP ANNUAL REPORTING

Incomplete Reporting **Conceals True Risks** to Critical Infrastructure

Accurate and thorough CIRMP reporting is essential for providing transparency in risk management efforts, ensuring compliance, and enabling continuous improvement in the protection of critical infrastructure.

SECURITY AND ARCHITECTURE

ACCESS & IDENTITY MANAGEMENT

Inadequate Access Controls Leave Industrial Systems Vulnerable

Rigorous access and identity management safeguards industrial systems by ensuring only authorised personnel have access, preventing unauthorised intrusions and mitigates risks.

OT ARCHITECTURE

Flawed OT Architecture Undermines Operational Resilience

A well-designed OT architecture, aligned with site operations and incorporating network segmentation, industrial firewalls and hardened devices, is the backbone of resilient site operations.

SECURITY LOGGING & MONITORING

Blind Spots in Monitoring eave Industrial Networks Vulnerable

Comprehensive security logging and monitoring eliminates blind spots, providing early detection of anomalies, enabling swift response to potential threats, and ensuring continuous operation.

VULNERABILITY MANAGEMENT & MONITORING

Get Proactive with Threat-Informed Vulnerability Management

Robust threat and vulnerability management proactively identifies and addresses weaknesses in your industrial control systems, staying one step ahead of evolving cyber threats.

THIRD PARTY SECURITY

Weak Third-party Interfaces Opens Backdoors to Industrial Environments

A stringent third-party security program ensures that vendors and suppliers adhere to rigorous security standards, protecting your industrial ecosystem from external threats.

INCIDENT RESPONSE

How you **Respond Matters!**

A well-defined and exercised incident response plan minimises downtime, enables swift containment, and ensures rapid recovery from cyber incidents, safeguarding your operational continuity.

01

02

03

04

ASSET MANAGEMENT

ASSET INVENTORIES

Managing **detailed inventory** allow for an efficient asset management strategy

Inventory management is integral to understanding recovery and management process associated with lifecycle management.

ASSET RELATIONSHIPS

Mapping asset dependencies is crucial to understanding dependencies between assets

This allows engineering staff to manage the risk associated with asset upgrades and migration.

ASSET LIFECYCLES

Defining product and asset software lifecycles form an integral part of OT asset management

Hardware and software have very different lifecycles that both need to be addressed separately.

CHANGE MANAGEMENT

Change management is **key to mitigating the risk** associated with hardware and software changes.

Understanding the risk associated with change, forms an integral part of the asset lifecycle process.

CONFIGURATION MANAGMENT

Configuration management is the **heart of any software** within an OT environment.

Treating software as an asset and managing it as such is of utmost importance in maintaining configuration files and recovery of assets affected by adverse events.

DISASTER RECOVERY

The ability to recover from adverse events is key to **recovering assets** to an operational state with minimum disruption

A detailed disaster recovery plan should support staff to minimise the delay in recovering a business system function or process.

01

02

03

04

ASTRA
SECURING CRITICAL INFRASTRUCTURE

ENABLING AND DEFENDING AUSTRALIA'S CRITICAL INFRASTRUCTURE

CREDENTIALS

OSCP OSEP OSWE

CISA CDPSE CRISC

GICSP GCIH GSEC

We improve operational resilience, enhance productivity and drive business growth, through industrial control systems and OT cyber security solutions.

SERVICES

OT Audits and Gap Assessments

Network and Communications Design

I.T. Infrastructure Services

Enterprise OT Architecture

OT Policy Framework

OT Development Roadmap

ICS Engineering and Integration

ICS FAT/SAT and Commissioning

- ✓ **ICS** Threat Modelling
- ✓ **ICS** Asset Discovery and Management
- ✓ **ICS** Security Risk Assessment
- ✓ **ICS** Network Assessment and Design
- ✓ **ICS** Crown Jewel Analysis
- ✓ **ICS** Security Architecture
- ✓ **ICS** Security Monitoring
- ✓ **ICS** Incident Response Readiness

TECHNOLOGIES

Rockwell Automation

AVEVA PARTNER NETWORK

Alliance Registered Schneider Electric

SIEMENS

canary Certified Partner

Ignition Gold Certified Integrator

TIER/ SIXTEEN/

ASTRA

SECURING CRITICAL INFRASTRUCTURE

Our strategic partnership not only addresses **current regulatory demands but also prepares clients for future challenges** in an increasingly complex operational technology security and architecture landscape.

INTEGRITY

INNOVATION

QUALITY

WHY US

With deep technical expertise, operational experience and practical implementation capabilities, we distinguish ourselves from competitors who primarily identify problems, conduct research, propose solutions, and facilitate changes.

Our experience is exemplified by our successful track record.

PERTH | 08 6270 6307 sales@tier16.com www.tier16.com

MANAGING DIRECTOR
Rheinhardt Peens
T / +61 (08) 6270 6307
E / rheinhardt@tier16.com

Disruption can have far-reaching consequences and ensuring operational resilience is crucial. **We approach organisational vulnerabilities with minimal disruption to business operations, a comprehensive understanding of industry challenges, and a proactive stance on security.** We focus on addressing the evolving challenges of critical infrastructure security, ensuring sustained protection and resilience in an increasingly volatile environment.