OpusV

Cybersecurity Solutions for Critical Infrastructure



Supporting Critical Infrastructure Environments in Adherence to the Australian Energy Sector Cybersecurity Framework (AESCSF)

WHAT IS THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018 (SOCI ACT)?

The Security of Critical Infrastructure Act 2018 (SOCI Act) provides a framework for the regulation and protection of the 11 critical infrastructure sectors within Australia.

Part 2A of the SOCI Act requires that the entity responsible for an asset classified as critical infrastructure must have, enforce, and comply with a **Critical Infrastructure Cyber Risk Management Program (CIRMP).**

WHAT IS A CRITICAL INFRASTRUCTURE CYBER RISK MANAGEMENT PROGRAM (CIRMP)?

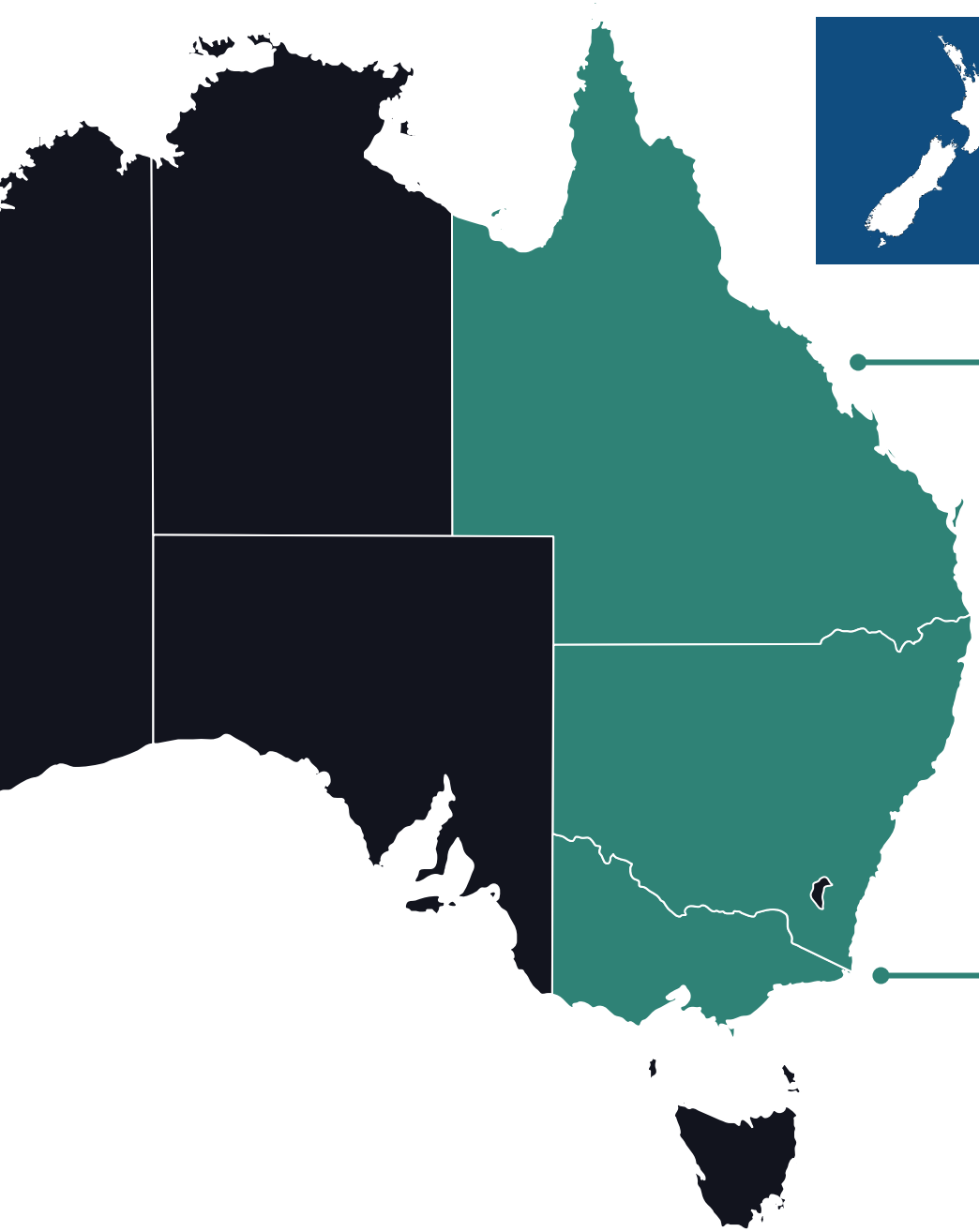
A Critical Infrastructure Cyber Risk Management Program (CIRMP) aims to uplift security practices and ensure that the entities responsible for the asset are proactive in identifying, mitigating, preventing, and responding to risks.

Under Subsection 8(4) of the *Security of Critical Infrastructure (Critical Infrastructure Cyber Risk Management Program) Rules (LIN 23/006)* the CIRMP should align with one of five acceptable frameworks, one of these being the **Australian Energy Sector Cybersecurity Program (AESCSF)** at Security Profile 1.

WHAT IS THE AUSTRALIAN ENERGY SECTOR CYBERSECURITY FRAMEWORK (AESCSF)?

The Australian Energy Sector Cyber Security Framework (AESCSF), developed by AEMO in collaboration with industry and the Australian Government, was first published in 2018.

This framework provides guidance for assessing and uplifting cybersecurity maturity across an asset within the Energy sector.



NEW ZEALAND

NETWORK INFRASTRUCTURE
MANUFACTURING
SOLAR

QUEENSLAND

MANUFACTURING
SOLAR
WIND
BESS

NEW SOUTH WALES

HYBRID (SOLAR/BESS)
SOLAR
BESS

VICTORIA

HYBRID (HYDRO/SOLAR)
GAS PROCESSING
MANUFACTURING
GAS STORAGE
SOLAR
WIND

OpusV Tech Group

Building cybersecurity resilience from the ground up.

OpusV integrates robust solutions at every stage—from asset design to operation. Our focus is on mitigating risk across diverse asset classes like solar, wind, storage, and hydro, ensuring secure environments and proactive threat management.

Encompassing over a dozen greenfield and brownfield projects, we deliver scalable, government-compliant solutions that provide security and reliability to your assets.

SOCI Compliance and the Australian Energy Sector Cyber Security Framework (AESCSF)

The Security of Critical Infrastructure Act (SOCI) aims to ensure the nation's critical assets are safeguarded from risks, including cyber-related risks. Part 2A of the SOCI Act requires that an assets responsible entity is to create and enforce a Critical Infrastructure Risk Management Plan (CIRMP) which allows for appropriate management of risks relating to the asset.

An acceptable CIRMP establishment requires the selection of one of five frameworks detailed in the SOCI (CIRMP) Rules (LIN 23/006). Based OpusV's experience in the industry, past consulting engagements and the endorsement from the Australian Cyber Security Centre (ACSC), we have closely aligned our solutions and designs with the Australian Energy Sector Cyber Security Framework (AESCSF). OpusV has assisted many of our partners in reaching AESCSF SP-1, and our experience with the framework allows OpusV to confidently assess compliance at any stage of an asset's lifecycle.

How OpusV Delivers Cybersecurity and Compliance

OpusV categorises its service offerings into four main pillars, each crafted to provide value and meet compliance requirements for AESCSF.

Cybersecurity Consulting

OpusV combines Technology, Cybersecurity and OT expertise obtained through real-world experience building and securing energy assets to ensure you are protected from cyber threats and are on the fastest path to SOCI/ AESCSF compliance.

- Solution Architecture Design
- Asset Discovery
- Cyber Risk Assessment
- Project Management and Delivery
- AESCSF Compliance Audit
- AESCSF Compliance Consulting
- Governance, Compliance and Technical Documentation
- Incident Response Consulting

Technology and Cybersecurity Solutions

Implement scalable technology and cybersecurity solutions using our subject matter experts and engineers to ensure sound power generation and uplift your resilience against cyber threats.

- Identity and Access Management
- Security Incident and Event Management
- Core Technology Infrastructure
- Business Continuity Systems
- Network Security
- Continuous Asset Visibility and Vulnerability Scanner
- End-Point Security and Anti-Malware
- OT Configuration Analyser

Cybersecurity Operations, Threat and Vulnerability Management Services

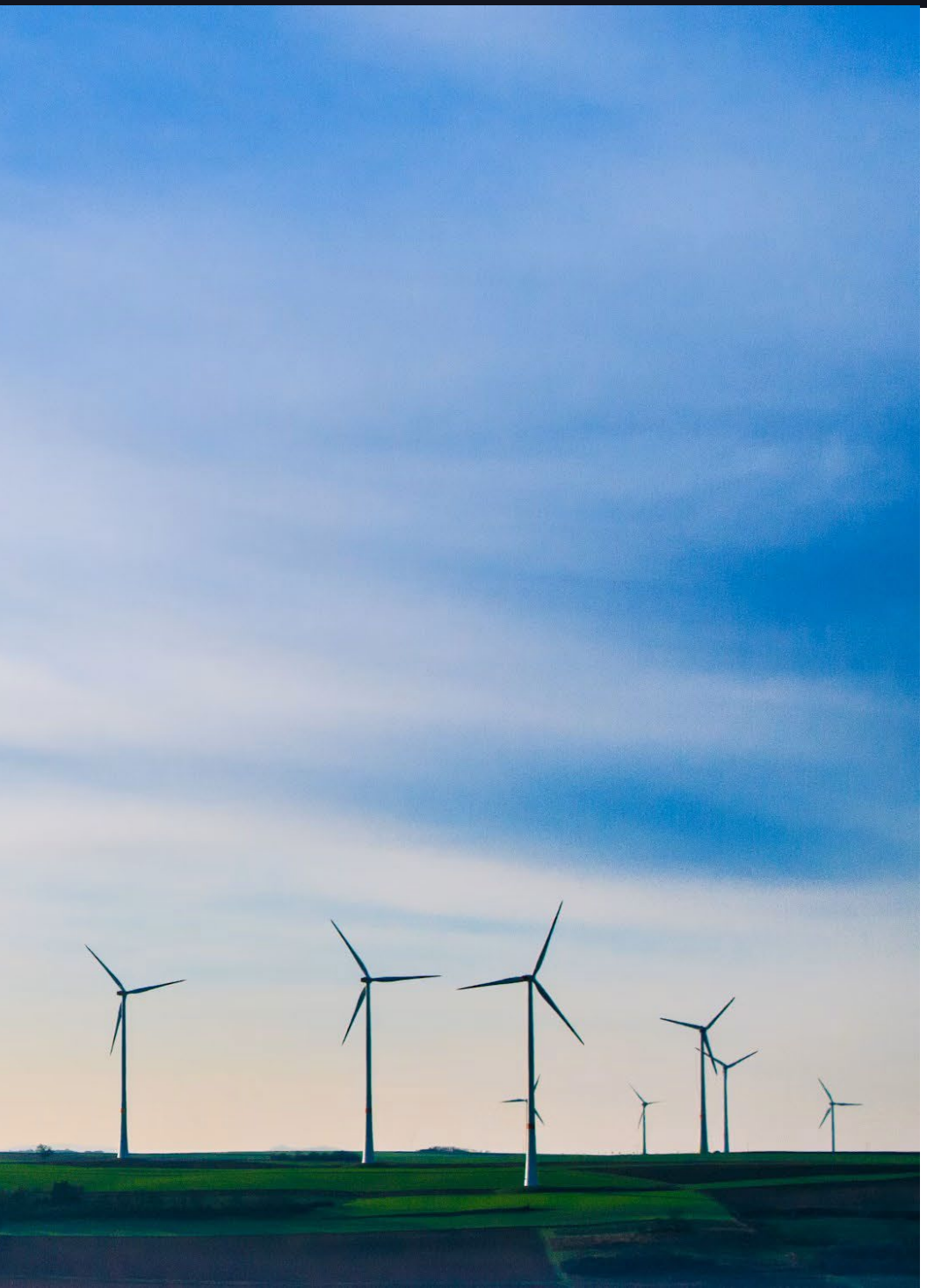
We support your cybersecurity journey throughout the lifecycle of your plant, with a focus on adherence to legislative requirements.

- Cyber Threat Intelligence
- Manage Threat Hunting
- 24/7 Management Detection, Hunting and Response (MDR)
- Asset Discovery and Vulnerability Management
- SIEM Log Management
- Managed Network and Endpoint Security

Technology Operations and Maintenance Services

OpusV partners with world-class providers to ensure the ongoing management, monitoring, and protection of your generating assets against cyber threats.

- Infrastructure Management and Network Engineering
- Operational Transformation
- Backup Integrity Assurance
- IT Business Continuity Testing
- System, Software and User Support
- Network and System Monitoring



CYBERSECURITY CONSULTING

Solution Architecture and Design
OpusV have extensive experience in integrating OT systems and environments such as RTACs, PLCs, SCAD and HMI with cybersecurity and IT solutions. Our experienced architects will design a secure and defensible, AESCSF-compliant network to protect your energy assets and ensure uninterrupted power generation.

Asset Discovery
Engage our experts to conduct an on-site physical and digital asset discovery, a crucial step in achieving AESCSF compliance.

Cyber Risk Assessment
Identify key cyber risks through our extensive on-site and digital cyber risk assessment engagement. Essential for efficient delivery of OpusV services, and meeting AESCSF compliance standards.

Project Management and Delivery
Leverage our leading industry experience for the efficient planning, execution, and completion of AESCSF aligned cybersecurity projects and deliverables throughout all phases of the lifecycle of your plant, including commissioning, energisation and hold-point testing.

AESCSF Compliance Audit
OpusV conducts an initial audit of your energy asset to determine the maturity alignment to AESCSF practices.

AESCSF Compliance Consulting
OpusV helps plan, manage, and oversee your organisation's AESCSF cybersecurity compliance. We identify the required security profile (SP1, SP2, or SP3) and coordinate the necessary solutions, services, and policies to meet the requirements.

Governance, Compliance and Technical Documentation
This service supports governance and compliance activities where policies, processes and technical documentation are required to be delivered for a specific project.

Incident Response Consulting
OpusV's cybersecurity experts support your organisation's Cyber Incident Response at every stage. From planning and exercises to technical help during an incident, we're here to assist.

TECHNOLOGY AND CYBERSECURITY SOLUTIONS

Identity and Access Management (IXID, Group Policy, RBAC, Identity Management)
Integrate our solutions to manage identities and access for all stakeholders during the build, deployment, and operation phases across IT and OT systems. OpusV secures access to your power assets with systems like our custom-built identity and access management system, IXID, designed specifically for the power industry.

Security Incident and Event Management (SIEM)
OpusV deploys a solution that provides real-time analysis of security alerts generated by applications and network hardware, offering comprehensive visibility, threat detection, incident response, and compliance management to enhance an organisation's security posture.

Core Technology Infrastructure (Network and Server Infrastructure)
OpusV deploys our core virtual and physical infrastructure to support the functional requirements of the assets and is the cornerstone platform where critical systems operate.

Business Continuity Systems (Backups, Redundancy and High Availability)
OpusV deploys business continuity solution to ensure your assets remain operational during and after disruptive events. Our solutions ensure safeguarding critical processes and data to minimise downtime and maintain seamless business operations.

Network Security (NextGen, Firewalls, IDS/IPS, DLP, Segmentation)
Our Network Security service provides comprehensive protection for your asset through our implementation of Palo Alto Next Gen Firewalls (NGFW), advanced threat protection, secure infrastructure, and intrusion detection systems.

Continuous Asset Visibility and Vulnerability Scanner
OpusV partners with Tenable OT's security offering to deploy advanced capabilities for continual asset visibility, vulnerability scanning and network security across your OT environment.

End-Point Security and Anti-Malware
OpusV partners with Microsoft and other leading security providers to deploy advanced threat protection and visibility against cyber threats and malware across applicable systems throughout your energy assets.

OT Configuration Analyser
Audit and test your OT devices at scale using OpusV's purpose-built Industrial systems configuration analyser, ensuring quality control and security across your environment.





CYBERSECURITY OPERATIONS, THREAT AND VULNERABILITY MANAGEMENT SERVICES

Cyber Threat Intelligence
Cyber Threat Intelligence offers proactive insights into potential and active cyber threats targeting an organisation. This service involves collecting, analysing, and interpreting data to identify threats, evaluate their relevance and impact, and recommend suitable mitigation strategies.

Managed Threat Hunting
An-add on to our *Cyber Threat Intelligence* service, Managed Threat Hunting proactively hunts for malicious adversary activities in your asset.

24/7 Managed Detection, Hunting and Response (MDR)
OpusV's premium 24/7 threat management service provides continuous monitoring, threat detection, and rapid response to cyber incidents. This service leverages advanced analytics, threat intelligence, our deployed solutions and expert security teams to identify and mitigate threats in real-time, ensuring robust protection, minimising the impact of security breaches.

Continuous Asset Discovery and Vulnerability Management
OpusV utilises our *Continuous Asset Visibility and Vulnerability Scanner* technology to proactively identify, assess, and manage the remediation of security vulnerabilities within an asset's IT and OT environment.

SIEM Log Management
OpusV's professional services ensure the right level of logging is configured and collected to ensure visibility across the environment.

Managed Network and Endpoint Security
Our managed service handles threat policies, updates, and client requests for network and endpoint security, including anti-malware, firewalls, intrusion detection/prevention, proxies, and web application firewalls.

TECHNOLOGY OPERATIONS AND MAINTENANCE SERVICES

System, Software and User Support
Our foundational Technology Operations and Maintenance support service that ensures we support the assets users and system requirements.

Infrastructure Management and Network Engineering
An add-on to our *System, Software and User Support service*, OpusV manages and maintains our *Core Technology* and *Business Continuity Systems* solutions to ensure the availability and integrity of your plant operations.

Network and System Monitoring
An add-on to our *System, Software and User Support service*, OpusV provides management and monitoring services that enables your energy assets systems and network to run optimally. We utilise CheckMK and Observium to proactively identify and resolve issues and risks reducing the likelihood of service impacts.

Backup Integrity Assurance
An add-on to our *System, Software and User Support service*, OpusV continuously monitor for the integrity of your back-up solutions.

Operational Transformation
Our *Operational Transformation* service involves rethinking and enhancing asset processes to align more effectively with the evolving demands and expectations of the ever-changing digital landscape.

IT Business Continuity Testing
OpusV supports your asset's Business Continuity Plan and Disaster Recovery through backup and recovery testing of our *Business Continuity Systems*, as well as documented processes.



Mapping OpusV Capabilities to AESCSF Domains

OpusV crafts a detailed plan to address areas falling short of SP-1 requirements, focusing on robust cybersecurity practices to ensure AESCSF compliance. This approach results in a comprehensive and tailored cybersecurity strategy, reducing the likelihood and severity of long-term cyber risks. Below is a summary of each AESCSF domain, along with OpusV capabilities that can help organisations improve their maturity levels in each domain.

AESCSF DOMAIN	AESCSF DOMAIN DESCRIPTION	OPUSV CAPABILITY	SOLUTION/SERVICE
RISK MANAGEMENT (RM)	Establish, operate, and maintain an enterprise cyber security Cyber Risk Management program to identify, analyse, and mitigate cyber security risk to the organisation, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.	Cybersecurity Consulting	Cyber Risk Assessment
CYBERSECURITY PROGRAM MANAGEMENT (CPM)	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organisation's cybersecurity activities in a manner that aligns cybersecurity objectives with the organisation's strategic objectives and the risk to critical infrastructure.	Cybersecurity Consulting	AESCSF Compliance Audit
			Solution Architecture and Design
			Project Management and Delivery
			AESCSF Compliance Consulting
ASSET, CHANGE, AND CONFIGURATION MANAGEMENT (ACM)	Manage the organisation's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organisational objectives.	Cybersecurity Consulting	Asset Discovery
		Technology and Cybersecurity Solutions	Continuous Asset Visibility and Vulnerability Scanner
IDENTIFY AND ACCESS MANAGEMENT (IAM)	Create and manage identities for entities that may be granted logical or physical access to the organisation's assets. Control access to the organisation's assets, commensurate with the risk to critical infrastructure and organisation objectives.	Cybersecurity Consulting	Solution Architecture and Design
		Technology and Cybersecurity Solutions	Identity and Access Management

AESCSF DOMAIN	AESCSF DOMAIN DESCRIPTION	OPUSV CAPABILITY	SOLUTION/SERVICE
INFORMATION SHARING AND COMMUNICATIONS (ISC)	Establish and maintain relationships with internal and external entities to collect and provide cyber security information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organisational objectives.	Cybersecurity Consulting	AESCSF Compliance Consulting
		Cybersecurity Operations, Threat and Vulnerability Management Services	Cyber Threat Intelligence
SUPPLY CHAIN AND EXTERNAL DEPENDENCIES MANAGEMENT (EDM)	Establish and maintain controls to manage the cyber security risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organisational objectives.	Cybersecurity Consulting	Cyber Risk Assessment
			Solution Architecture and Design
			AESCSF Compliance Consulting
		Technology and Cybersecurity Solutions	Identity and Access Management
THREAT AND VULNERABILITY MANAGEMENT (TVM)	Establish and maintain plans, procedures, and technologies to detect, identify, analyse, manage, and respond to cyber security threats and vulnerabilities, commensurate with the organisation's infrastructure (e.g., critical, IT, operational) and organisational objectives.	Technology and Cybersecurity Solutions	End-Point Security and Anti-Malware
			Network Security
			Continuous Asset Visibility and Vulnerability Scanner
			Security Incident and Event Management (SIEM)
		Cybersecurity Operations, Threat and Vulnerability Management Services	Managed Threat Hunting
			24/7 Managed Detection, Hunting and Response (MDR)
			Asset Discovery and Vulnerability Management
			Cyber Threat Intelligence

AESCSF DOMAIN	AESCSF DOMAIN DESCRIPTION	OPUSV CAPABILITY	SOLUTION/SERVICE
AUSTRALIAN PRIVACY MANAGEMENT (APM)	Establish and maintain plans, procedures, and technologies to reduce privacy related risks, and manage personally identifiable information through its lifecycle - collection, storage, use and disclosure, and disposal (including de-identification).	Cybersecurity Consulting	Cyber Risk Assessment
			Solution Architecture and Design
			AESCSF Compliance Consulting
		Technology and Cybersecurity Solutions	Core Technology Infrastructure
			Network Security
		Technology Operations and Maintenance Services	Information Systems and Network Infrastructure Management
SITUATIONAL AWARENESS (SA)	Establish and maintain activities and technologies to collect, analyse, alarm, present, and use operational and cyber security information, including status and summary information from the other model domains, to form a common operating picture (COP).	Technology and Cybersecurity Solutions	Security Incident and Event Management (SIEM)
			End-Point Security and Anti-Malware
			Network Security
			Continuous Asset Visibility and Vulnerability Scanner
		Cybersecurity Operations, Threat and Vulnerability Management Services	SIEM Log Management
			24/7 Managed Detection, Hunting and Response (MDR)
			Managed Threat Hunting
WORKFORCE MANAGEMENT (WM)	Establish and maintain plans, procedures, technologies, and controls a culture of cyber security and to ensure that ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organisational objectives.	Cybersecurity Consulting	Cyber Risk Assessment
			AESCSF Compliance Consulting

AESCSF DOMAIN	AESCSF DOMAIN DESCRIPTION	OPUSV CAPABILITY	SOLUTION/SERVICE
EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS (IR)	Establish and maintain plans, procedures, and technologies to detect, analyse, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organisational objectives.	Cybersecurity Consulting	Solution Architecture and Design
		Technology and Cybersecurity Solutions	Core technology Infrastructure
			Business Continuity Systems
			Security Incident and Event Management (SIEM)
			End-Point Security and Anti-Malware
			Network Security
			Continuous Asset Visibility and Vulnerability Scanner
		Cybersecurity Operations, Threat and Vulnerability Management Services	Managed Threat Hunting
			24/7 Managed Detection, Hunting and Response (MDR)
		Technology Operations and Maintenance Services	ICT Business Continuity Testing



Appendices

Appendix A. OpusV OT Cybersecurity Consulting Services Detail

AESCSF Maturity Assessment

OpusV conducts an audit of your energy asset to determine the maturity alignment to AESCSF practices. This consists of a physical site visit, review of documentation (policies, procedures, network diagrams, asset registers), interviewing relevant personnel as well as a site visit to obtain a full understanding of asset cyber maturity.

OpusV has created customised reporting that shows the exact maturity of clients, including recommendations which require focused investment and uplift to be considered compliant with the AESCSF practices.

AESCSF SP-1 Maturity Assessment

ID	PRACTICE	MIL	REQS MET?	FINDINGS AND COMMENTS	ACTION NEEDED TO MEET REQUIREMENTS
ACM-1A	There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc	MIL-1	Yes	An asset register was provided from asset management system, including information assets such as firewall and network rules.	N/A
ACM-1B	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	MIL-1	Yes	As per above.	N/A
ACM-2A	Configuration baselines are established, at least in an ad hoc manner, for inventoried assets where it is desirable to ensure that multiple assets are configured similarly	MIL-1	Yes	Configurations are stored, versioned, and deployed from a configuration deployment system for network gear, and documented for OT and turbine gear.	N/A
ACM-2B	Configuration baselines are used, at least in an ad hoc manner, to configure assets at deployment	MIL-1	Yes	Evidence was observed directly of configurations deployment being used from known config states.	N/A
ACM-3A	Changes to inventoried assets are evaluated, at least in an ad hoc manner, before being implemented	MIL-1	No	No evidence of change control processes or assessments being performed prior to changes being made.	Implement and enforce a Change Control Procedure.
ACM-3B	Changes to inventoried assets are logged, at least in an ad hoc manner	MIL-1	No	No evidence existed to suggest that inventoried assets are logged.	Implement and enforce a Change Control Procedure.
ACM-3C	Changes to assets are tested prior to being deployed, whenever possible	MIL-2	No	No evidence existed to suggest that testing is done prior to deployment.	Implement and enforce a Change Control Procedure.
APM-1A	Privacy requirements applicable to the organisation have been identified, even in an ad-hoc manner.	MIL-1	Yes	Privacy Policy was provided upon request.	N/A
APM-1B	The organisation has defined what it considers personal information in the context of its business activities, even in an ad-hoc manner.	MIL-1	Yes	As per Privacy Policy supplied.	N/A
APM-1C	There is a point of contact (person or role) to whom privacy issues could be reported, even in an ad-hoc manner.	MIL-1	Yes	As per Privacy Policy supplied.	N/A
APM-1D	Business activities which involve the collection, processing, storage or transmission of personal information have been identified	MIL-2	No	Although a Privacy Policy exists, it does not clearly state which activities collect, process, store or transmit personal data, nor what personal data may be collected.	Update Privacy Policy to ensure that it is clearly stated what data may be collected and how it is used.
APM-AP1	The function is unaware whether personal information is collected	MIL-2	Present	See APM-1D for more information.	See APM-1D for more information.
			SP1 COMPLIANT PRACTICES	7	ANTI PATTERNS PRESENT 1

Figure 1 Sample Detailed Assessment

DOMAIN	PRACTICES IN SECTION	NO OF REQS MET	ANTI PATTERNS PRESENT	COMPLIANCE PERCENTAGE
ACM	12	7	1	58%
CPM	6	5	0	83%
EDM	4	2	0	50%
IAM	13	8	2	62%
IR	19	13	1	68%
ISC	3	3	0	100%
RM	5	3	0	60%
SA	9	5	1	56%
TVM	9	1	1	11%
WM	8	2	0	25%
Total	88	49	6	56%

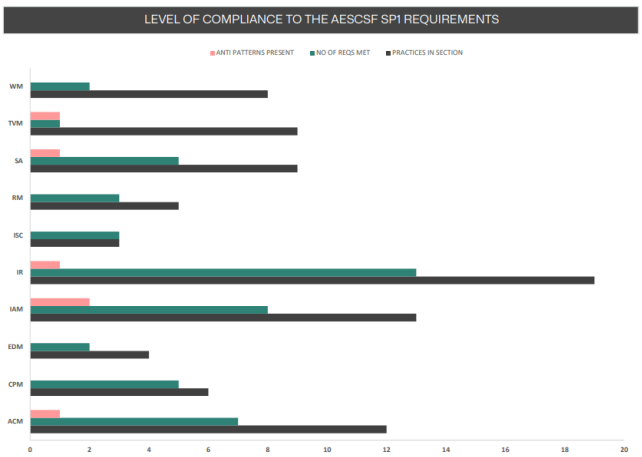




Figure 2 Sample Report Maturity Assessment

Solution Architecture and Design

OpusV's Solution Architecture and Design offering is available both as a standalone offering or in lieu post an *AESCSF Maturity Assessment* is conducted. OpusV recognises the importance of a sound architecture and design that meets the requirements and addresses the gaps and deficiencies outlined in the assessment.

This service can address AESCSF CPM-3A,3C,3D (Establish and Maintain Cyber Security Architecture) which establishes a Cyber Security architecture for your energy asset, but also is foundational to various other AESCSF domains that require technology and control implementation.

Below is our current Architecture and Design Process:



Project Management and Delivery

OpusV supports delivery of AESCSF aligned solutions and services through our Project Management and Delivery capabilities. Our project team will be engaged throughout the project and program of work from the initial engagement through to completion.

Asset Discovery

OpusV conducts a comprehensive physical asset discovery on-the site. All our staff are certified for site visits and understand how powerplants operate. An asset discovery underpins and supports efficient delivery of other OpusV services and solution offerings, and a requirement of AESCSF compliance.

Perform remote scan of network, identify any devices which are not listed on asset register, if no asset register exists, asset register is created.

If requested, visit site to perform physical inspection and capture any assets that either were not discoverable from a remote scan, or not enough detail was able to be captured.

Appendix B. OpusV Technology and Cybersecurity Solutions Detail

Identity and Access Management (IXID)

IXID is OpusV's purpose-built solution for managing identities and access to sites in a secure and integrated manner. It provides your organisation solution that centralises access control across multiple sites and multiple vendors – meaning employees, contractors and OEM providers can use a single company login (or "user identity") for all devices at those locations. Federated authentication and authorisation requests are channelled through IXID's network backend, keeping the sensitive process and identity data safe even if a local device is compromised.

IXID Features

- User Administration
- Onboarding and Offboarding processes
- Multi-Factor Authentication Setup
- Access management
    - Granular Access Control - Site, Subnet, and Device
    - Group Based Access Controls
    - Time Based Access Controls
    - Conditional Access Controls
- Logging and Access Dashboards

Current Integrations

- RADIUS
- TACACS+
- Active Directory/LDAP
- SCADA
- OT Switches
- RTAC Systems
- Additional integrations available if required.

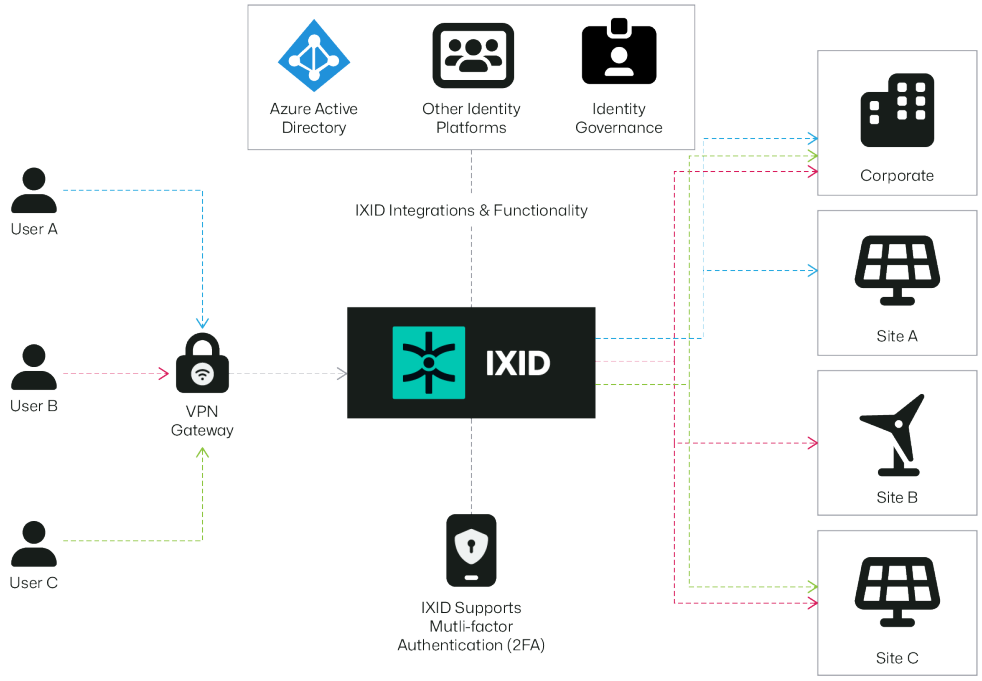


Figure 3 IXID Functional Diagram

Security Incident and Event Management (SIEM)

The SIEM (Security, Information and Event Management) platform serves as a centralised hub for aggregating log data, events, and security alerts. It enables real-time security monitoring as well as providing comprehensive visibility into the IT landscape. This assists us with the timely detection and response to cyber threats, facilitates compliance auditing, and enhances security reporting.

OpusV currently utilises a hybrid architecture which utilises *Wazuh* and *Microsoft Sentinel* for log storage and threat detection. Below is a typical SIEM architecture.

This solution coincides with OpusV's *Log Management and Log-onboarding service* to deliver a wholistic solution.

Solutions Services Dependant on SIEM deployment

- Managed Threat Hunting
- Managed Detection and Response
- Threat Detection Engineering

Core Technology Infrastructure (Network and Systems)

OpusV's core technology infrastructure encompasses the essential hardware, software, network resources, and services required for the operation and management of your energy asset. This includes:

- **Server Infrastructure:** Virtualised Infrastructure to run systems required for plant function
- **Network Infrastructure**: Routers, switches, firewalls, and other networking equipment that facilitate communication and data exchange across local area networks (LANs), wide area networks (WANs), and the internet.
- **Storage Systems**: Solutions for data storage, including databases, storage area networks (SANs), network-attached storage (NAS), and cloud storage, ensuring data is accessible, secure, and backed up.
- **Operating Systems and OT Environment**: Software that manages hardware resources and provides common services for applications, including Windows, Linux, and OT platforms like SCADA, Historian and RTAC.
- **Security Infrastructure**: OpusV utilises core infrastructure to host and support its cybersecurity technology tech stack, such as SIEM, intrusion detection systems (IDS), intrusion prevention systems (IPS), OT Vulnerability scanners, antivirus software etc.
- **Backup and Disaster Recovery**: OpusV utilises Veeam technologies for data backup, recovery, and business continuity in case of data loss or system failure.
- **Monitoring and Management Tools**: OpusV utilises CheckMK and Observium to oversee the performance, security, and health of the technology environment, including network monitoring, system management, and alerting tools.

Together, these components ensure that OpusV infrastructure is robust, scalable, and secure, supporting its business operations and enabling efficient data and resource management.

Server Hardware Specifications

Currently, the deployed servers to client sites consist of two Xeon servers, with hardware sourced from SuperMicro, Lenovo or Cisco's server range (depending on budget and risk appetite) with the following specifications:

Option A: SuperMicro Industrial Servers

Low-cost additional stack where budget and dependency on controls is lower

Option B: Lenovo Rackmount Business Server

Mid-range option where redundancy is required for control purposes (IAM dependency normally), but not specifically running control software.

Option C: Cisco UCS Rackmount Servers

Cisco Solution will be quoted to specification as requested. This is OpusV's standard design vendor when control and SCADA servers and applications co-exist with the cybersecurity stack.

Storage Hardware

There are two devices associated with storage: a Shared Storage NAS for running virtual compute, and a Nearline Backup NAS to protect site assets and security infrastructure assets.

Network Hardware

Network equipment will vary depending on site. At minimum a Cisco switch will be deployed for deployed infrastructure connectivity and to provide uplink to plant infrastructure. When edge routers are required to be replaced due to a lack in feature or functionality, it is replaced with a Cisco Router.

Where possible, two of each model of network equipment is installed to provide High Availability and Failover functions.

System Monitoring

CheckMK monitors both physical and virtual servers, primarily to detect and notify of any outages or issues. If a server goes down, an automated alert is generated and sent to the critical queue for immediate attention. When CheckMK identifies a potential issue, a warning notice is issued and sent to the queue for review.

Network Monitoring

OpusV uses Observium to monitor network devices and assets. Observium is a network monitoring and management platform that provides real-time status updates on network health and performance, along with historical data. It can automatically discover devices and services, collect performance metrics, and generate alerts when issues are detected.