INDUSTRIAL DEFENDER®

Australian Energy Sector Cybersecurity Framework (AESCSF)

Mapping Guide

READ NOW ➤

TIP

Click orange rectangles in table to see details for each domain

What is the AESCSF?

The Australian Energy Sector Cybersecurity Framework (AESCSF) is a set of cybersecurity guidelines designed to enable owners and operators of energy infrastructure in Australia to assess, evaluate, prioritise, and improve their cybersecurity posture. The AESCSF was released in 2018 by the Australian Energy Market Operator (AEMO) and is tailored to the unique cybersecurity requirements of the energy sector.

The AESCSF is closely aligned with many other industry standards for OT security, like the NIST Cybersecurity Framework and the Cybersecurity Capability Maturity Model (C2M2). As such, it serves as a broadly relevant example of a top-notch OT security model that is worth looking at regardless of your location or industry. Let's dive into how Industrial Defender helps you align with every domain in this model.

DOMAIN 1

Asset, Change and Configuration Management (ACM)

DOMAIN 2

Cybersecurity Program Management (CPM)

DOMAIN 3

Supply Chain and External Dependencies Management (EDM)

DOMAIN 4

Identity and Access Management (IAM)

DOMAIN 5

Event and Incident Response, Continuity of Operations (IR)

DOMAIN 6

Information Sharing and Communications (ISC)

DOMAIN 7

Risk Management (RM)

DOMAIN 8

Situational Awareness (SA)

DOMAIN 9

Threat and Vulnerability Management (TVM)

DOMAIN 10

Workforce Management (WM)

DOMAIN 11

Australian Privacy Management (APM)

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Domain 1: Asset, Change and Configuration Management (ACM)

Manage the organisation's operational technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organisational objectives.

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
ACM-1: Manage Asset Inventory	• There is an inventory of OT and IT assets important to the delivery of the function • Inventoried assets are prioritised based on their importance to the delivery of the function • The asset inventory is current (as defined by the organisation)	• Industrial Defender provides inventory of assets using both active and passive methods, as well as manual entry of data for network islands or other technical barriers. • Industrial Defender provides a built-in set of administrative properties for all assets and an ability to extend it as needed for additional dimensions of classification. • Industrial Defender provides visibility into asset functions based on all available data, includes software inventory, running services, network ports in use, traffic flow, as well as manual designations by a user.	• ACM-1A • ACM-1B • ACM-1C • ACM-1D • ACM-1E • ACM-1F
ACM-2: Manage Asset Configuration	• Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly, as well as to configure assets at deployment • The design of configuration baselines includes cybersecurity objectives • Configuration of assets are monitored for consistency with baselines throughout the assets' life cycle • Configuration baselines are reviewed and updated at an organisationally- defined frequency	• Industrial Defender manages the full spectrum of asset information, including software, patches, users, ports, services, network configuration, firmware, and a myriad of other details. Collected information and supported asset types are easily extended to accommodate evolving use cases. • Industrial Defender provides comprehensive baseline management with views into actual values, baselines, and deviations between them over time. Baselines are maintained for each asset but can be viewed and managed in bulk where there should be uniformity in groups of assets. • Industrial Defender enforces periodic baseline reviews and deviation handling as elements of the risk score for every asset. • Industrial Defender provides security roles to enforce an asset group and user group matrix of views and allowable configuration operations.	• ACM-2A • ACM-2B • ACM-2C • ACM-2D • ACM-2E
ACM-3: Manage Changes to Assets	• Changes to inventoried assets are evaluated and logged before being implemented • Changes to assets are tested prior to being deployed, whenever possible • Change management practices address the full life cycle of assets • Changes to assets are tested for cybersecurity impact prior to being deployed • Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)	• Industrial Defender provides strong support for detecting and logging changes to assets in software, patches, firmware, ports, users, among other elements, with inherent flexibility to augment measured characteristics as needed. • Industrial Defender supports architectures with QA or development environments to test asset changes prior to deployment in production. Baselines can be migrated between systems to isolate and expose unexpected changes between environments. • Industrial Defender provides a policy mechanism to measure compliance of assets to an organization's cybersecurity requirements. Policies can be used for change validation or detecting unexpected policy violations. • Industrial Defender provides a multi-tiered baseline approval process to reflect authorization and documentation requirements of change management procedures and subsequent audits.	• ACM-3A • ACM-3B • ACM-3C • ACM-3D • ACM-3E • ACM-3F

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Domain 2: 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.

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
CPM-1: Establish Cybersecurity Program Strategy	• The organisation has a cybersecurity program strategy • The strategy defines objectives for the organisation's cybersecurity activities • The strategy and priorities are documented and aligned with the organisation's strategic objectives and risk to critical infrastructure • The strategy defines the organisation's approach to provide program oversight and governance for cybersecurity activities • The strategy defines the structure and organisation of the cybersecurity program	• Industrial Defender provides a broad range of features supporting a cyber security program. Recognising that a comprehensive cyber security program will likely include a collection of such tools, ID also provides a comprehensive API for integration with them. • Industrial Defender provides a comprehensive asset classification mechanism and risk scoring system. Objectively identifying critical assets and their risk level is a key element of resource allocation to implement any strategy.	• CPM-1B • CPM-1C • CPM-1D
CPM-2: Sponsor Cybersecurity Program	• Resources are provided to establish and operate a cybersecurity program aligned with the strategy • Senior management actively and visibly sponsors the program • The development and maintenance of cybersecurity policies is sponsored • Program responsibility is assigned to a role with requisite authority • Program performance is monitored to ensure alignment with the strategy • The program is independently reviewed for achievement of objectives • The program addresses and enables regulatory compliance as necessary • The program monitors and/or participates in selected industry standards or initiatives	• Industrial Defender is a foundational component for a cyber security program. • Industrial Defender provides real-time operational capabilities suitable for implementing a comprehensive cyber security program. • Industrial Defender provides historical data views suitable for analysis and review for the purpose of refining the cyber security program, as well as satisfying audits of compliance to common standards such as AESCSF, NERC CIP, NIST, or others. • Industrial Defender provides high level dashboard views, a rich set of reports, and an API for custom reports and integration with other visualization systems. Data is available for continuous monitoring and program improvement.	• CPM-2A • CPM-2C • CPM-2D • CPM-2I • CPM-2K

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
CPM-3: Establish and Maintain Cybersecurity Architecture	• A strategy to architecturally isolate the organisation's IT systems from OT systems is implemented • A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy • Architectural segmentation and isolation is maintained according to a documented plan • cybersecurity architecture is updated at an organisation-defined frequency to keep it current	• Industrial Defender utilizes secure communication methods to support placement of its components consistent with the target system architecture. Existing segmentation and isolation of networks is maintained. • Industrial Defender provides robust and secure management of credentials used to remotely access devices where local agents are not utilized. • Industrial Defender security and user roles limit data views to appropriate personnel.	• CPM-3A • CPM-3B • CPM-3C • CPM-3D
CPM-4: Perform Secure Software Development	• Software to be deployed on assets important to the delivery of the function is developed using secure software development practices • Policies require that software that is to be deployed on assets that are important to the delivery of the function be developed using secure software development practices	• All Industrial Defender components are produced in a mature agile development environment employing a robust testing and quality assurance program. Appliances are hardened and deployed with only necessary software and services in use. • All product releases are scanned using Veracode for malware and other vulnerabilities, as well as standard anti-virus scans for all deliverable software. Full port scans of all appliances validate the presence of necessary network access points and no others. • All deliverables are digitally signed to maintain integrity. • Industrial Defender functions on a best-method-available principle of data collection. Depending on customer and vendor risk tolerance, monitoring methods range from host-based agents to passive monitoring, to manual data entry. Each asset can be monitored using the most appropriate technology.	• CPM-4A • CPM-4B

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Domain 3: Supply Chain and External Dependencies Management (EDM)

Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with risk to critical infrastructure and organisational objectives.

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
EDM-1: Identify Dependencies	• Important IT and OT supplier dependencies are identified • Important customer dependencies are identified • Supplier dependencies are identified according to established criteria • Customer dependencies are identified according to established criteria • Single-source and other essential dependencies are identified • Dependencies are prioritised • Dependency prioritisation and identification are based on the organisation's risk criteria	• Industrial Defender collects asset software inventory and firmware information. Views by vendor may be used to assess and track dependencies. • Industrial Defender through its partnership with FoxGuard provides visibility to supplier software and patch availability, applicability and authenticity.	• EDM-1A • EDM-1C • EDM-1E • EDM-1G
EDM-2: Manage Dependency Risk	• Cybersecurity risks due to suppliers and other third-party dependencies are identified and addressed • Cybersecurity requirements are considered when establishing relationships with third parties • Identified cybersecurity dependency risks are entered into the risk register • Contracts and agreements with third parties incorporate sharing of cybersecurity threat information • Cybersecurity requirements are established for third parties according to a defined practice • Agreements with third parties include cybersecurity requirements • Selection of third parties includes consideration of their ability to meet cybersecurity requirements • Agreements with third parties require notification of cybersecurity incidents related to the product or service • Third parties are periodically reviewed for their ability to meet the cybersecurity requirements • Cybersecurity risks due to external dependencies are managed based on to the organisation's risk management criteria and process • Cybersecurity requirements are established for supplier dependencies based on risk criteria • Agreements with suppliers require notification of vulnerability-inducing product defects throughout the lifecycle of delivered products • Acceptance testing of procured assets includes testing for cybersecurity requirements • Information sources are monitored to identify and avoid supply chain threats	• Industrial Defender monitors logs across all asset types for authorized and unauthorized user access. Unusual correlations of activity will produce escalated events for real-time notification. • Industrial Defender inventories user accounts are inventoried as part of the baselining process. Detection of new accounts as well as validation of removal or disabling of accounts is a core feature. • Industrial Defender vulnerability and patch management capabilities identify known vulnerabilities and available patches available from OT vendors. • Industrial Defender inventories all software, firmware and hardware including custom vendor software installed in non-typical ways (files, executables, DLLs). This inventory information is critical when reviewing supplier vulnerability and defect information.	• EDM-2A • EDM-2B • EDM-2J • EDM-2L

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Domain 4: Identity and Access Management (IAM)

IAM entails creating and managing 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.

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
IAM-1: Establish and Maintain Identities	• Identities are provisioned and credentials issued for personnel and entities requiring access to assets • Identities are deprovisioned when no longer required • Identities are periodically reviewed and updated to ensure validity • Credentials are periodically reviewed to ensure that they are associated with the correct person or entity • Identities are deprovisioned within organisationally defined time thresholds when no longer required • Credential requirements are informed by the organisation's risk criteria	• Industrial Defender monitors authentication activity to support validation of compliance to cybersecurity policies. • Industrial Defender collects configuration of users for assets and applications. Deviations from or conformance to policy regarding (de) provisioning of identities can be obtained across all assets. • Industrial Defender collects configuration of password and account policies such as minimum password length and maximum password age. Deviations from security policies can be identified or conformance validated.	• IAM-1A • IAM-1B • IAM-1C • IAM-1D • IAM-1E • IAM-1F • IAM-1G
IAM-2: Control Access	• Access requirements are determined • Access is granted to identities based on requirements • Access is revoked when no longer required • Access requirements include least privilege and separation of duties principles • Access requests are reviewed and approved by the asset owner • Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny • Access privileges are reviewed and updated to ensure validity at an organisationally defined frequency • Access to assets is granted by the asset owner based on risk • Anomalous access attempts are monitored as indicators of cybersecurity events	• Industrial Defender solution components use role-based and asset-based access controls to enforce principles of least privilege and separation of duties. • Industrial Defender maintains asset owner name and contact information for review and management of access requests. • Industrial Defender monitors authentication activity for anomalous activity and generates escalated events. • Industrial Defender collects configurations of users for assets and applications for review of account status, usage, and privilege level.	• IAM-2A • IAM-2B • IAM-2C • IAM-2D • IAM-2F • IAM-2G • IAM-2I

Domain 5: 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.

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
IR-1: Detect Cybersecurity Events	• There is a point of contact to whom cybersecurity events are reported • Detected cybersecurity events are logged, tracked, and reported • Criteria are established for cybersecurity event detection • There is a repository where cybersecurity events are logged based on the established criteria • Event information is correlated to support incident analysis by identifying patterns, trends, and other common features • Cybersecurity event detection activities are adjusted based on the organisation's risk register and threat profile to help detect known threats and monitor for identified risks • The common operating picture for the function is monitored to support the identification of cybersecurity events	• Industrial Defender vulnerability monitoring identifies known vulnerabilities in software, firmware, and operating systems. • Industrial Defender administrative properties contain point of contact information for each asset along with owner organization, physical location, and criticality level. • Industrial Defender monitors OT and IT systems for cyber events using the best mechanisms allowed, from host-based agents to remote log monitoring to passive monitoring of network traffic. • Industrial Defender normalizes event streams from all assets into a rich categorization and prioritization scheme suitable for filtering and analysis. • Industrial Defender provides event notification mechanisms including email, an API, and syslog integration points to other organizational entities. • Industrial Defender correlation engine provides means to detect patterns across assets for escalation events. • Industrial Defender asset baseline system quickly identifies changes in configuration, firmware, or software inventory for assets as well as deviations from baselines for the same. • Industrial Defender policies quickly identify deviations from established cyber security policy settings. • Industrial Defender supports external integration to other entities and applications with APIs, database views, asynchronous events via email, and scheduled reports. • Industrial Defender supports external integration to other entities and applications with APIs, database views, e-mails, alerts, e-mails and custom reporting. • Industrial Defender has a Risk Framework which applies a risk-based analysis of events and asset information. • Industrial Defender has customized integrations for data sharing SIEM systems providing deep OT asset context for analysts. • Industrial Defender employs both rule-based and machine learning-based threat detection methods.	• IR-1A • IR-1B • IR-1C • IR-1D • IR-1E • IR-1F • IR-1G • IR-1H

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
IR-2: Escalate Cybersecurity Events and Declare Incidents	• Criteria for cybersecurity event escalation are established, including incident declaration criteria • Cybersecurity events are analysed to support escalation and the declaration of incidents • Escalated cybersecurity events and incidents are logged and tracked • Criteria for cybersecurity event escalation, including incident criteria, are established based on the potential impact to the function • Criteria for cybersecurity event escalation, including incident declaration criteria, are updated at an organisation-defined frequency • There is a repository where escalated cybersecurity events and incidents are logged and tracked to closure • Criteria for cybersecurity event escalation, including incident declaration criteria, are adjusted according to the organisation's risk register and threat profile • Escalated cybersecurity events and declared incidents inform the function's common operating picture • Escalated cybersecurity events and declared incidents are correlated to support the discovery of patterns, trends, and other common features	• Industrial Defender maintains a review status for all events with annotation capability. Thresholds on the age of unreviewed events are also used as a risk factor for assets. • Industrial Defender monitors OT and IT systems for cyber events using the best mechanisms allowed, from host-based agents to remote log monitoring to passive monitoring of network traffic. • Industrial Defender normalizes event streams from all assets into a rich categorization and prioritization scheme suitable for filtering and analysis. • Industrial Defender correlation engine provides means to detect patterns across assets for escalation events. • Industrial Defender asset baseline system quickly identifies changes in configuration, firmware, or software inventory for assets as well as deviations from baselines for the same. • Industrial Defender policies quickly identify deviations from established cyber security policy settings. • Industrial Defender supports external integration to other entities and applications with an API, via email and scheduled reports. • Industrial Defender has customized integrations for data sharing with SIEM systems providing deep OT asset context for analysts. • Industrial Defender employs both rule based and machine learning based threat detection methods. • Industrial Defender administrative properties contain point of contact information for each asset along with owner organization, physical location, and criticality level.	• IR-2A • IR-2B • IR-2C • IR-2D • IR-2E • IR-2F • IR-2G • IR-2H • IR-2I

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
IR-3: Respond to Incidents and Escalated Cybersecurity Events	• Cybersecurity event and incident response personnel are identified, and roles are assigned • Responses to escalated events and incidents are implemented to limit impact to the function and restore normal operations • Reporting of escalated events and incidents is performed • Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident life cycle • Response plans are exercised at an organisation-defined frequency • Response plans address important OT and IT assets • Response teams receive training • Root-cause analysis and lessons- learned activities are performed, and corrective actions are taken • Responses are coordinated with government entities as appropriate • Response personnel participate in joint cybersecurity exercises with other organisations • Response plans are reviewed and at an organisation-defined frequency • Response activities are coordinated with relevant external entities • Response plans are aligned with the function's risk criteria and threat profile • Policy and procedures for reporting event and incident information to authorities conform with applicable laws, regulations, and agreements • Restored assets are configured appropriately and inventory information is updated following execution of response plans	• Industrial Defender monitors OT and IT systems for cyber events using the best mechanisms allowed, from host-based agents to remote log monitoring to passive monitoring of network traffic. • Industrial Defender normalizes event streams from all assets into a rich categorization and prioritization scheme suitable for filtering and analysis. • Industrial Defender correlation engine provides means to detect patterns across assets for escalation events. • Industrial Defender asset baseline system validates restoration of assets to pre-incident configuration. • Industrial Defender policies quickly identify deviations from established cyber security policy settings. • Industrial Defender vulnerability monitoring identifies known vulnerabilities in software, firmware, and operating systems to support root-cause analysis and identify other vectors before they are exploited. • Industrial Defender supports external integration to other entities and applications with an API, asynchronous events via email, and scheduled reports. • Industrial Defender has customized integrations for data sharing with SIEM systems providing deep OT asset context for analysts. • Industrial Defender administrative properties contain point of contact information for each asset along with owner organization, physical location, and criticality level.	• IR-3C • IR-3D • IR-3F • IR-3H • IR-3K • IR-3L • IR-3O

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
IR-4: Plan for Continuity	• The activities necessary to sustain minimum operations of the function are identified • The sequence of activities necessary to return the function to normal operation is identified • Continuity plans are developed to sustain and restore operation of the function • Business impact analyses inform the development of continuity plans • Recovery time objectives and recovery point objectives are incorporated into continuity plans • Continuity plans are evaluated and exercised • Business impact analyses are periodically reviewed and updated • Recovery time objectives and recovery point objectives are aligned with the function's risk criteria • The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly • Continuity plans are periodically reviewed and updated • Restored assets are configured appropriately and inventory information is updated following execution of continuity plans	• Industrial Defender baseline management documents and tracks necessary configuration, software, and services for normal and minimal operation. • Industrial Defender event database and historical asset configuration across all managed OT and IT assets provide deep forensic insight for root-cause analysis. • Industrial Defender vulnerability monitoring identifies known vulnerabilities in software, firmware, and operating systems to support root-cause analysis and identify other vectors before they are exploited. • Industrial Defender asset baseline system validates restoration of assets to pre-incident configuration. • Industrial Defender supports external integration to other entities and applications with an API, asynchronous events via email, and scheduled reports. • Industrial Defender has customized integrations for data sharing with SIEM systems providing deep OT asset context for analysts.	• IR-4A • IR-4I • IR-4K

Domain 6: Information Sharing and Communications (ISC)

Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organisational objectives.

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
ISC-1: Share Cybersecurity Information	• Information is collected from and provided to selected individuals and/or organisations • Responsibility for cybersecurity reporting obligations are assigned to personnel and/or law enforcement • Information-sharing stakeholders are identified based on their relevance to the continued operation of the function • Information is collected from and provided to identified information- sharing stakeholders • Technical sources are identified for consulting on cyberecurity issues • Provisions are established and maintained to enable secure sharing of sensitive or classified information • Information-sharing practices address both standard operations and emergency operations • Information-sharing stakeholders are identified based on shared interest in and risk to critical infrastructure • The function or organisation participates with information sharing and analysis centres • Information-sharing requirements have been defined for the function and address timely dissemination of cybersecurity information • Procedures are in place to analyse and de-conflict received information • A network of internal and external trust relationships has been established to vet and validate information about cyber events	• Industrial Defender supports external integration to other entities and applications with an API, asynchronous events via email, and scheduled reports. • Industrial Defender has customized integrations for data sharing with SIEM systems providing deep OT asset context for analysts. • Industrial Defender administrative properties contain point of contact information for each asset along with owner organization, physical location, and criticality level. • Industrial Defender external integration points support secure and encrypted transfer of data and proper tagging as sensitive or classified information. • Industrial Defender supports granular control of integration points to manage the recipient of shared information and content.	• ISC-1A • ISC-1C • ISC-1D • ISC-1E • ISC-1F • ISC-1G • ISC-1I • ISC-1J

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Domain 7: Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyse, and mitigate cybersecurity risk to the organisation, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
RM-1: Establish a Cybersecurity Risk Management Strategy	• There is a documented cybersecurity risk management strategy • The cybersecurity risk management strategy provides an approach for risk prioritisation • Organisational risk criteria are defined and available • The cybersecurity risk management strategy is periodically updated to reflect the current threat environment • An organisation-specific risk taxonomy is documented and is used in risk management activities	• Industrial Defender management of asset types, classifications, criticality, network location, physical location, organization, owner, etc. are all input elements in a risk management strategy. • Industrial Defender calculates real-time risk factors for assets which are a dimension of prioritizing risk along with the static risk analysis of each asset.	• RM-1B • RM-1C • RM-1D • RM-1E
RM-2: Manage Cybersecurity Risk	• Cybersecurity risks are identified • Identified risks are mitigated, accepted, tolerated, or transferred • Risk assessments are performed to identify risks in accordance with the risk management strategy • Identified risks are documented • Identified risks are analysed to prioritise response activities in accordance with the cybersecurity risk management strategy • Identified risks are monitored in accordance with the cybersecurity risk management strategy • Risk analysis is informed by network (IT and/or OT) architecture • The cybersecurity risk management program defines and operates risk management policies and procedures that implement the cybersecurity risk management strategy • A current cybersecurity architecture is used to inform risk analysis • A cybersecurity risk register (a structured repository of identified risks) is used to support cybersecurity risk management activities	• Industrial Defenders vulnerability monitoring identifies known vulnerabilities in software, firmware, and operating systems. • Industrial Defender calculates real-time risk factors for assets which are a dimension of prioritizing risk along with the static risk analysis of each asset. This includes visibility to the risk mitigation process as well as custom risk scoring based upon the properties of assets that make up your network. • Industrial Defenders management of asset types, classifications, criticality, network location, physical location, organization, owner, etc. are all input elements in a risk management strategy.	• RM-2A • RM-2B • RM-2C • RM-2D • RM-2E • RM-2F • RM-2G • RM-2I • RM-2J

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Domain 8: Situational Awareness (SA)

Establish and maintain activities and technologies to collect, analyse, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP).

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
SA-1: Perform Logging	• Logging occurs for assets important to the function where possible • Logging requirements are defined for all assets important to the function • Log data are aggregated • Logging requirements are based on the risk to the function • Log data support other business and security processes	• Industrial Defender monitors OT and IT systems for cyber events using the best mechanisms allowed, from host-based agents to remote log monitoring to passive monitoring of network traffic. All events are normalized into a cohesive stream suitable for analysis and correlation of events across the environment. • Active and passive scanning methods of Industrial Defender are based on a mature library of rules from a broad range of devices, but also fully support custom additions for new devices and applications. • Industrial Defender log scanning is defined on a per-asset basis to allow maximum flexibility in detail level. • Industrial Defender includes in the event stream activity related to configuration changes of assets and configuration of ID itself.	• SA-1A • SA-1B • SA-1D • SA-1D • SA-1E
SA-2: Perform Monitoring	• Cybersecurity monitoring activities are performed • OT environments are monitored for anomalous behaviour • Monitoring and analysis requirements are defined for the function and address timely review of event data • Alerts aid in the identification of cybersecurity events • Indicators of anomalous activity have been defined and are monitored across the OT environment • Monitoring activities are aligned with the function's threat profile, requirements are based on risk • Monitoring is integrated with other business and security processes • Continuous monitoring is performed across the OT environment to identify anomalous activity • Risk register content is used to identify anomalous activity • Alerts are configured according to indicators of anomalous activity	• Industrial Defender monitors OT and IT systems for cyber events using the best mechanisms allowed, from host-based agents to remote log monitoring to passive monitoring of network traffic. All events are normalized into a cohesive stream suitable for analysis and correlation of events across the environment. • Industrial Defender monitors key performance indicators of assets related to memory, processor capacity, storage, and network activity to detect anomalous behaviour. • Industrial Defender monitors removable media activity. • Industrial Defender provides an event review system with annotation capability. Thresholds on the age of unreviewed events are used as a risk factor for assets.	• SA-2A • SA-2B • SA-2C • SA-2D • SA-2E • SA-2F • SA-2G • SA-2H • SA-2I • SA-2J • SA-2K

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
SA-3: Establish & Maintain a Common Operating Picture (COP)	• Methods of communicating the state of cybersecurity for the function are established and maintained • Monitoring data are aggregated to provide an understanding of the operational state of the function • Information from across the organisation is available to enhance the common operating picture • Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state for the function to enhance the common operating picture • Information from outside the organisation is collected to enhance the common operating picture • Predefined states of operation are defined and invoked based on the common operating picture	• Industrial Defender endeavours to be the single pane of glass aggregating all cyber security event and configuration management activities and anomalies. • Industrial Defender monitors OT and IT systems for cyber events using the best mechanisms allowed, from host-based agents to remote log monitoring to passive monitoring of network traffic. All events are normalized into a cohesive stream suitable for analysis and correlation of events across the environment. • Industrial Defender vulnerability monitoring identifies known vulnerabilities in software, firmware, and operating systems to support root-cause analysis and identify other vectors before they are exploited. • Industrial Defender consolidates event anomalies, identified vulnerabilities, configuration activity, conformance to baselines, and solution communication integrity into a real-time risk score for each asset. • Industrial Defender offers flexible high-level views of current asset risk assessment, performance anomalies, and event activity. • Industrial Defender offers a library of built-in reports for ad-hoc data analysis along with a custom report generation capability. • Industrial Defender offers data interfaces for flexible alerting, real-time event streams, and scheduled report delivery.	• SA-3A • SA-3B • SA-3C • SA-3D • SA-3E • SA-3F

Domains

1. Asset, Change and Configuration Management (ACM)
2. Cybersecurity Program Management (CPM)
3. Supply Chain and External Dependencies Management (EDM)
4. Identity and Access Management (IAM)
5. Event and Incident Response, Continuity of Operations (IR)
6. Information Sharing and Communications (ISC)
7. Risk Management (RM)
8. Situational Awareness (SA)
9. Threat and Vulnerability Management (TVM)
10. Workforce Management (WM)
11. Australian Privacy Management (APM)

Domain 9: Threat and Vulnerability Management (TVM)

Establish and maintain plans, procedures, and technologies to detect, identify, analyse, manage and respond to cybersecurity threats and vulnerabilities, commensurate with the organisation's infrastructure and organisational objectives.

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
TVM-1: Identify and Respond to Threats	• Information sources to support threat management activities are identified • Cybersecurity threat information is gathered and interpreted for the function • Threats considered important to the function are addressed • A threat profile for the function is established that includes characterisation of intent, capability, and target of threats to the function • Threat information sources that address all components of the threat profile are prioritised and monitored • Identified threats are analysed and prioritised, and addressed according to the assigned priority • The threat profile is validated at an organisation-defined frequency • Analysis and prioritisation of threats are informed by the function's (or organisation's) risk criteria • Threat information is added to the risk register.	• Industrial Defender vulnerability monitoring identifies known vulnerabilities in software, firmware, and operating systems using ICS Cert Advisories and OSINT before they are exploited. • Industrial Defender integrates with Foxguard's patch management system to identify vendor-approved patches for OT systems. • As a real time threat monitoring tool Industrial Defender provides visibility to threats that have either breached your protection mechanisms. • Industrial Defender provides visibility to potential attack paths and techniques mentioned in typical threat intel. • Industrial Defender provides visibility to the threat remediation process.	• TVM-1A • TVM-1B • TVM-1C • TVM-1D • TVM-1E • TVM-1F • TVM-1G • TVM-1H • TVM-1I • TVM-1J
TVM-2: Reduce Cybersecurity Vulnerabilities	• Information sources to support cybersecurity vulnerability discovery are identified • Vulnerability information is gathered and interpreted for the function • Vulnerabilities considered important to the function are addressed • Vulnerability information sources that address all assets important to the function are monitored • Vulnerability assessments are performed • Identified vulnerabilities are analysed and prioritised • Vulnerabilities are addressed according to the assigned priority • Operational impact to the function is evaluated prior to deploying patches • Vulnerability assessments are performed for all assets important to the delivery of the function at an organisation-defined frequency • Vulnerability assessments are informed by the function's risk criteria • Vulnerability assessments are performed by parties independent of the operations of the function • Analysis and prioritisation of vulnerabilities are informed by the function's risk criteria • Vulnerability information is added to the risk register • Risk monitoring activities validate the responses to vulnerabilities	• Industrial Defender monitors OT and IT systems for cyber events using the best mechanisms allowed, from host-based agents to remote log monitoring to passive monitoring of network traffic. All events are normalized into a cohesive stream suitable for analysis and correlation of events across the environment. • Industrial Defender vulnerability monitoring identifies known vulnerabilities in software, firmware, and operating systems before they are exploited. • Industrial Defender asset risk scoring is continuously updated to reflect changing conditions and support continuous improvement activities. • Industrial Defender helps to automate the continual vulnerability assessment process. • Industrial Defender provides raw vulnerability information to help prioritize which vulnerabilities should be mitigated.	• TVM-2A • TVM-2B • TVM-2C • TVM-2D • TVM-2E • TVM-2F • TVM-2G • TVM-2H • TVM-2I • TVM-2J • TVM-2K • TVM-2L • TVM-2M • TVM-2N

Domain 10: Workforce Management (WM)

Establish and maintain plans, procedures, technologies, and controls a culture of cybersecurity and to ensure that ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organisational objectives.

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
WM-1: Assign Cybersecurity Responsibilities	• Cybersecurity responsibilities for the function are identified, documented, and assigned to specific people and roles, including service providers • Responsibilities and job requirements are reviewed and updated as needed • Responsibilities are included in job performance evaluation criteria • Assigned responsibilities are managed to ensure adequacy and redundancy of coverage	• Industrial Defender enables these processes with important data about OT systems and devices but does not perform these actions directly.	• N/A
WM-2: Control the Workforce Lifecycle	• Personnel vetting is performed at hire for positions with access to assets required for delivery of the function • Personnel termination procedures address cybersecurity • Personnel vetting is performed at an organisation-defined frequency for positions with access to the assets required for delivery of the function • Personnel transfer procedures address Cyber Security • Risk designations are assigned to all positions with access to the assets required for delivery of the function • Vetting is performed for all positions at a level commensurate with position risk designation • Succession planning is performed for personnel based on risk designation • A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established Security policies and procedures	• Industrial Defender provides visibility and confirmation that user accounts and access has been revoked after termination.	• WM-2B • WM-2D
WM-3: Develop a Cybersecurity Workforce	• Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities • Cybersecurity knowledge, skill, and ability gaps are identified • Identified gaps are addressed through recruiting and/or training • Training is provided as a prerequisite to granting access to assets that support the delivery of the function • Cybersecurity workforce management objectives that support operational needs are established and maintained • Recruiting and retention are aligned to workforce management objectives • Training is aligned to workforce management objectives • The effectiveness of training is routinely evaluated and improved • Training includes educational opportunities for personnel with cybersecurity responsibilities	• Industrial Defender enables these processes with important data about OT systems and devices but does not perform these actions directly.	• N/A
WM-4: Increase Cybersecurity Awareness	• Cybersecurity awareness activities occur • Objectives for awareness activities are established and maintained • Awareness content is based on the organisation's threat profile • Awareness activities are aligned with the predefined states of operation • The effectiveness of awareness activities is evaluated at an organisation-defined frequency and improvements are made as appropriate	• Industrial Defender enables these processes with important data about OT systems and devices but does not perform these actions directly.	• N/A

Domain 11: 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).

Objective	Description	How Industrial Defender Helps	ID Coverage Areas
APM-1: Manage Personal Information and Privacy	• Privacy requirements applicable to the organisation have been identified • The organisation has defined personal information in the context of its business activities • There is a point of contact to whom privacy issues could be reported • Business activities involving the collection, processing, storage or transmission of personal information have been identified • The organisation's personal information holdings are documented • A privacy policy has been documented and communicated in the organisation and to the public • The organisation's requirements for handling personal information have been defined within the policy • Roles and accountabilities have been assigned for privacy management • A privacy management plan has been implemented to govern ongoing compliance with privacy requirements • Privacy related risks have been identified, assessed, and documented • A documented process exists for responding to privacy enquiries and complaints, including customer correction of personal information • Staff who handle personal information receive privacy training • Existing incident response plans consider data breach scenarios involving personal information and are routinely tested and improved • Compliance with privacy requirements is periodically assessed and reported to senior management	• N/A	• N/A

So how do you make the AESCSF work for you?

Tackling this framework must be an ongoing program, not a one-time project. Assess what you already have in place, prioritize controls you need to implement and evaluate solutions against the business needs of your organization. Industrial Defender has deep OT domain experience and a long history of supporting the unique needs industrial companies from the control room to the boardroom, ensuring KPIs are being met every step of the way.

We can help your team align with every domain in this model and improve maturity in many other rigorous cybersecurity models. To see for yourself how we can help you align with the AESCSF, reach out to one of our OT security architects to **schedule a demo.**

THE INDUSTRIAL DEFENDER DIFFERENCE

Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while providing cross-functional teams with a unified view of security. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. They secure some of the largest critical control system deployments with vendors such as GE, Honeywell, ABB, Siemens, Schneider Electric, Yokogawa and others to protect the availability and safety of these systems, simplify standards and regulatory requirements, and unite OT and IT teams.

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com
225 Foxborough Blvd, Foxborough, MA 02035
industrialdefender.com