AES | CSF
Australian Energy Sector | Cyber Security Framework

2019 AESCSF Glossary

Term	Definition	Source
access	Ability and means to enter a facility, to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.	Adapted from CNSSI 4009
access control	Limiting access to organisational assets only to authorised entities (e.g., users, programs, processes, or other systems). See asset.	Adapted from CNSSI 4009
access management	Management processes to ensure that access granted to the organisation's assets is commensurate with the risk to critical infrastructure and organisational objectives. See access control and asset.	Adapted from CERT RMM
ad hoc	In the context of this model, ad hoc (i.e., an ad hoc practice) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organisational guidance in the form of a prescribed plan (verbal or written), policy, or training. The methods, tools, and techniques used, the priority given a particular instance of the practice, and the quality of the outcome may vary significantly depending on who is performing the practice, when it is performed, and the context of the problem being addressed. With experienced and talented personnel, high-quality outcomes may be achieved even though practices are ad hoc. However, because lessons learned are typically not captured at the organisational level, approaches and outcomes are difficult to repeat or improve across the organisation.	ES-C2M2
advanced metering infrastructure (AMI)	Advanced Metering Infrastructure (AMI) refers to systems that measure, collect, and analyse energy usage, from advanced devices such as 'smart' electricity meters, gas meters, and/or water meters, through various communication media on request or on a predefined schedule.	Adapted from SGMM v1.1 Glossary
anomalous	Inconsistent with or deviating from what is usual, normal, or expected.	Merriam-Webster.com
anomaly	See anomalous.	Merriam-Webster.com
asset	Something of value to the organisation. Assets include many things, including technology, information, roles performed by personnel, and facilities. For the purposes of this model, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the function.	ES-C2M2
asset owner	A person or organisational unit, internal or external to the organisation, that has primary responsibility for the viability, productivity, and resilience of an organisational asset.	CERT RMM

Australian Energy Market Operator (AEMO)	The Australian Energy Market Operator (AEMO) is responsible for operating Australia's largest gas and electricity markets and power systems, including the National Electricity Market (NEM), the interconnected power system in Australia's eastern and south-eastern seaboard and Wholesale Electricity Market (WEM) and power system in Western Australia.	aemo.com.au
Australian Energy Regulator (AER)	The AER regulates wholesale and retail energy markets, and energy networks, under national energy legislation and rules. The AER functions mostly relate to energy markets in eastern and southern Australia	aer.gov.au
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an IT or ICS.	DOE RMP
authenticator	The means used to confirm the identity of a user, processor, or device (e.g., user password or token).	NIST 800-53
availability	Ensuring timely and reliable access to and use of information. For an asset, the quality of being accessible to authorised users (people, processes, or devices) whenever it is needed.	DOE RMP & CERT RMM
business impact analysis	A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs) and recovery point objectives (RPOs). These recovery requirements are then used to develop strategies, solutions and plans.	Adapted from Gartner
capacity	Maximum electric output an electricity generator can produce under specific conditions.	AESCSF
change control (change management)	A continuous process of controlling changes to information or technology assets, related infrastructure, or any aspect of services, enabling approved changes with minimum disruption.	CERT RMM

commercial customer	An entity engaged in establishing and maintaining; - Any utility (water, gas, telecommunications) that is not a critical customer (see critical customer); - Hospitals, aged-care facilities (including any individual customer who has life-support equipment located at their residential address); - Traffic lights and emergency services (Police, fire, ambulance); - Heavy industry; - Cold storage facilities; - Food processing/fresh producers; - Sporting stadiums; - Large shopping centres, and; - Large office buildings. This list is provided as a guide only, and is not an exhaustive list of commercial customer types.	AESCSF
computer security incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An 'imminent threat of violation' refers to a situation in which the organisation has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet. Also, see incident.	NIST 800-61 (computer security incident)
confidentiality	The preservation of authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. For an information asset, confidentiality is the quality of being accessible only to authorised people, processes, and devices.	DOE RMP & Adapted from CERT RMM
configuration baseline	A documented set of specifications for an IT or OT system or asset, or a configuration item within a system, that has been formally reviewed and agreed upon at a given point in time, and which should be changed only through change control procedures. The configuration baseline is used as a basis for future builds, releases, and/or changes.	Adapted from NIST 800-53 Glossary
configuration management	A collection of activities focused on establishing and maintaining the integrity of assets, through control of the processes for initialising, changing, and monitoring the configurations of those assets throughout their life cycle.	NIST SP 800-128

contingency plan	Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The contingency plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the continuity of operations plan or disaster recovery plan for major disruptions.	CNSSI 4009
continuous monitoring	Maintaining ongoing awareness of the current cybersecurity state of the function throughout the operational environment by collecting, analysing, alarming, presenting, and using power system and cybersecurity information to identify anomalous activities, vulnerabilities, and threats to the function in order to support incident response and organisational risk management decisions.	Adapted from NIST 800-137
controls	The management, operational, and technical methods, policies, and procedures-manual or automated-(i.e., safeguards or countermeasures) prescribed for an IT and ICS to protect the confidentiality, integrity, and availability of the system and its information.	DOE RMP
Council of Australian Governments (COAG) Energy Council	The role of COAG is to initiate, develop and monitor the implementation of policy reforms that are of national significance and which require cooperative action by Australian governments.	coag.gov.au
credential	An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.	NIST SP 800-63-2
critical customer	Any customer that operates a critical infrastructure asset. See critical infrastructure.	AESCSF
critical electricity asset	A network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers or an electricity generator station that is critical to ensuring the security and reliability of electricity networks or electricity systems in a State or Territory	SOCI, Section 10

critical infrastructure	Critical Infrastructure are pieces of infrastructure that would have a significant impact to Australia if they were disrupted. The Security of Critical Infrastructure Act (SOCI) defines Critical Infrastructure as: An asset is a critical infrastructure asset if it is: (a) a critical electricity asset; or (b) a critical port; or (c) a critical water asset; or (d) a critical gas asset; or (e) an asset declared under section 51 (of the act) to be a critical infrastructure asset; or (f) an asset prescribed by the rules for the purposes of this paragraph.	SOCI, Section 9
current	Updated at an organisation-defined frequency (e.g., as in the asset inventory is kept 'current') that is selected such that the risks to critical infrastructure and organisation objectives associated with being out-of-date by the maximum interval between updates are acceptable to the organisation and its stakeholders.	ES-C2M2
customer	Any individual (or entity) who purchases a non-commercial quantity of electricity. See commercial customer.	AESCSF
cyber attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or for destroying the integrity of the data or stealing controlled information.	DOE RMP
cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks. Measures taken to protect a computer or computerised system (IT and OT) against unauthorised access or attack.	DOE RMP and Merriam-Webster.com
cybersecurity architecture	An integral part of the enterprise architecture that describes the structure and behaviour for an enterprise's security processes, cybersecurity systems, personnel, and subordinate organisations, showing their alignment with the organisation's mission and strategic plans. See enterprise architecture and network architecture.	DOE RMP
cybersecurity event	Any observable occurrence in a system or network that is related to a cybersecurity requirement (confidentiality, integrity, or availability). See also event.	ES-C2M2
cybersecurity impact	The effect on the measures that are in place to protect from and defend against cyber attack.	ES-C2M2

cybersecurity plan	Formal document that provides an overview of the cybersecurity requirements for an IT and ICS and describes the cybersecurity controls in place or planned for meeting those requirements.	DOE RMP
cybersecurity policy	A set of criteria for the provision of security services.	DOE RMP
cybersecurity program	A cybersecurity program is an integrated group of activities designed and managed to meet cybersecurity objectives for the organisation and/or the function. A cybersecurity program may be implemented at either the organisation or the function level, but a higher-level implementation and enterprise viewpoint may benefit the organisation by integrating activities and leveraging resource investments across the entire enterprise.	ES-C2M2
cybersecurity program strategy	A plan of action designed to achieve the performance targets that the organisation sets to accomplish its mission, vision, values, and purpose for the cybersecurity program.	CERT RMM
cybersecurity requirements	Requirements levied on IT and OT that are derived from organisational mission and business case needs (in the context of applicable legislation, Executive Orders, directives, policies, standards, instructions, regulations, procedures) to ensure the confidentiality, integrity, and availability of the services being provided by the organisation and the information being processed, stored, or transmitted.	Adapted from DOE RMP
cybersecurity responsibilities	Obligations for ensuring the organisation's cybersecurity requirements are met.	ES-C2M2
cybersecurity risk	The risk to organisational operations (including mission, functions, image, reputation), resources, and other organisations due to the potential for unauthorised access, use, disclosure, disruption, modification, or destruction of information and/or IT and ICS. See risk.	DOE RMP
cybersecurity workforce management objectives	Performance targets for personnel with cybersecurity responsibilities that the organisation sets to meet cybersecurity requirements.	Adapted from CERT RMM
defined practice	A practice that is planned (i.e., described, explained, made definite and clear, and standardised) and is executed in accordance with the plan.	Adapted from CERT RMM
dependency risk	Dependency risk is measured by the likelihood and severity of damage if an IT or OT system is compromised due to a supplier or other external party on which delivery of the function depends. Evaluating dependency risk includes an assessment of the importance of the potentially compromised system and the impact of compromise on organisational operations and assets, individuals, other organisations, and the Nation. See upstream dependencies and supply chain risk.	Adapted from NIST 7622, pg. 10
deprovisioning	The process of revoking or removing an identity's access to organisational assets. See also provisioning.	CERT RMM

distribution	The delivery of energy to retail customers (e.g., homes, businesses, industry, government facilities).	Adapted from EIA Glossary
Distribution Network Service Provider (DNSP)	Owner and operator of substations and the wires that transport from distribution centres to end-use consumers. Also provider of technical services, including construction of power lines, inspection of equipment, maintenance and street lighting.	AESCSF
domain	In the context of the model structure, a domain is a logical grouping of cybersecurity practices.	ES-C2M2
domain objectives	The practices within each domain are organised into objectives. The objectives represent achievements that support the domain (such as 'Manage Asset Configuration' for the ACM domain and 'Increase Cybersecurity Awareness' for the WM domain). Each of the objectives in a domain comprises a set of practices, which are ordered by maturity indicator level.	ES-C2M2
downstream dependencies	External parties dependent on the delivery of the function, such as customers and some operating partners.	ES-C2M2
electrical substation	Electrical substations act as connection points between the electricity networks and electricity generators, large load customers, and the lower voltage distribution network it serves (including switch yards).	AESCSF
electricity sector information sharing and analysis center (ES-ISAC)	The Electricity Sector Information Sharing and Analysis Center (ES-ISAC) shares critical information with industry participants about infrastructure protection. The ES-ISAC serves the electricity sector by facilitating communications between electricity sector participants, federal governments, and other critical infrastructures. It is the job of the ES-ISAC to promptly disseminate threat indications, vulnerabilities, analyses, and warnings, together with interpretations, to help electricity sector participants take protective actions. See Information Sharing and Analysis Center (ISAC).	Adapted from Electricity Sector Information Sharing and Analysis Center (ES-ISAC) website home page
electricity subsector	A portion of the energy sector that includes the generation, transmission, and distribution of electricity.	ES-SPP
enterprise	The largest (i.e., highest-level) organisational entity to which the organisation participating in the AESCSF survey belongs. For some participants, the organisation taking the survey is the enterprise itself. See organisation.	Adapted from SGMM v1.1 Glossary
enterprise architecture	The design and description of an enterprise's entire set of IT and OT: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. See cybersecurity architecture and network architecture.	DOE RMP (but changed ICS to OT)
entity	Something having separate or distinct existence.	Merriam-Webster.com

establish and maintain	The development and maintenance of the object of the practice (such as a program). For example, 'Establish and maintain identities' means that not only must identities be provisioned, but they also must be documented, have assigned ownership, and be maintained relative to corrective actions, changes in requirements, or improvements.	CERT RMM
event	Any observable occurrence in a system or network. Depending on their potential impact, some events need to be escalated for response. To ensure consistency, criteria for response should align with the organisation's risk criteria.	NIST 800-61
function	The high-level electricity system activity or set of activities performed by the utility to which the model is being applied. Generally, the function will be generation, transmission, distribution, and/or markets. When using the AESCSF evaluation survey, the function is the organisational line-of-business (generation, transmission, distribution, or markets) that is being evaluated by completing the model.	ES-C2M2
generation	The process of producing electric energy by transforming other forms of energy; also, the amount of electric energy produced, expressed in kilowatt- hours.	EIA Glossary
generation capacity	Measured in Megawatts (MW)	AESCSF
governance	An organisational process of providing strategic direction for the organisation while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. Governance also typically includes the concepts of sponsorship (setting the managerial tone), compliance (ensuring that the organisation is meeting its compliance obligations), and alignment (ensuring that processes such as those for cybersecurity program management align with strategic objectives).	Adapted from CERT RMM
guidelines	A set of recommended practices produced by a recognised authoritative source representing subject matter experts and community consensus, or internally by an organisation. See standard.	ES-C2M2
Human Machine Interface (HMI)	A Human Machine Interface consists of hardware and software that allow operators to monitor and control a process control system. A HMI enables people to support and interact with complex technological systems.	AESCSF
identity	The set of attribute values (i.e., characteristics) by which an entity is recognisable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.	CNSSI 4009
impact	Negative consequence to subsector functions.	ES-C2M2

incident	An event (or series of events) that significantly affects (or has the potential to significantly affect) critical infrastructure and/or organisational assets and services and requires the organisation (and possibly other stakeholders) to respond in some way to prevent or limit adverse impacts. See also computer security incident and event.	Adapted from CERT RMM
incident life cycle	The stages of an incident from detection to closure. Collectively, the incident life cycle includes the processes of detecting, reporting, logging, triaging, declaring, tracking, documenting, handling, coordinating, escalating and notifying, gathering and preserving evidence, and closing incidents. Escalated events also follow the incident life cycle, even if they are never formally declared to be incidents.	Adapted from CERT RMM
information assets	Information or data that is of value to the organisation, including diverse information such as operational data, intellectual property, customer information, and contracts.	Adapted from CERT RMM
information sharing and analysis center (ISAC)	An Information Sharing and Analysis Center (ISAC) shares critical information with industry participants on infrastructure protection. Each critical infrastructure industry has established an ISAC to communicate with its members, its government partners, and other ISACs about threat indications, vulnerabilities, and protective strategies. ISACs work together to better understand cross-industry dependencies and to account for them in emergency response planning. See Electricity Sector Information Sharing and Analysis Center (ES-ISAC).	Adapted from Electricity Sector Information Sharing and Analysis Center (ES-ISAC) website home page
information technology (IT)	A discrete set of electronic information resources organised for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate.	DOE RMP
institutionalisation	The extent to which a practice or activity is ingrained into the way an organisation operates. The more an activity becomes part of how an organisation operates, the more likely it is that the activity will continue to be performed over time, with a consistently high level of quality. ('Incorporated into the ingrained way of doing business that an organisation follows routinely as part of its corporate culture.' - CERT RMM). See also maturity indicator level.	ES-C2M2
integrity	Guarding against improper information modification or destruction. Integrity includes ensuring information nonrepudiation and authenticity. For an asset, integrity is the quality of being in the condition intended by the owner and therefore continuing to be useful for the purposes intended by the owner.	DOE RMP & CERT RMM
interconnector	An interconnector is infrastructure that connects the energy transmission systems of two regions, allowing energy (such as electricity or gas) to flow between them.	AESCSF

isolated	Physically or logically independent from another.	AESCSF
least privilege	A security control that addresses the potential for abuse of authorised privileges. The organisation employs the concept of least privilege by allowing only authorised access for users (and processes acting on behalf of users) who require it to accomplish assigned tasks in accordance with organisational missions and business functions. organisations employ the concept of least privilege for specific duties and systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organisational missions and/or functions. organisations consider the creation of additional processes, roles, and information system accounts as necessary to achieving least privilege. organisations also apply least privilege concepts to the design, development, implementation, and operations of IT and OT systems.	Adapted from NIST 800-53
load	The quantum of electricity delivered to, or demanded from, any one or more customers (including commercial and critical customers).	AESCSF
logging	Logging typically refers to automated recordkeeping (by elements of an IT or OT system) of system, network, or user activity. Logging may also refer to keeping a manual record (e.g., a sign-in sheet) of physical access by personnel to a protected asset or restricted area, although automated logging of physical access activity is commonplace. Regular review and audit of logs (manually or by automated tools) is a critical monitoring activity that is essential for situational awareness (e.g., through the detection of cybersecurity events or weaknesses).	ES-C2M2
logical control	A software, firmware, or hardware feature (i.e., computational logic, not a physical obstacle) within an IT or OT system that restricts access to and modification of assets only to authorised entities. For contrast, see physical control.	Adapted from CNSSI 4009 definition of 'internal security controls'
markets	Venues where participants buy and sell products and services. In the context of this model, markets refers to trading involving wholesale electricity.	FERC
maturity	The extent to which an organisation has implemented and institutionalised the cybersecurity practices of the model.	ES-C2M2

maturity indicator level (MIL)	A measure of the cybersecurity maturity of an organisation in a given domain of the model. The model currently defines four maturity indicator levels (MILs) and holds a fifth level in reserve for use in future versions of the model. Each of the four defined levels is designated by a number (0 through 3) and a name, for example, 'MIL3: managed.' A MIL is a measure of the progression within a domain from individual and team initiative, as a basis for carrying out cybersecurity practices, to organisational policies and procedures that institutionalise those practices, making them repeatable with a consistently high level of quality. As an organisation progresses from one MIL to the next, the organisation will have more complete or more advanced implementations of the core activities in the domain.	ES-C2M2
monitoring	Collecting, recording, and distributing information about the behaviour and activities of systems and persons to support the continuous process of identifying and analysing risks to organisational assets and critical infrastructure that could adversely affect the operation and delivery of services.	Adapted from CERT RMM (monitoring and risk management)
monitoring requirements	The requirements established to determine the information gathering and distribution needs of stakeholders.	CERT RMM
multifactor authentication	Authentication using two or more factors to achieve authentication. Factors include (i) something you know (e.g., password/PIN), (ii) something you have (e.g., cryptographic identification device, token), (iii) something you are (e.g., biometric), or (iv) you are where you say you are (e.g., GPS token). See authentication.	Adapted from NIST 800-53
National Electricity Market (NEM)	Comprised of five physically connected regions on the east coast of Australia: Queensland, NSW (including ACT), Victoria, Tasmania and South Australia.	aemo.com.au
network architecture	A framework that describes the structure and behaviour of communications among IT and/or OT assets and prescribes rules for interaction and interconnection. See enterprise architecture and cybersecurity architecture.	Adapted from CNSSI 4009 (IA architecture)
Network Services Providers (NSP)	Operates electricity networks. An NSP can refer to both a TNSP or DNSP.	AESCSF
operating picture	Real-time (or near-real-time) awareness of the operating state of a system or function. An operating picture is formed from data collected from various trusted information sources that may be internal or external to the system or function (e.g. temperature, weather events and warnings, cybersecurity alerts). The operating picture may or may not be presented graphically. It involves the collection, analysis (including fusion), and distribution of what is important to know to make decisions about the operation of the system. A common operating picture (COP) is a single operating picture that is available to the stakeholders of the system or function so that all stakeholders can make decisions based on the same reported operating state. See common operating picture.	ES-C2M2

operating states	See pre-defined states of operation.	ES-C2M2
operational resilience	The organisation's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organisation's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk. See the related term operational risk.	CERT RMM
operational risk	The potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events. In the context of this model, our focus is on operational risk from cybersecurity threats.	Adapted from CERT RMM
operational technology	See operations technology.	AESCSF
operations technology (OT)	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.	ES-C2M2
organisation	An organisation of any size, complexity, or positioning within an organisational structure that is charged with carrying out assigned mission and business processes and that uses IT and OT in support of those processes. In the context of the model, the organisation is the entity using the model or that is under examination.	Adapted from DOE RMP
periodic review/activity	A review or activity that occurs at specified, regular time intervals, where the organisation-defined frequency is commensurate with risks to organisational objectives and critical infrastructure.	Adapted from SEI CMM Glossary
personal information	Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.	Australian Government OAIC
personnel	Employees of the organisation. This includes full time, part time, and contracted employees.	AESCSF
physical control	A type of control that prevents physical access to, and modification of, information assets or physical access to technology and facilities. Physical controls often include such artifacts as card readers and physical barrier methods.	CERT RMM
policy	A high-level overall plan embracing the general goals and acceptable procedures of an organisation.	Merriam-Webster.com
position description	A set of responsibilities that describe a role or roles filled by an employee. Also known as a job description.	ES-C2M2

practice	An activity described in the model that can be performed by an organisation to support a domain objective. The purpose of these activities is to achieve and sustain an appropriate level of cybersecurity for the function, commensurate with the risk to critical infrastructure and organisational objectives.	ES-C2M2
pre-defined states of operation	Distinct operating modes (which typically include specific IT and OT configurations as well as alternate or modified procedures) that have been designed and implemented for the function and can be invoked by a manual or automated process in response to an event, a changing risk environment, or other sensory and awareness data to provide greater safety, resiliency, reliability, and/or cybersecurity. For example, a shift from the normal state of operation to a high-security operating mode may be invoked in response to a declared cybersecurity incident of sufficient severity. The high-security operating state may trade off efficiency and ease of use in favour of increased security by blocking remote access and requiring a higher level of authentication and authorisation for certain commands until a return to the normal state of operation is deemed safe.	ES-C2M2
procedure	In this model, procedure is synonymous with process.	ES-C2M2
process	A series of discrete activities or tasks that contribute to the fulfilment of a task or mission.	CERT RMM (Business Process)
provisioning	The process of assigning or activating an identity profile and its associated roles and access privileges. See also deprovisioning.	CERT RMM
Recovery Time Objectives (RTO)	Documented goals and performance targets the organisation sets for recovery of an interrupted function in order to meet critical infrastructure and organisational objectives.	ES-C2M2
region	An AEMO defined term, there are five Regions in the NEM. The NEM regions are: QLD, NSW, VIC, SA, and TAS.	aemo.com.au
retailers	Electricity retailers buy electricity at spot price and on-sell it to end-use customers.	AESCSF
risk	A measure of the extent to which an organisation is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs and (2) the likelihood of occurrence.	DOE RMP
risk analysis	A risk management activity focused on understanding the condition and potential consequences of risk, prioritising risks, and determining a path for addressing risks. Determines the importance of each identified risk and is used to facilitate the organisation's response to the risk.	Adapted from CERT RMM
risk assessment	The process of identifying risks to organisational operations (including mission, functions, image, reputation), resources, other organisations, and the Nation, resulting from the operation of an IT and ICS.	DOE RMP

risk criteria	Objective criteria that the organisation uses for evaluating, categorising, and prioritising operational risks based on impact, tolerance for risk, and risk response approaches.	ES-C2M2
risk designation, as in 'position risk designation'	An indication, such as high, medium, or low, of the position's potential for adverse impact to the efficiency, integrity, or availability of the organisation's services.	Adapted from OPM
risk disposition	A statement of the organisation's intention for addressing an operational risk. Typically limited to 'accept,' 'transfer,' 'research,' or 'mitigate.'	CERT RMM
risk management program	The program and supporting processes to manage cybersecurity risk to organisational operations (including mission, functions, image, and reputation), resources, other organisations, and the Nation. It includes (1) establishing the context for risk-related activities, (2) assessing risk, (3) responding to risk once determined, and (4) monitoring risk over time.	DOE RMP
risk management strategy	Strategic-level decisions on how senior executives manage risk to an organisation's operations, resources, and other organisations.	DOE RMP
risk mitigation	Prioritising, evaluating, and implementing appropriate risk-reducing controls.	DOE RMP
risk mitigation plan	A strategy for mitigating risk that seeks to minimise the risk to an acceptable level.	CERT RMM
risk parameter/risk parameter factors	Organisation-specific risk tolerances used for consistent measurement of risk across the organisation. Risk parameters include risk tolerances and risk measurement criteria.	CERT RMM
risk register	A structured repository where identified risks are recorded to support risk management.	ES-C2M2
risk response	Accepting, avoiding, mitigating, sharing, or transferring risk to organisational operations, resources, and other organisations.	DOE RMP
risk taxonomy	The collection and cataloguing of common risks that the organisation is subject to and must manage. The risk taxonomy is a means for communicating these risks and for developing mitigation actions specific to an organisational unit or line-of-business if operational assets and services are affected by them.	Adapted from CERT RMM
role	A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.	CNSSI 4009
SCADA	Supervisory Control and Data Acquisition is an industrial computer system for process control and gathering of data in real time from remote locations in order to control equipment and conditions.	AESCSF

secure software development	Developing software using recognised processes, secure coding standards, best practices, and tools that have been demonstrated to minimise security vulnerabilities in software systems throughout the software development life cycle. An essential aspect is to engage programmers and software architects who have been trained in secure software development.	ES-C2M2
separation of duties	[A security control that] 'addresses the potential for abuse of authorised privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Organisations with significant personnel limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls.'	NIST 800-53, pp. 31, F-13
service level agreement (SLA)	Defines the specific responsibilities of the service provider, including the satisfaction of any relevant cybersecurity requirements, and sets the customer's expectations regarding the quality of service to be provided.	Adapted from CNSSI 4009
single point of failure (SPOF)	An environment/system where one failure can result in the failure of the entire system. For high availability systems, a design goal is to reduce the number of single points of failure.	AESCSF
situational awareness	A sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a system (including its cybersecurity safeguards), in the context of the threat environment and risks to the system's mission, to support effective decision making with respect to activities that depend on and/or affect how well a system functions. It involves the collection of data (e.g., via sensor networks), data fusion, and data analysis (which may include modelling and simulation) to support automated and/or human decision making (for example, concerning power system functions). Situational awareness also involves the presentation of the results of the data analysis in a form (e.g., using data visualisation techniques, appropriate use of alarms) that aids human comprehension and allows operators or other personnel to quickly grasp the key elements needed for good decision making.	Adapted from SGMM Glossary

sponsorship	Enterprise-wide support of cybersecurity objectives by senior management as demonstrated by formal policy or by declarations of management's commitment to the cybersecurity program along with provision of resources. Senior management monitors the performance and execution of the cybersecurity program and is actively involved in the ongoing improvement of all aspects of the cybersecurity program.	ES-C2M2
stakeholder	An external organisation or an internal or external person or group that has a vested interest in the organisation or function (that is being evaluated using this model) and its practices. Stakeholders involved in performing a given practice (or who oversee, benefit from, or are dependent upon the quality with which the practice is performed) could include those from within the function, from across the organisation, or from outside the organisation.	Adapted from CERT RMM
standard	A standard is a document, established by consensus that provides rules, guidelines, or characteristics for activities or their results. See guidelines.	Adapted from ISO/IEC Guide 2:2004
states of operation	See pre-defined states of operation.	ES-C2M2
strategic objectives	The performance targets that the organisation sets to accomplish its mission, vision, values, and purpose.	CERT RMM
strategic planning	The process of developing strategic objectives and plans for meeting these objectives.	CERT RMM
supply chain	The set of organisations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organisation's customers. The supply chain encompasses the full product life cycle and includes design, development, and acquisition of custom or commercial off-the-shelf (COTS) products, system integration, system operation (in its environment), and disposal. People, processes, services, products, and the elements that make up the products wholly impact the supply chain.	NISTIR 7622 Source of 1st paragraph cited as [NDIA ESA]
supply chain risk	Supply chain risk is measured by the likelihood and severity of damage if an IT or OT system is compromised by a supply chain attack, and takes into account the importance of the system and the impact of compromise on organisational operations and assets, individuals, other organisations, and the Nation. Supply chain attacks may involve manipulating computing system hardware, software, or services at any point during the life cycle. Supply chain attacks are typically conducted or facilitated by individuals or organisations that have access through commercial ties, leading to stolen critical data and technology, corruption of the system/ infrastructure, and/or disabling of mission-critical operations. See risks and supply chain.	Adapted from NIST 7622, pg. 7 & pg. 10
telecommunications	Internal private telecommunication hardware. Telecommunications networks that earn additional revenue may be classified as Regulated Telecommunications	AESCSF

threat	Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), resources, and other organisations through IT, OT, or communications infrastructure via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.	Adapted from DOE RMP
threat assessment	The process of evaluating the severity of threat to an IT and ICS or organisation and describing the nature of the threat.	DOE RMP
threat profile	A characterisation of the likely intent, capability, and targets for threats to the function. It is the result of one or more threat assessments across the range of feasible threats to the IT and OT of an organisation and to the organisation itself, delineating the feasible threats, describing the nature of the threats, and evaluating their severity.	ES-C2M2
threat source	An intent and method targeted at the intentional exploitation of a vulnerability or a situation, or a method that may accidentally exploit a vulnerability.	DOE RMP
traceability	The ability to determine whether or not a given attribute of the current state is valid (e.g., the current configuration of a system or the purported identity of a user) based on the evidence maintained in a historical record showing how the attribute was originally established and how it has changed over time.	ES-C2M2
transmission	The movement or transfer of electric energy over an interconnected group of lines and associated equipment between points of supply and points at which it is transformed for delivery to consumers or is delivered to other electric systems. Transmission is considered to end when the energy is transformed for distribution to the consumer.	EIA Glossary
Transmission Network Service Provider (TNSP)	Owner and operator of the high-voltage transmission towers, electrical substations, and wires that transport electricity.	AESCSF
upstream dependencies	External parties on which the delivery of the function depends, including suppliers and some operating partners.	ES-C2M2
validate	Collect and evaluate evidence to confirm or establish the quality of something (e.g., information, a model, a product, a system, or component) with respect to its fitness for a particular purpose.	ES-C2M2
Virtual Power Plants (VPP)	A Virtual Power Plant (VPP) refers to an aggregation of resources, coordinated using software and communications technology, to deliver services that have traditionally been performed by a conventional power plant. In Australia, grid-connected VPPs are focused on coordinating rooftop PV and battery storage.	AEMO

vulnerability	A cybersecurity vulnerability is a weakness or flaw in IT, OT, or communications systems or devices, system procedures, internal controls, or implementation that could be exploited by a threat source. A vulnerability class is a grouping of common vulnerabilities.	Adapted from NISTIR 7628 Vol. 1, pp. 8
vulnerability assessment	Systematic examination of an IT or product to determine the adequacy of cybersecurity measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cybersecurity measures, and confirm the adequacy of such measures after implementation.	DOE RMP
Wholesale Electricity Market (WEM)	The Wholesale Electricity Market in Western Australia facilitates competition and private investment, and allows generators and wholesale purchasers of electricity greater flexibility as to how they sell or procure electricity, and who they transact with.	AESCSF
wide area network (WAN)	The hardware and software configuration of devices that enable data communications across sites. WAN technologies can include both Internet Protocol (IP) and Time Division Multiplex (TDM)/Serial Network technologies.	AESCSF
workforce life cycle	For the purpose of this model, the workforce life cycle comprises the distinct phases of workforce management that apply to personnel both internal and external to the organisation. Specific cybersecurity implications and requirements are associated with each life cycle phase. The workforce life cycle includes recruiting, hiring, on boarding, skill assessments, training and certification, assignment to roles (deployment), professional growth and development, re-assignment and transfers, promotions and demotions, succession planning, and termination or retirement. The phases may not be in strict sequences, and some phases (like training, re-assignment, and promotions) may recur.	ES-C2M2
workforce management objectives	See cybersecurity workforce management objectives.	ES-C2M2