



# CYBER SECURITY SUPPLY CHAIN MANAGEMENT

*WHAT CAN  
ENGINEERS DO?*

**ITEE - QLD**



**ENGINEERS  
AUSTRALIA**



# !!i WARNING !!i

- This is general advice and your environment will be **different** and I don't know how it works – so think before making any changes
- The information presented today does not represent the views of my current or previous employers
- This a very complicated and nuanced topic – the point of this session is to provide an overview of existing materials and help you as engineers make better decisions
- Please don't sue me

# Today's Agenda

1. What is Cyber Security Supply Chain Management
2. Australian Cyber Security Centre (ACSC) Supply Chain Advice Overview
3. Case studies
  - a) Integrating Third Party systems and devices
  - b) Cloud Security Deep dive
4. Relevant Cyber Security Standards and Frameworks for Cyber Security Supply Chain
  1. NIST Cyber Security Framework
  2. Australian Energy Sector Cyber Security Framework (AESCSF)
5. Other resources
6. Next Steps and Q&A

# /whois

- Graduated Bachelor Engineering (Telecommunications) First Class Honours at QUT in 2009
- Worked as a telecommunications engineer at QR -> QR National -> Aurizon for 7 years – as a Data Communications Engineer (IP Route/Switch/MPLS, Network Security & Network Management)
- Did some other stuff – went back to Uni and studied a Master of Business in Applied Finance and I am now interested in Asset Management (engineering not the finance type)
- Currently an Operational Technology Cyber Security Specialist
- SABSA Chartered Foundation (SCF), GIAC Incident Response and Defense (GRID), ALC Cyber Security Foundation+Practitioner, QUT ICS Security, Former CCNP, CCDP and CCNA Security (Lapsed 2017)
- Vice Chair of the College of the Queensland Branch of Information, Telecommunications and Electronics Engineers (ITEE), Engineers Australia & Volunteer at BSides Brisbane



# WHAT IS CYBER SECURITY SUPPLY CHAIN MANAGEMENT?

---

# Cyber Security Supply Chain Risk Management

- **Understanding and managing** cyber security risks that are due to the use of third party systems and services
  - **Understanding** – having an awareness of what third party systems and services you are using in your project/enterprise
  - **Managing** – how do you manage cyber security risks across the life cycle of the system or service – from conceptual design, procurement, development and installation, operations and decommissioning
- Cyber Security Supply Chain Risk Management **exists in the entire technology environment** and **relies on multiple departments** in the organisation – Engineering, Operations, Information Security, Procurement and Legal
- Taking it from we **‘don’t know’** to a **managed process**



# ACSC ADVICE



# ACSC Advice

- In November 2019 the Australian Cyber Security Centre (ACSC) released their Cyber Security Supply Chain Risk Management advice – <https://www.cyber.gov.au/publications/cyber-supply-chain-risk-management>
- It defines the below key tasks:
  - Identify the cyber supply chain
  - Understand the cyber supply chain
  - Set cyber security expectations with suppliers
  - Audit suppliers for compliance
  - Monitor and improve cyber supply chain security
- The site also provides the additional material:
  - Cyber Supply Chain Risk Management Practitioner Guide
  - Questions to ask your Managed Service Provider
  - How to manage your security when engaging a managed service provider
  - Specific Cloud Computing advice



## ACSC Advice – *Identify the Cyber Supply Chain*

- *“This includes all suppliers, such as software and hardware vendors, managed services providers, and where possible, their sub-contractors”*
- *“As a starting point, organisations should establish a list of suppliers they have business arrangements with. While an exhaustive list of all suppliers, especially their sub-contractors, may not be possible, the identification of those responsible for products or services with security enforcing functions, privileged access or handling particularly sensitive information should be prioritised.”*

# ACSC Advice – Understand the cyber supply chain

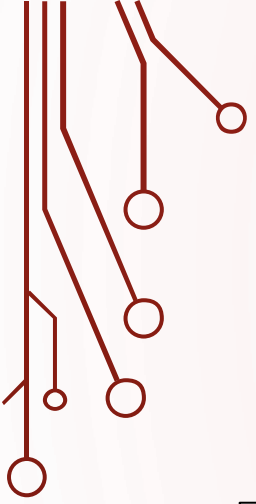
- *“organisations should seek to understand the cyber supply chain risk that those suppliers pose through established risk management practices within their organisation.”*
- *“This may involve speaking to suppliers about their existing cyber security arrangements, determining whether suppliers hold any security certifications, looking at the track record of security vulnerabilities in a supplier’s product or service offerings and their responsiveness to resolving them, and whether the supplier has a vulnerability disclosure policy.”*
- *“in some cases the Government may deem a particular supplier, or one of their products or services, to be a national security concern. ... In particular, for critical infrastructure providers, the **Security of Critical Infrastructure Act 2018** grants provision for specific direction to be issued by the Government where national security concerns exist.”*
- *“As a result of understanding their cyber supply chain risk, organisations should be able to develop both a prioritised list of suppliers that present a high risk to their organisation along with an associated cyber supply chain risk management plan”*

# ACSC Advice – Set cyber security expectations with suppliers

- *“organisations should seek to establish cyber security expectations with all of their suppliers. As part of this, cyber security expectations should be clearly documented in contracts or memorandum of understandings in order to ensure that suppliers are appropriately managing their own security posture, including their cyber supply chain risk.”*
- *“In many cases, cyber security expectations set out in contracts or memorandum of understandings should not be excessively restrictive; except where suppliers are involved in the provision or support to highly classified systems. Rather, cyber security expectations should be justifiable, achievable and proportional to the information being entrusted to suppliers or the role that their products or services play in an organisation’s systems.”*
- *“Finally, organisations should seek to ensure that any cyber security expectations set out in contracts or memorandum of understandings with suppliers are passed through in turn to their suppliers.”*

## ACSC Advice – Audit Suppliers for compliance

- *“it is important that organisations have confidence that those expectations are being met. One way to achieve such assurances is through routine audits or other forms of technical assessments. Provisions for such activities should be stipulated within contracts or memorandum of understandings (often referred to as a ‘right to audit’ clause) and can serve as a way to gain independent assurances of the security posture of suppliers.”*



## ACSC Advice – *Monitor and improve cyber supply chain security*

- *“Ultimately, effective cyber supply chain risk management is based upon trusting partnerships between suppliers and customers. Such partnerships can be strengthened through common cyber security goals and information sharing arrangements, such as sharing best practices and threat intelligence, as well as assisting each other with responding to cyber security incidents and involving each other in any cyber security exercises.”*

# ACSC Advice – Practitioner Guide

The document <sup>#</sup> provides detailed advice and further guidance for each of the key steps, relevant case studies and worked case study examples:

- This is an excellent resource to reference for your design and to communicate with the business on why this is such an important topic
- It provides useful practical advice for each of the steps defined in the Cyber Security Supply Chain Life Cycle

## Worked Case Studies

1. *Open source software components*
2. *The cellular network dongle*
3. *The national infrastructure project*



# CASE STUDIES

---

INTEGRATING THIRD  
PARTY SYSTEMS AND  
DEVICES

# Integrating Third Party Systems and Devices

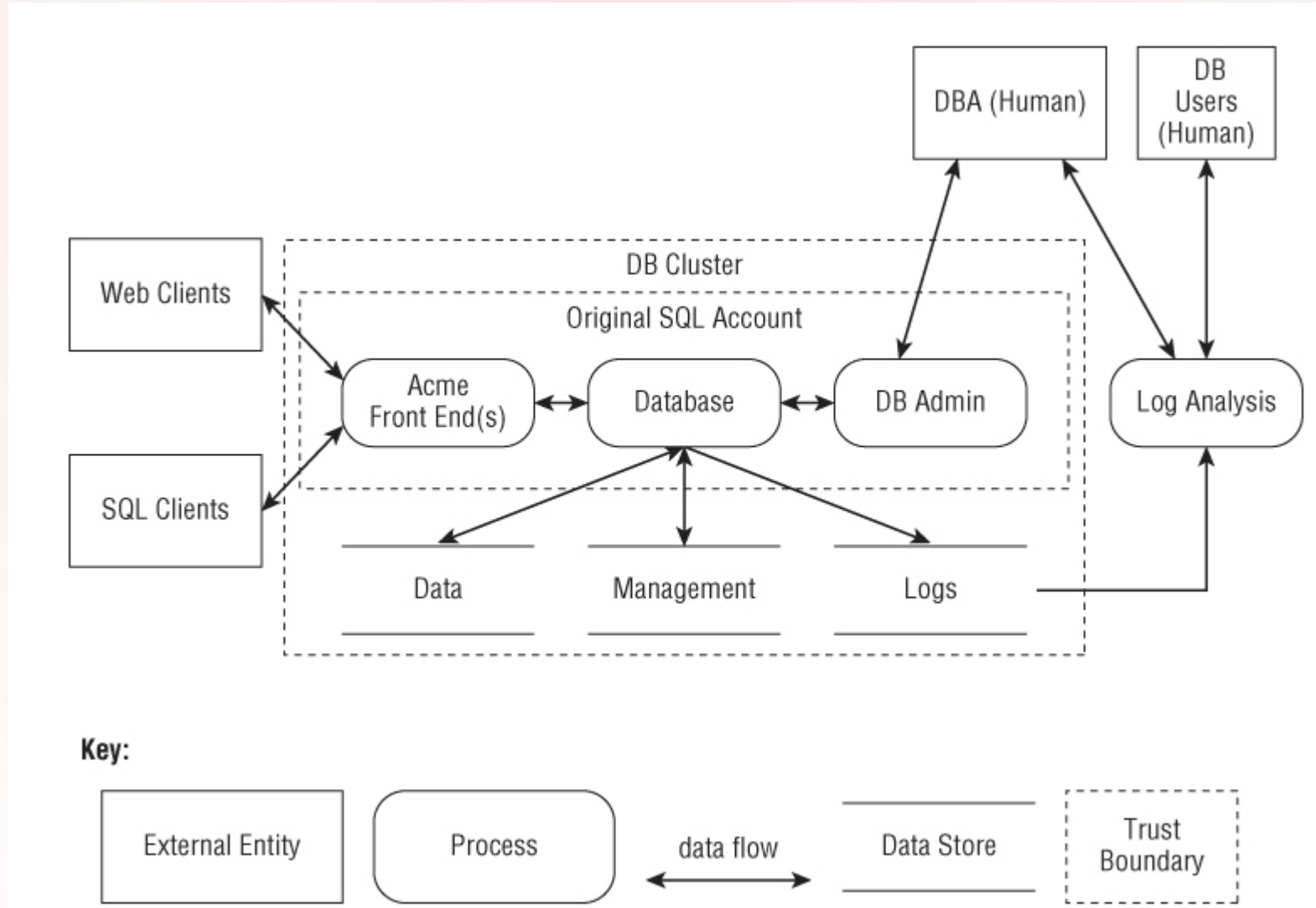




# Understand the System

- Understand the business problem, the criticality of the system and the criticality of your organization (e.g. are you Critical National Infrastructure as per the Security Of Critical Infrastructure Act)
- Define what the system is (Assets, Users, Services), understand its scope and interfaces are
- Think about data classification and trust boundaries
- Draw up a data flow diagram

# Understand the System – Data Flow Diagram




## Integrating Third Party Systems and Devices (cont.)

- Risk Assessments – things to think about for third parties (even fourth parties)
- Identify key cyber security controls and seek vendor advice
- What kind of questions should you be asking the vendor:
  - What is the vendor's security program – do they have an Information Security Program or an Information Security Management System
  - What is the Vendor's Security Development Life Cycle (SDLC) – how well is it supported through it's entire life cycle
  - What does the vendor recommend to harden the platform – does it align with existing frameworks (i.e. CIS benchmarks)
  - Vendor's security certification
  - ... the product/service security certification
- Can you get assistance from the Australian Government?

# Go Live Assurance and Life Cycle Management

- How can you assure the design (i.e. penetration testing, validating detective controls etc.)
- How do you manage cyber security supply chain management in operations, how do you apply patching and receive vulnerability advisories, how do you securely permit access to your vendors (consider the ACSC Remote Access Protocol)
- How do you manage the vendor through the systems life cycle (including contract management)



# CASE STUDIES

---

CLOUD  
SPECIFIC

# Cloud Specific

- Similar to the first case study but extra analysis should be considered:
  - The cloud workloads may not always be hosted in Australia, and different components of the service could be hosted in different regions – also, depending on the service offering things workloads could shift dramatically
  - Data Sovereignty Issues – what type of data will be exposed to a cloud service? I like Mike Burgess's 5 knows of cyber security (relevant for all hosting types):
    1. Know the value of your data
    2. Know who access to your data
    3. Know where your data is located
    4. Know who is protecting your data
    5. Know how well your data is protected

# Cloud Specific (cont.)

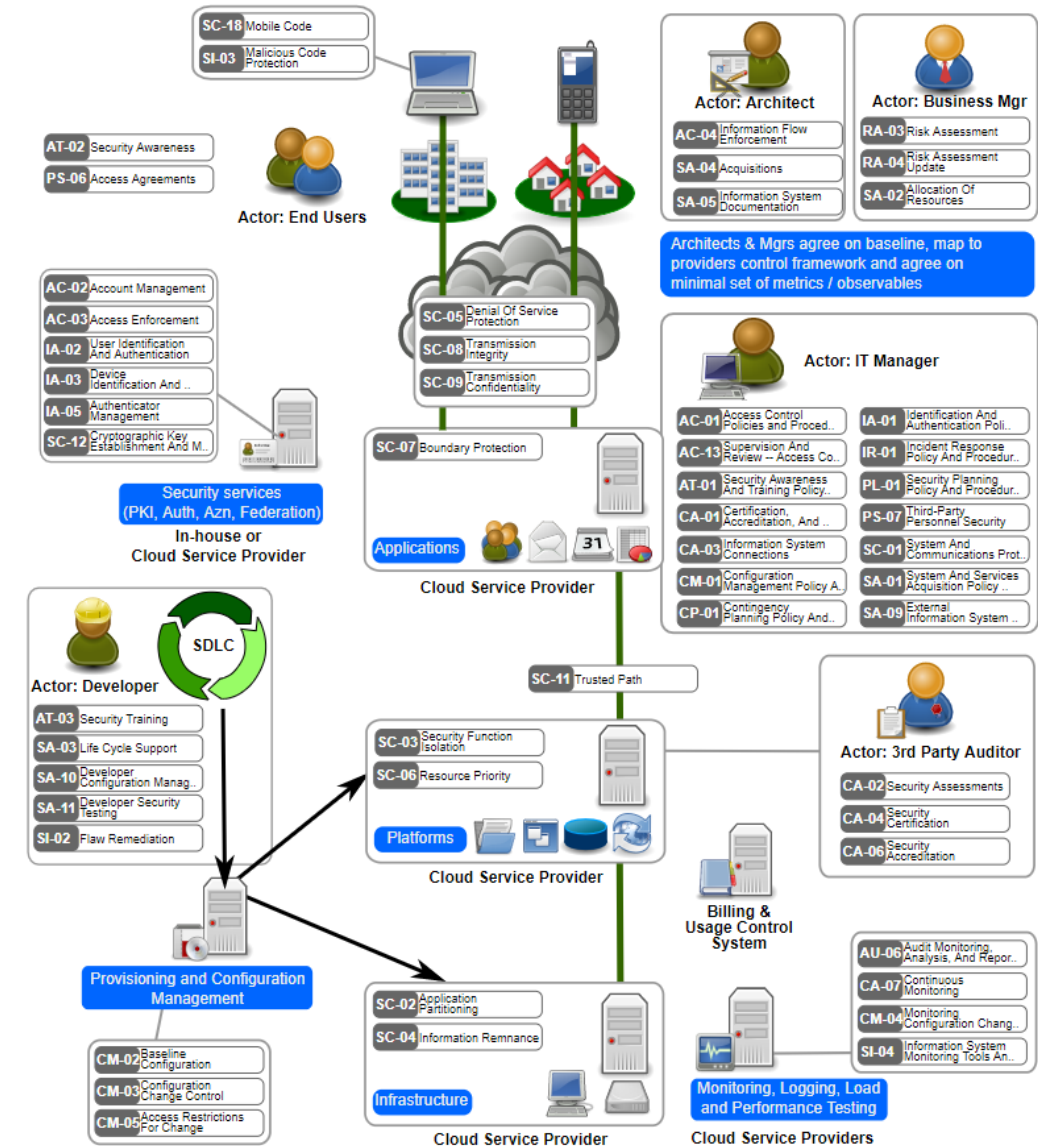
- I like the Open Security Architecture pattern for Cloud Computing

Ref -

<https://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing>

## SP-011: Cloud Computing Pattern

Diagram:





# Cloud Specific (cont.)

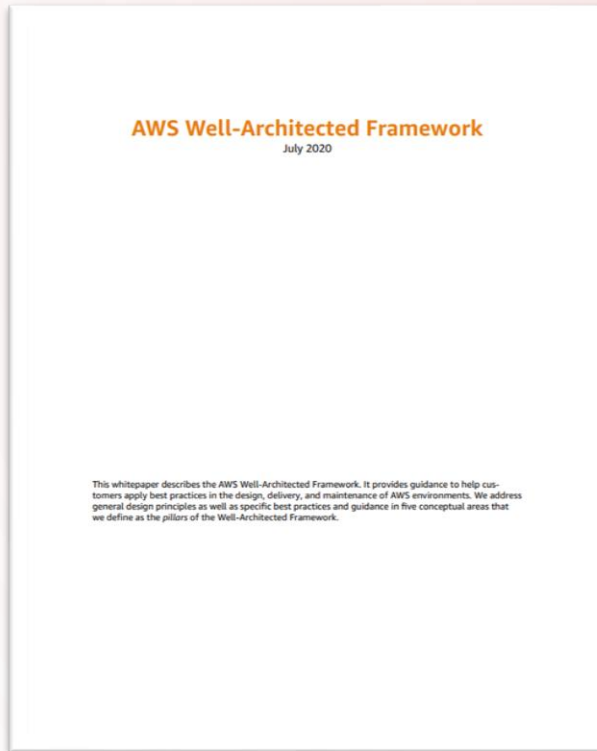
## Cloud Security Alliance – Treacherous 12

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues

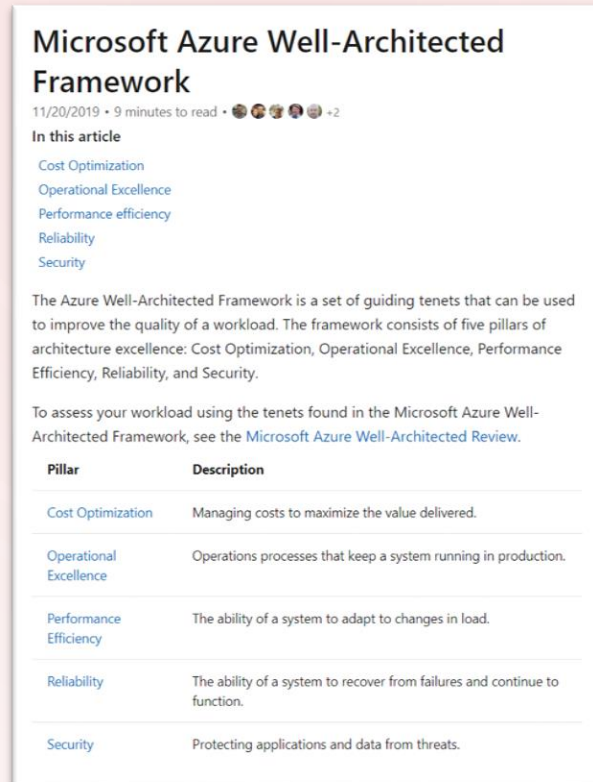
Ref - <https://cloudsecurityalliance.org/artifacts/the-treacherous-twelve-cloud-computing-top-threats-in-2016/>



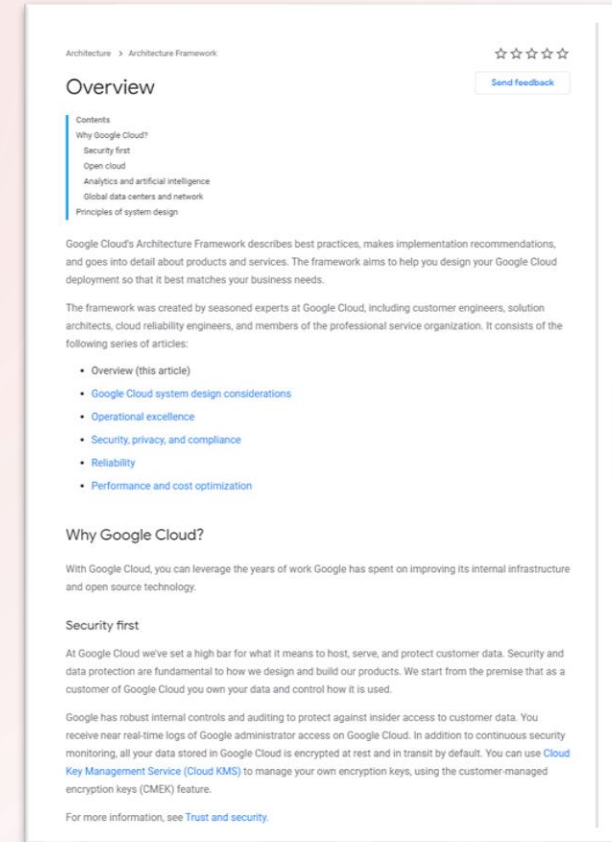
# Cloud Specific (cont.)



<https://aws.amazon.com/architecture/well-architected/>



<https://docs.microsoft.com/en-us/azure/architecture/framework/>



<https://cloud.google.com/architecture/framework>



# FRAMEWORKS

---

*NIST CSF*

*AESCSF*

# NIST Cyber Security Framework

- First released in 2015, V1.1 released in 2018 – one of the main additions in v1.1 was the addition of Cyber Security Supply Chain Management
- Has 5 Functions, 23 Categories and 142 Sub-Categories



Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

# NIST Cyber Security Framework (CSF) (cont.)

- The NIST CSF is a document that is designed to bind together many other cyber security standards and references, it maps it's sub categories to the following informative references:
  - Centre for Internet Security (CIS) – Critical Security Controls (CSC) (Formally the SANS Top 20)
  - COBIT 5 – ISACA
  - ISA 62443 – A highly regarded cyber security standard for Industrial Control Systems
  - ISO 27001 – A well regarded Information Security Management System standard which a system/organization can be accredited against
  - NIST SP 800-53 – US Government Federal Standard regarding Information Security Controls

# NIST Cyber Security Framework (CSF) cont.

Function	Category	Subcategory
IDENTIFY (ID)	<b>Business Environment (ID.BE):</b> <i>The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</i>	<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated
	<b>Supply Chain Risk Management (ID.SC):</b> <i>The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</i>	<b>ID.SC-1:</b> Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
		<b>ID.SC-2:</b> Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
		<b>ID.SC-3:</b> Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
		<b>ID.SC-4:</b> Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
		<b>ID.SC-5:</b> Response and recovery planning and testing are conducted with suppliers and third-party providers

# Australian Energy Sector Cyber Security Framework (AESCSF)<sup>#</sup>

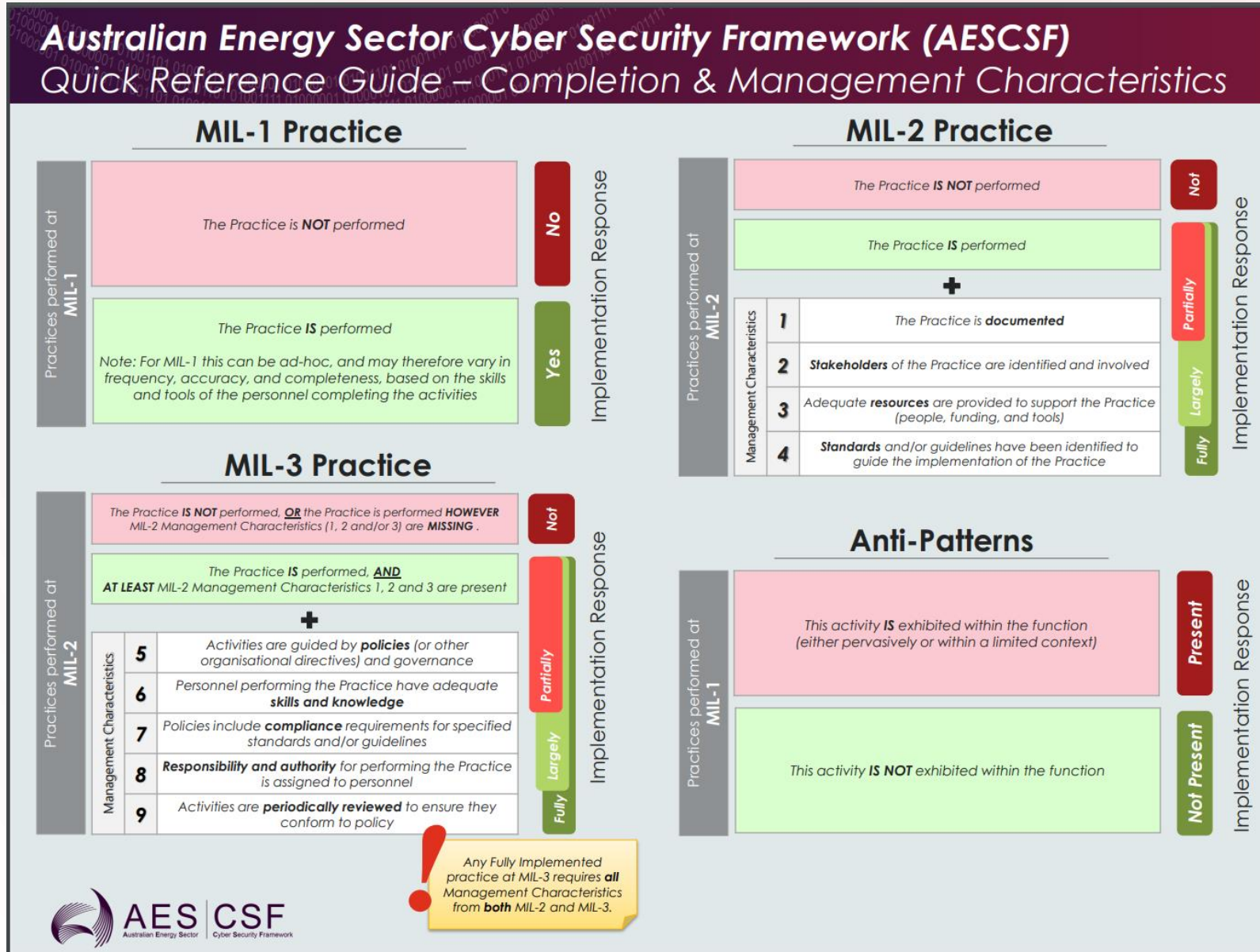
- Led by the Australian Energy Market Operator (AEMO) but developed in collaboration with the Australian Electricity Industry – it is based off the US Dept of Energy – Electricity Subsector – Cyber Security Capability Maturity Model (US DoE – ES-C2M2)<sup>&</sup>
- Has the concept of a Maturity Indicator Level (MIL) – from 1 to 3
- Of the 11 domains, one is the Supply Chain and External Dependency Management (EDM) which has two objectives:
  - EDM-1 - Identify Dependencies
  - EDM-2 - Manage Dependency Risk

<sup>#</sup><https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources>

<sup>&</sup><https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1>



# AESCSF (cont.) – Management Characteristics




**AES CSF**  
Australian Energy Sector Cyber Security Framework

Any Fully Implemented practice at MIL-3 requires **all** Management Characteristics from **both** MIL-2 and MIL-3.

# AESCSF (cont.) – Framework Core

A	B	C	D	E	F	G	H	I	J	K
Domain	Objective ID	Objective	Maturity Indicator Level	Security Profile	Practice ID	Practice	Context and Guidance	Australian References	NIST CSF Subcategory	Informative References
<b>ACM: Asset, Change and Configuration Management</b>										
ACM-1: Manage Asset Inventory										
ACM-2: Manage Asset Configuration										
ACM-3: Manage Changes to Assets										
ACM-AP: Anti-Patterns										
<b>CPM: Cyber Security Program Management</b>										
CPM-1: Establish Cyber Security Program Strategy										
CPM-2: Sponsor Cyber Security Program										
CPM-3: Establish and Maintain Cyber Security Architecture										
CPM-4: Perform Secure Software Development										
CPM-AP: Anti-Patterns										
<b>EDM: Supply Chain and External Dependencies Management</b>										
<b>EDM-1: Identify Dependencies</b>										
EDM	EDM-1	Identify Dependencies	MIL-1	SP-1	EDM-1A	Important IT and OT supplier dependencies are identified (i.e., external parties on which the delivery of the function depend, including operating partners), at least in an ad hoc manner	Are you aware of any external vendors who the organisation is dependant on for the management, operation or support of business-critical IT or OT systems?	N/A - No Australian References identified for this practice.	ID-AM-4: External information systems are catalogued ID-BE-4: Dependencies and critical functions for delivery of critical services are established	CIS CSC (v7.1) 12 COBIT 5 APO02.02, APO10.04, DSS01.02 COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
EDM	EDM-1	Identify Dependencies	MIL-1	SP-1	EDM-1B	Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function including operating partners), at least in an ad hoc manner	Are you aware of any external parties who are heavily dependent on your organisation? Examples may include critical energy customers, telecommunications networks, organisations which co-locate equipment in your data centre, etc.	N/A - No Australian References identified for this practice.	ID-BE-1: The organization's role in the supply chain is identified and communicated ID-BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 CP-2, SA-12 NIST SP 800-53 Rev. 4 PM-8
EDM	EDM-1	Identify Dependencies	MIL-2	SP-2	EDM-1C	Supplier dependencies are identified according to established criteria	Have you established specific criteria by which you can identify external vendors who the organisation is dependant on for the management, operation or support of business-critical IT or OT systems?  This activity is commonly performed within an organisation's Vendor/Category Management function.  EDM-1a must be completed as a pre-requisite for this practice.	N/A - No Australian References identified for this practice.	ID-AM-4: External information systems are catalogued ID-BE-4: Dependencies and critical functions for delivery of critical services are established	CIS CSC (v7.1) 12 COBIT 5 APO02.02, APO10.04, DSS01.02 COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14



# AESCSF (cont.) - EDM-1 - Identify Dependencies

## MIL-1

- EDM-1A - *Important IT and OT supplier dependencies are identified (i.e., external parties on which the delivery of the function depend, including operating partners), at least in an ad hoc manner*
- EDM-1B - *Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function including operating partners), at least in an ad hoc manner*

## MIL-2

- EDM-1C - *Supplier dependencies are identified according to established criteria*
- EDM-1C - *Customer dependencies are identified according to established criteria*
- EDM-1E - *Single-source and other essential dependencies are identified*
- EDM-1F - *Dependencies are prioritized*

## MIL-3

- EDM-1G - *Dependency prioritisation and identification are based on the function's or organisation's risk criteria (RM-1c).*

# AESCSF (cont.) - EDM-2 - Manage Dependency Risk

## MIL-1

- EDM-2A - Significant Cyber Security risks due to suppliers and other dependencies are identified and addressed, at least in an ad hoc manner
- EDM-2B - Cyber Security requirements are considered, at least in an ad hoc manner, when establishing relationships with suppliers and other third parties

## MIL-2

- EDM-2C - Identified Cyber Security dependency risks are entered into the risk register (RM-2j)

- EDM-2D - Contracts and agreements with third parties incorporate sharing of Cyber Security threat information
- EDM-2E - Cyber Security requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate
- EDM-2F - Agreements with suppliers and other external entities include Cyber Security requirements
- EDM-2G - Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet Cyber Security requirements.

# AESCSF (cont.) - EDM-2 - Manage Dependency Risk

## MIL-2 (cont.)

- EDM-2H - *Agreements with suppliers require notification of Cyber Security incidents related to the delivery of the product or service*
- EDM-2I - *Suppliers and other external entities are periodically reviewed for their ability to continually meet the Cyber Security requirements*

## MIL-3

- EDM-2J - *Cyber Security risks due to external dependencies are managed according to the organisation's risk management criteria and process*

- EDM-2K - *Cyber Security requirements are established for supplier dependencies based on the organisation's risk criteria (RM-1 c)*
- EDM-2L - *Agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended life cycle of delivered products*
- EDM-2M - *Acceptance testing of procured assets includes testing for Cyber Security requirements*
- EDM-2N - *Information sources are monitored to identify and avoid supply chain threats (e.g., counterfeit parts, software, and services).*

A decorative graphic on the left side of the slide consisting of dark red lines that resemble a circuit board or a stylized tree. These lines branch out and terminate in small white circles. The background of the slide features a series of concentric, light-colored circles that create a subtle ripple effect.

# OTHER RESOURCES

# CISA – Cyber Security Procurement Language

## Department of Homeland Security: Cyber Security Procurement Language for Control Systems

*September 2009*



Control Systems Security Program  
National Cyber Security Division



### Topics the document addresses:

- System Hardening
- Perimeter Protection
- Account Management
- Coding Practices
- Flaw Remediation
- Malware Detection and Protection
- Hostname Resolution
- End Devices
- Remote Access
- Physical Security
- Network Partitioning
- Wireless Technologies

### The document defines for each Topic, Sub Topic the template addresses:

- Basis
- Language Guidance
- Procurement Language
- Factory Acceptance Test (FAT) Measures
- Site Access Test (SAT) Measures
- Maintenance Guide
- References
- Dependencies



# CISA – Cyber Security Procurement Language (cont.)

## 2. SYSTEM HARDENING

System hardening refers to making changes to the default configuration of a network operating system (OS), software applications, and required third-party software to reduce vulnerabilities.

### 2.1 Removal of Unnecessary Services and Programs

Unnecessary services and programs are often installed on network devices.

#### 2.1.1 Basis

Unused services in a host operating system that are left enabled are possible entry points on the network and are generally not monitored because these services are not used. Only used for control systems operation and maintenance shall be enabled to limit possible entry

#### 2.1.2 Language Guidance

Often, networked devices ship with a variety of services enabled and default operating programs/utilities pre-installed. These range from system diagnostics to chat programs, some have well-known vulnerabilities. Various attacks have been crafted to exploit these services, information leading to compromise the system.

Any program that offers a network service that “listens” on specific addresses for connection requests. On a Transmission Control Protocol (TCP)/Internet Protocol (IP) network, this combination of IP address and TCP or User Datagram Protocol (UDP) ports. A recommended activity is simply disabling or removing any services or programs, which are not required for system operation, thus removing potential vulnerabilities.

Port scans are the normal method of ensuring existence of required services and absence of unnecessary services. A port scan shall be run before the FAT with a representative, fully functional system configuration. All input/output (I/O) ports need to be scanned for UDP and TCP. The scan shall be run before the FAT and again prior to the SAT. Port scans can rarely be used on production systems, scanners will disrupt operations.

#### 2.1.3 Procurement Language

Post-contract award, the Vendor shall provide documentation detailing all application system services, scripts, configuration files, databases, and all other software required and configurations, including revisions and/or patch levels for each of the computer systems and the control system.

The Vendor shall provide a listing of services required for any computer system running applications or required to interface the control system applications. The listing shall include ports and services required for normal operation as well as any other ports and services required for emergency operation. The listing shall also include an explanation or cross reference to justify why each service is necessary for operation.

The Vendor shall verify and provide documentation that all services are patched to current levels.

The Vendor shall provide, within a pre-negotiated period, appropriate software and services or workarounds to mitigate all vulnerabilities associated with the product and to maintain an established level of system security.

operation and maintenance of the control system prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but not be limited to:

1. Games
2. Device drivers for network devices not delivered
3. Messaging services (e.g., MSN, AOL IM)
4. Servers or clients for unused Internet services
5. Software compilers in all user workstations and servers except for development workstations and servers
6. Software compilers for languages that are not used in the control system
7. Unused networking and communications protocols
8. Unused administrative utilities, diagnostics, network management utilities
9. Backups of files, databases, and programs used only during development
10. All unused data and configuration files
11. Sample programs and scripts
12. Unused document processing utilities (Microsoft Word, OpenOffice, etc.).

#### 2.1.4 FAT Measures

The Vendor shall verify that the Purchaser requires the Vendor to perform a vulnerability and active port scan, with the most current signature files, before the FAT. This assessment is then compared to the current patching status, and documentation, to validate this requirement.

1. The Vendor shall provide for each networked device or component (e.g., switch) the following configuration documentation lists:
  - a. Network services required for the operation of the device (e.g., TCP and UDP) and port range
  - b. Dependencies on underlying operating system services
  - c. Dependencies on networked services residing on other devices
  - d. All the software configuration parameters required for the device
  - e. Certified OS, driver, and other software versions installed
  - f. Results found by the vulnerability scans with mitigation measures
2. The Vendor shall install firmware updates available for the device from the system manufacturer at the time of installation and provide documentation of the updates.
3. The Vendor shall provide a summary table indicating each device's patching status. Include the following information in this table:
  - a. Product Disclaimer  
References herein to any specific commercial product, process, or service, whether or not otherwise, does not necessarily constitute or imply its endorsement, approval, or any agency thereof.

- a. Source device name and media access control (MAC) and/or IP address
  - b. Destination device name and MAC and/or IP address
  - c. Protocol (e.g., TCP and UDP) and port or range of ports.
4. The Vendor shall perform network-based validation and documentation steps on each device:
    - a. Full TCP and UDP port scan on Ports 1–65535. This scanning needs to be completed during a simulated “normal system operation.”

#### 2.1.5 SAT Measures

The Vendor shall compare the results of cyber security scans run on the system, as a primary activity of the SAT, with an inventory of the required services, patching status, and required documentation. At the conclusion of the SAT and before cutover or commissioning, the above cyber security scans (with the most current signature files) must be run again.

#### 2.1.6 Maintenance Guidance

Document the system operating system and software patches as the system software evolves to allow traceability and to verify no extra services are reinstalled. Anytime the system is upgraded, it is recommended that system Vendors rerun appropriate subsets of the FAT on the baseline system before delivery to the purchaser.

#### 2.1.7 References

North American Electric Reliability Corporation (NERC) CIP-007-1 R2, “Ports and Services,” Cyber Security—Critical Infrastructure Protection, June 1, 2006.

ANSI/ISA-99.00.01, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Section 5.<sup>1</sup>

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 5.3, B.14, C.3.

National Institute of Standards and Technology (NIST)<sup>1</sup>—Special Publication 800-42, “Guideline on Network Security Testing.”

#### 2.1.8 Dependencies

None. This topic is stand-alone.

## CISA – Cyber Security Procurement Language (cont.)

### Cybersecurity Procurement Language for Energy Delivery Systems

April 2014



Energy Sector Control Systems  
Working Group (ESCSWG)

This document specifies procurement language that focuses on the below systems:

- Supervisory Control and Data Acquisition (SCADA)  
Energy Management Systems EMS
- Distribution Management Systems DMS
- Distributed Control Systems DCS

It addresses:

- General Cybersecurity Procurement Language
- The Suppliers Life Cycle Security Program
- Intrusion Detection
- Physical Security
- Wireless Technology
- Cryptographic System Management



# CISA – Cyber Security Procurement Language (cont.)

## 3. THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM

The Supplier's life cycle security program is an important consideration in the procurement process. Vulnerabilities frequently result from architecture, design, weaknesses, and vulnerabilities in hardware, software, and firmware coding, as well as in bundled third-party products. Many energy delivery system security vulnerabilities are the direct result of writing software with inadequate attention to secure coding practices that reduce the risk of successful deliberate and persistent malicious attacks. Life cycle security programs provide a structured way for developing robust products with fewer weaknesses and vulnerabilities or finding and remediating them before software and systems are delivered and installed in the Acquirer's environment. Supplier post-production support is critical for maintaining secure software and systems, including remediating newly discovered vulnerabilities and ensuring that spare parts can be replaced with genuine parts. Validating that hardware, software, or firmware has been delivered as it was ordered and shipped—without being tampered with or otherwise modified—is also important. After a product has been removed from service, the disposal of that product provides opportunities for the compromise of information and configurations that the Acquirer or Supplier may deem sensitive.

### 3.1 Secure Development Practices

Secure product development practices are a set of processes integrated into the system development life cycle (SDLC) that reduce the security risks of the overall product. These practices help to develop more robust hardware, software, and firmware with fewer weaknesses and vulnerabilities, as well as identify and remediate weaknesses and vulnerabilities before implementation. Secure development practices ensure that security is integrated into all phases of the SDLC and is considered a key component of system development.

Baseline procurement language:

- 3.1.1. The Supplier shall provide summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided energy delivery system hardware, software, and firmware. If applicable, the Supplier shall document how the most critical application security weaknesses (including *OWASP Top 10* or *SANS Top 25 Most Dangerous Software Errors*) are addressed in the Supplier's SDLC.
- 3.1.2. As specified by the Acquirer, the Supplier shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware). The Supplier shall identify the countries where the development, manufacturing, maintenance, and service for the product are provided. The Supplier shall notify the Acquirer of changes in the list of countries where product maintenance or other services are provided in support of the procured product. This notification shall occur within [a negotiated time period] prior to initiating a change in the list of countries.

23

- 3.1.3. The Supplier shall provide a Quality Assurance program and validate that the software and firmware of the procured product have undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities. This testing shall include fuzz testing, static testing, dynamic testing, and penetration testing. The Supplier shall use positive and appropriate negative tests to verify that the procured product operates in accordance with requirements and without extra functionality, as well as monitor for unexpected or undesirable behavior during these tests. This testing may be done by the Supplier or an independent entity. The Supplier shall provide summary documentation of the results of the testing that includes unresolved vulnerabilities and recommended mitigation measures.
- 3.1.4. The Supplier shall provide summary documentation of its coding reviews, including defect lists and plans to correct identified vulnerabilities.
- 3.1.5. The Supplier shall communicate security-related technical issues with a single technical point of contact (e.g., a company support email address or a company support phone number), as specified by the Acquirer. The Supplier shall communicate with the Acquirer within [a negotiated time period] (see Section 3.3.3). This is not intended for non-technical contract-related issues.
- 3.1.6. The Supplier shall provide documentation of all input validation testing including, but not limited to, measures for prevention of command injection, Structured Query Language (SQL) injection, directory traversal, Remote File Include, Cross-Site Scripting (XSS), and buffer overflow.
- 3.1.7. The Supplier shall provide a contingency plan for sustaining the security of the procured product in the event the Supplier leaves the business (e.g., security-related procedures and products placed in escrow).
- 3.1.8. The Acquirer shall have the right to request documentation of the Supplier's implemented cybersecurity program, including recent assessment results or conduct periodic [at a negotiated frequency and scope] on-site security assessments at the Supplier's facilities. These on-site security assessments may be conducted by an independent third party, at the discretion of the Acquirer.

### 3.2 Documentation and Tracking of Vulnerabilities

When security vulnerabilities are discovered in hardware, software, and firmware, the timely application of corrective actions and/or mitigation steps can reduce the likelihood that adversaries will be able to exploit these vulnerabilities in energy delivery systems. Some of these vulnerabilities may be publicly disclosed before the Supplier can develop remedies; others may be kept from disclosure until remedies are available.

Security breaches may also affect the cybersecurity of the procured product. Such breaches may involve a compromise of security involving the Supplier's organization, or any organization involved in the product's supply chain. Security breaches may result in the loss of sensitive product design

24





# NEXT STEPS

---

*YOUR NEXT  
PROJECT*

*WHOLE OF  
ORGANISATION*

# Next Steps

## Next Week

1. Download the ACSC Cyber Security Supply Chain Risk Management Materials
2. Download the NIST CSF
3. Download the AESCSF Materials
4. Read the materials and get used to the concepts and content

## Next Month

1. Organise a meeting with your internal Security Team about your company's Cyber Security Supply Chain Strategy
2. Organise a meeting with your company's security team and company's procurement team to discuss how to approach the process for upcoming projects and how to approach embedding it into your enterprise procurement processes

## Next 2 – 6 Months

1. Build a process for any new projects to ensure Cyber Security Supply Chain Management is considered through the Systems Life Cycle
2. Work with your Security and Procurement contacts to enable your uplift project



Q&A!

*THANK  
YOU!*

@beLarge

<https://github.com/belarge>