

# Supplier Sharing Virtual Workshop

November 7, 2023

**Open Distribution for Supply Chain Materials**

Copyright © 2023 North American Transmission Forum (“NATF”). All rights reserved. Presentations are provided with the presenter’s permission for distribution.

**No Representations or Warranty**

The NATF makes no and hereby disclaims all representations or warranties (express or implied) relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF or NATF members for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use. Further, no liability is assumed for any presentation materials, artwork or photographs used in presentations not developed by NATF.

# Guidelines for this workshop/seminar

- This is an NATF open virtual workshop/seminar
  - Notice of the webinar was distributed beyond the NATF membership
  - Attendees include individuals not in the NATF membership
    - Do not share NATF confidential information
  - May include members of the press or media
- All attendees
  - Obey anti-trust laws and guidelines; avoid conduct that unreasonably restrains competition
  - Adhere to your organization's standards of conduct regarding sharing of any non-public transmission information
  - Respect and do not share intellectual property unless authorized

# Please Participate

- Raise your hand
  - We will unmute you
  - Make sure you are identified in the participant list
- Put a question or comment in the chat
- Put a question or comment in the Q&A

*If you put a question or comment in the chat or Q&A but want to remain anonymous, please open with your request*



Tom Galloway

NATF President and CEO

# Opening Remarks

Tom Galloway,  
NATF President and CEO

# Purpose of the NATF Supplier Sharing Activities

- Provide an opportunity for suppliers to talk about cyber security issues and practices ranging from
  - How establish a security program to
  - In-depth discussions on a specific technical challenge
- Leverage knowledge from lessons learned
- Share information
- Calls will be limited to suppliers unless otherwise noted

# Contributing Organizations

- Aspen Technology / OSI
- Hitachi Energy
- International Society of Automation (ISA)
- National Electrical Manufacturers Association (NEMA)
- Schneider Electric
- Schweitzer Engineering Laboratories (SEL)
- Siemens
- Siemens Energy
- US Chamber of Commerce
- With support from:
  - Nebraska Public Power District
  - Southern Company
  - North American Transmission Forum (NATF)

# Agenda and Today's Presenters

- Streamlining Supply Chain Risk Management with Customers

Frank Harrill, VP, Security Schweitzer Engineering (SEL)

- Managing Software Bills of Materials and Inventories of Software Components

Andre Ristaino, Managing Director, Global Consortia, Conformity Assessment, International Society of Automation (ISA)

Dmitry Raidman, CTO, Cybeats

Gonda Lamberink, VP of Sales, Cybeats

Chris Blask, VP of Strategy, Cybeats

- Break (15 min)

- Leveraging Certifications

Andy Turke, Siemens Industry, Inc.

Andre Ristaino, Managing Director, Global Consortia, Conformity Assessment, International Society of Automation (ISA)

- Cloud Security

Kristine Martz, Industry Specialist – Energy & Utilities, Amazon Web Services

# Streamlining Supply Chain Risk Management with Customers

Frank Harrill  
VP, Security Schweitzer Engineering (SEL)





# Streamlining Supply Chain Risk Management with Customers

Frank Harrill  
SEL Vice President of Security

November 7, 2023

CIP-013 requires an entity to create, implement, and periodically review an effective process to identify and assess cybersecurity risks to the Bulk Electric System from vendor products and services

---



An industry has formed  
around cybersecurity  
vetting and verification



**FORTRESS**  
Critical Infrastructure. Secured.

**ProcessUnity** 

**KY3P<sup>®</sup>**

**S&P Global**

Cyber  **GRX**

**thirdpartytrust** 

  
**venminder**

800 Search Company or Domain Application

Company Details for Reports

BitSight Security Rating  
[About Rating](#)

800

ADVANCED

Rating Related Risk

Ransomware Incidents vs a < 750 company

Source

Half as Likely

Data Breach Incidents vs a < 700 company

Source

Half as Likely

Company Info

S  
d  
s!

+ more

Subscription **Total Risk Monitoring**

Relationship **My Company**

Monitored by **33 companies**

Homepage

Industry **Manufacturing**

IP addresses **1,496**

Searched by **1,028 users**

Company ID

# External Surface Assessments

UpGuard Security Rating Company info Website

A 931 / 950

UpGuard's Cyber Security Ratings range from 0 to 950. The higher the score, the better the security practices on the primary domain for Schweitzer Engineering Laboratories.

Company	
Employees	5,000
Location	United States
CEO	

SecurityScorecard All Search companies, scorecards, portfolios and tags...

Dashboard Portfolio My Scorecard Marketplace Attack Surface (ASI) Reporting Center

A 99

+1Δ

Improve Score

Energy · 53 followers

No artifacts shared

# External Surface Quick Looks

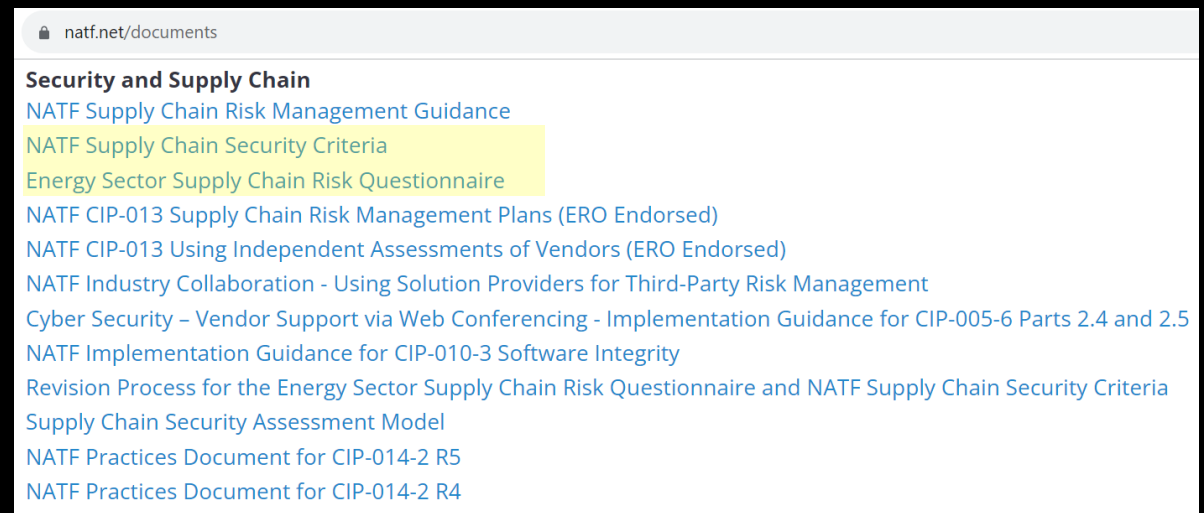
[https://securityscorecard.com/security-rating/\\_\\_\\_\\_\\_.com](https://securityscorecard.com/security-rating/_____.com)

<https://www.upguard.com/webscan>

---

The NATF with cross-industry collaboration created and curates two supply chain risk assessment instruments:

- The Criteria
  - The Questionnaire
- 



# The NATF criteria is mapped to a variety of standards and frameworks

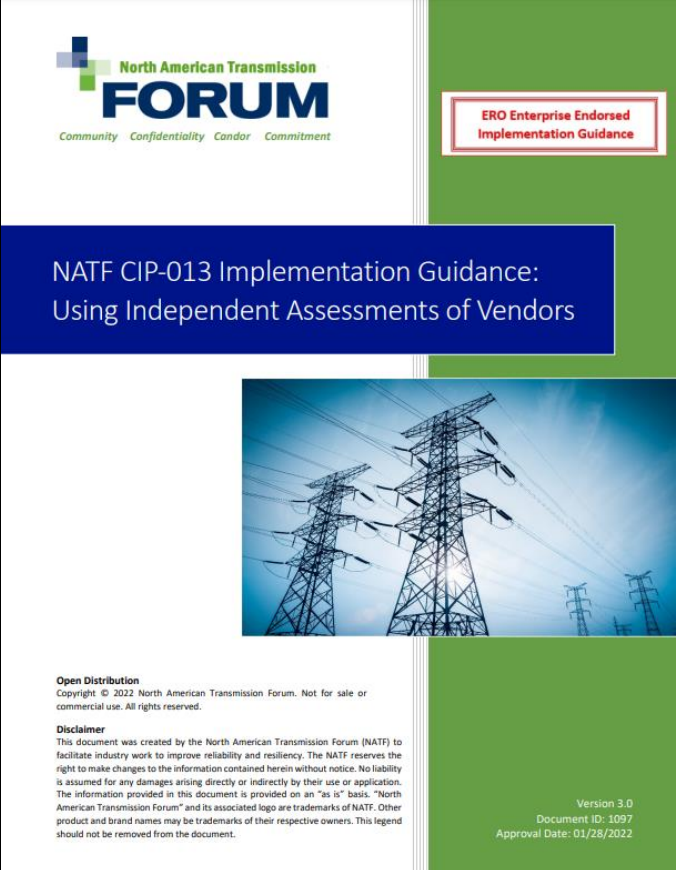
Open Distribution

Copyright © 2023 North American Transmission Forum, Inc.

Criteria Identification Number	Risk Area	NATF Supply Chain Security Criteria	Required by NERC Reliability Standards?		Mapping to Existing Frameworks						
			Good security practices; exceeds NERC CIP Standards' requirements	CIP-013	NIST			IEC 62443	ISO 27001	SOC 2 / SOC for Supply Chain / SOC for Cybersecurity	
					NIST SP 800-161	NIST SP 800-53r4	NIST SP 800-171r1	Cybersecurity Framework Version 1.1	62443-1-1:2009 62443-2-1:2010 62443-2-3:2015 62443-2-4:2017 62443-3-1:2009 62443-3-3:2013 62443-4-1:2018 62443-4-2:2019	ISO/IEC 27001:2013	2017 Trust Services Criteria
1	Access Control and Mgmt	Supplier establishes and maintains an identity and access management program that ensures sustainable, secure product manufacturing/development		R1.2.3 R1.2.6	AC-1 - 6 IA Family AC-17 - 20 CM-7 PE-2 - 6 SC-7	AC-1 - 6 IA Family AC-16 - 20 CM-7 PE-2 - 6 PE-9 SC-7		PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-3	2-4 SP.03.01 2-4 SP.03.07 2-4 SP.03.08	A.9.1.1 A.9.4.1	CC5.1 CC6.1 CC6.2 CC6.3 CC6.4 CC6.6 CC6.8
1.1	Access Control and Mgmt	Supplier's organization, including the computing application system, supports multi-factor authentication (e.g., Duo, Google Authenticator, OTP, etc.)									
2	Access Control and Mgmt	Supplier establishes and maintains a program that ensures storage security at supplier's site (e.g. chain of custody)	x		MP-4	AC-16 MP-4		PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-3	2-4 SP.03.10	A.15.1.2	CC5.1 CC5.7 C1.2 C1.3
3	Access Control and Mgmt	Supplier's personnel vetting process allows supplier to share background check criteria and results with entity for confirmation of process or verification of sampled employees	x						2-4 SP.01.04	A.7.1.1	CC1.4
4	Access Control and Mgmt	Supplier has a process that requires supplier to have background checks (e.g. personnel risk assessments) conducted for all of its employees and contractors. Please provide a list of any exempted employees or contractors due to restrictions by country of employment (i.e. by country)  Supplier's process requires supplier to conduct background checks at least every 7 years. If process does not require at least every 7 years, provide frequency that supplier's process requires	x		PS-3	PS-3		PR.AC-1 PR.AC-4 PR.AC-6	2-4 SP.01.04 No mention of min 7 years	A.7.1.1	CC1.4
5	Access Control and Mgmt	Supplier requires approval for access based on need for all employees and contractors with access to supplier's assets and facilities	x		AC-2 AC-3 AC-5 AC-6	AC-2 AC-3 AC-5 AC-6 AC-16		PR.AC-4 PR.PT-3	2-4 SP.01.07	A.9.1.1 A.9.1.2	CC5.1 CC5.4
6	Access Control and Mgmt	Supplier maintains an access list of all individuals with access to supplier's assets, information, and facilities	x		AC-2 AC-3 AC-5 AC-6	AC-2 AC-3 AC-5 AC-6 AC-16		PR.AC-1 PR.AC-4 PR.AC-6	2-4 SP.01.07	A.9.2.1 A.9.2.2	CC5.1 CC5.4 CC5.6 CC6.2 CC6.3 CC6.4
7	Access Control and Mgmt	Supplier conducts an annual review of all individuals' access to supplier's assets, information, and facilities	x		AC-2 IA Family	AC-2 IA Family		PR.AC-1 PR.PT-1 DE.AE-3	2-4 SP.01.07	A.9.2.5 A.15.1.1	CC5.4 CC6.4

Confidentiality Change Log General Information Organizational Information Supplier Criteria Abbreviations and Definitions

NATF guidance endorsed by NERC ERO Enterprise, validates the use of independent assessments of suppliers to satisfy CIP-013 requirements.



The image shows the cover page of a document titled "NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors". The cover features the North American Transmission Forum (NATF) logo in the top left, which includes the text "North American Transmission FORUM" and the tagline "Community Confidentiality Candor Commitment". In the top right, there is a red-bordered box with the text "ERO Enterprise Endorsed Implementation Guidance". The title is displayed in a blue banner across the middle. Below the title is a photograph of high-voltage power transmission towers against a blue sky. At the bottom, there are sections for "Open Distribution" (Copyright © 2022 North American Transmission Forum. Not for sale or commercial use. All rights reserved.), "Disclaimer" (This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.), and version information (Version 3.0, Document ID: 1097, Approval Date: 01/28/2022).

**North American Transmission FORUM**  
Community Confidentiality Candor Commitment

ERO Enterprise Endorsed  
Implementation Guidance

NATF CIP-013 Implementation Guidance:  
Using Independent Assessments of Vendors

**Open Distribution**  
Copyright © 2022 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

**Disclaimer**  
This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Version 3.0  
Document ID: 1097  
Approval Date: 01/28/2022



ISO/IEC 27001

IEC 62443-4-1

Acceptance of the NATF questionnaire or a independently audited certification to internationally recognized standards is becoming a common approach to supplier qualification

---

Questions?

---

# Managing Software Bills of Materials and Inventories of Software Components

# Presenters

- Andre Ristaino, ISA Managing Director, Conformance Programs and Consortia, Conformity Assessment, International Society of Automation (ISA)
- Gonda Lamberink, VP of Sales, Cybeats
- Chris Blask, VP of Strategy, Cybeats
- Dmitry Raidman, CTO, Cybeats

# Agenda

- Introduction
- ISA/IEC 62443 Inventory Requirements
- What is an SBOM vs. Inventory Overview and Status
- Who are the SBOM Creators and Users?
- Use Cases - Zero Trust and how to incorporate it
- What's Next?



# ISA/IEC 62443-4-1 Inventory Requirements

The ISA/IEC 62443-4-1 standard includes a number of supplier requirements for maintaining an 'inventory' of items comprising the component/system. SBOM's are an approach for meeting the inventory requirements. Inventory requirements include:

- Software components
- Hardware components
- Compilers
- Configuration control
- Development and test applications (SUM-1, others)
- Third party and open-source components (SM-9, SM-10, others)

You can scan the ISASecure specification for all of the requirements by downloading it for free using the following link for the ISASecure SDLA-312 document:

- [ISASecure ISA/IEC 62443-4-1 assessment matrix](#)

Open Distribution for Supply Chain Materials



# CYBEATS

## SBOM/VEX Analogy

You wouldn't give your allergic kid a snack with nuts to school! Why would you install vulnerable software in production?

- Allergies
- Food sensitivities
- People want to know what they eat
- Healthy living

Why do people not ask about the ingredients of their devices and software?



# CYBEATS

## What is in an SBOM?

- ✓ Author
- ✓ Supplier Name
- ✓ Software Component Name
- ✓ Software Component Version
- ✓ Dependency Relationship
- ✓ Assembly Timestamp
- ✓ SBOM Generation Tool
- ✓ Component Unique IDs

```
{
  "bomFormat" : "CycloneDX",
  "specVersion" : "1.3",
  "serialNumber" : "urn:uuid:290804a5-75cd-49cd-afeb-366ffab26bac",
  "version" : 1,
  "metadata" : {
    "timestamp" : "2022-04-20T21:04:53Z",
    "tools" : [
      {
        "vendor" : "CycloneDX",
        "name" : "CycloneDX Maven plugin",
        "version" : "2.5.1",
        "hashes" : [
          {
            "alg" : "MD5",
            "content" : "1a5528adfeb75e1fef6264a90a0de94b"
          },
          {
            "alg" : "SHA-1",
            "content" : "bcbf4d76880f8b7b9008bd08fb72454e7f666957"
          },
          {
            "alg" : "SHA-256",
            "content" : "42fc254f37585624de9ed2dd9e1701d44e34cb5856433075afc851f4ae37857e"
          },
          {
            "alg" : "SHA-384",
            "content" : "6dc2adf4e002def6c49f1593f3d490c8ef5de6df77b390f0177ee84637fa9263e6948c0bb8daaef6f352a2f5f06714b6"
          },
          {
            "alg" : "SHA-512",
            "content" :

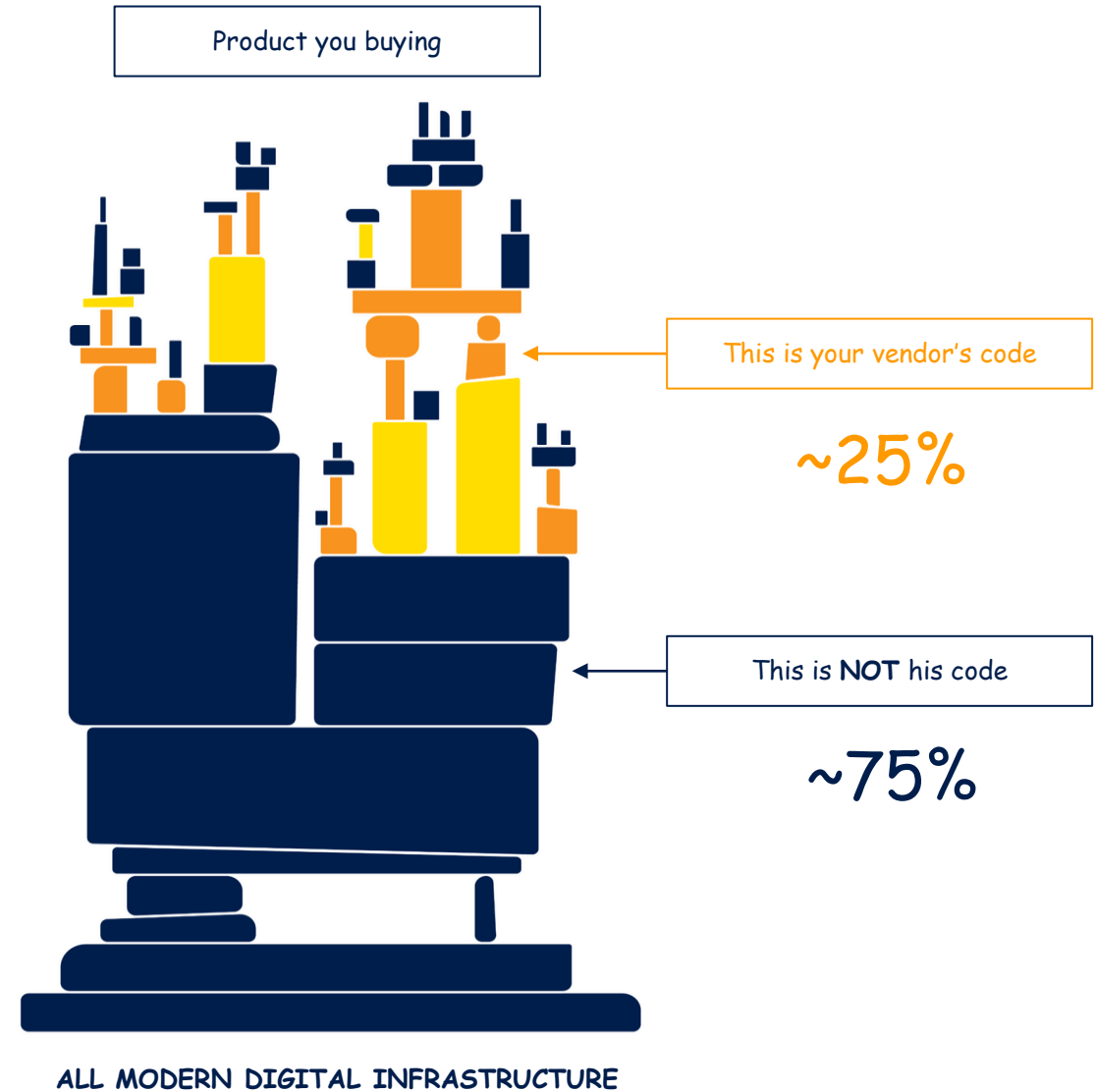
```

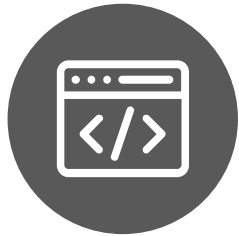
**Action Item:** Ask about components in your software! Through SBOM in SPDX or CycloneDX format.



## You are as secure as the weakest link of your supply chain

Over **90%** of Commercial Applications Contain **Outdated** or **Abandoned** Open Source Software Components

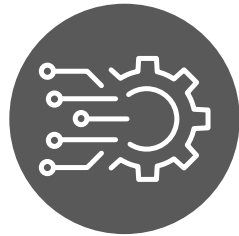




Upstream  
Open  
Source



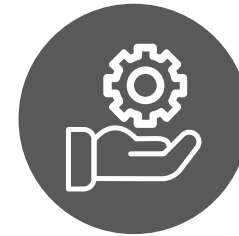
Vendor



Integrator



Regulator



Service  
Provider



Industry  
Association



Private Sector  
Information  
Sharing



Public Sector  
Information  
Sharing



Data Value  
Addition  
Providers



Utility



Utility  
Customers



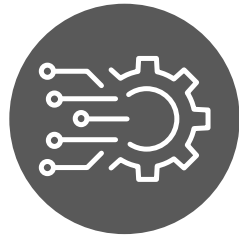
Open source  
Library  
Author

SBOM  
Producer



Firmware  
Author

SBOM  
Distributor



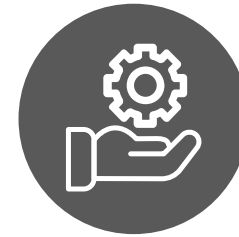
Sub-Assembly  
Manufacturer

SBOM  
Distributor



OEM

SBOM  
Distributor



Integrator

SBOM  
Distributor



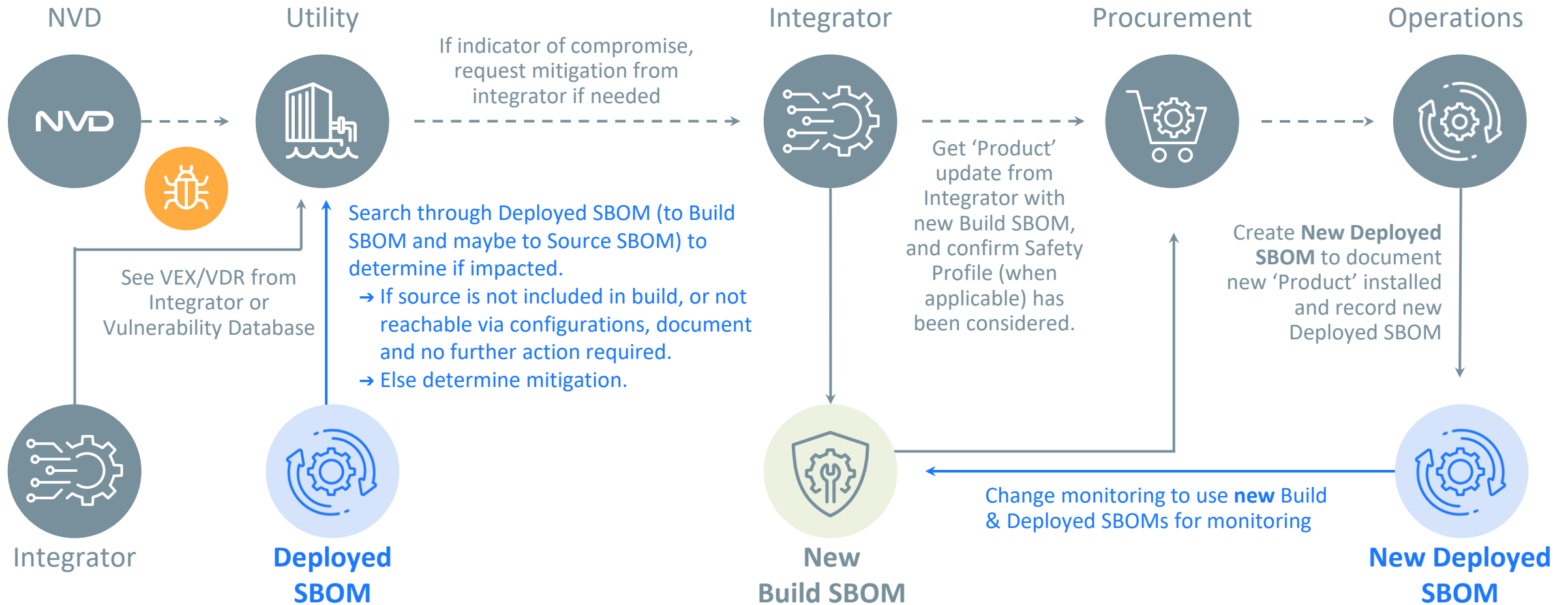
Utility

SBOM  
Consumer

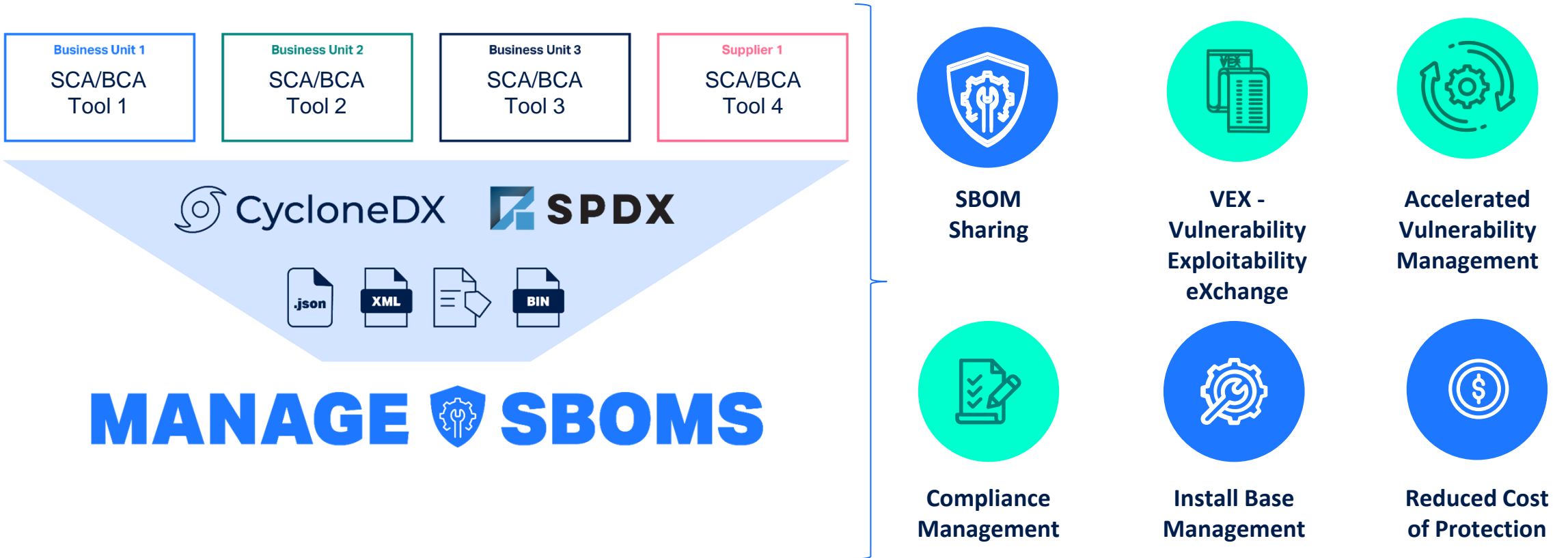
**SBOM Producer:** Actor who creates an SBOM and makes it available.

**SBOM Distributor:** Actor who makes an SBOM available they did not produce.

**SBOM Consumer:** Actor who makes use of an SBOM for a purpose other than making it available.



## What are the SBOM Formats & High-Level Use Cases?





- Do you track due dates for Known Exploited Vulnerabilities by CISA/EPSS?
- Do you understand your device firmware dependencies and their risk in depth?
- Are you aware of Outdated or Abandoned software?
- If there is a new critical vulnerability can you get answers in seconds not in weeks?
- Are you aware of software End of Life, End of Support events?
- Can you collect and observe all the data in one place?
- What would be the effort to perform it continuously?



- Aligning with globally recognized standard instead of a tool or method
- Cross referencing with the asset management data gaining in depth view
- Knowing about dependency vulnerabilities at the same time as the vendor?
- Optimization of MTTD and MTTR for cases like log4j, solarwinds
- Knowing what you have, software asset inventory and transparency
- Better understanding of transitive supply chain
- Vulnerability Assessment from Point In Time to Continuous
- Better Risk insights and faster communication

# CYBEATS The future of BOMs

**2023**

**SBOM**



**2024**

**HBOM**



**2024 - 2025**

**CBOM**





# Thank you!

We meet you  
where you are



# BREAK

Return at 3:05

# Leveraging Certifications

Andy Turke, Cyber Security Officer, Siemens Industry, Inc.

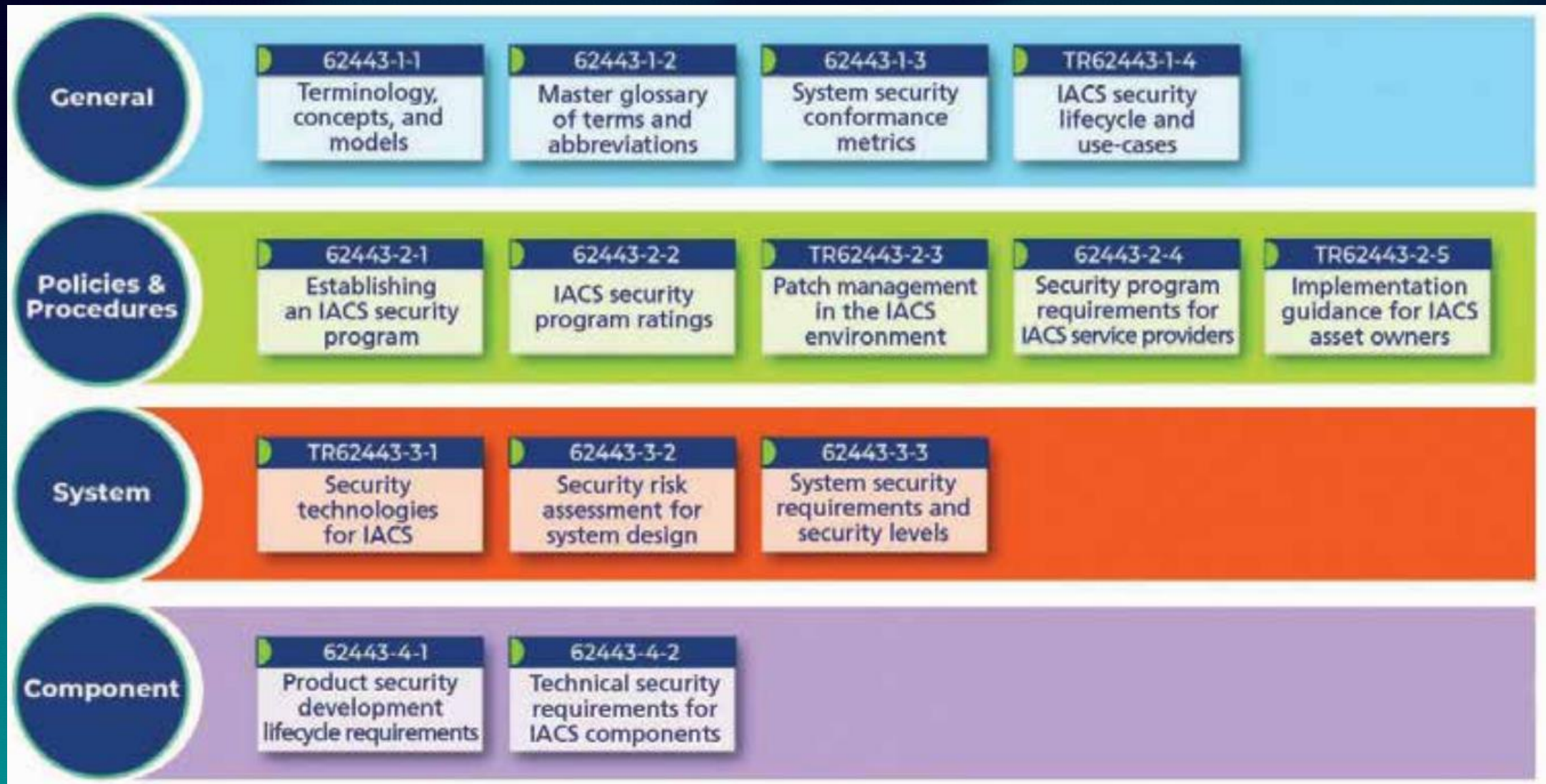
and

Andre Ristaino, Managing Director, Global Consortia,  
Conformity Assessment, International Society of  
Automation (ISA)



*Cybersecurity Certification*  
*ISO 27001 and ISA/IEC 62443*

# ISA/IEC 62443 - Family of Standards







# ISA/IEC 62443 4-1

## Maturity Levels in Product Development Processes

Level	CMMI	62443	Description
1	Initial	Initial	<ul style="list-style-type: none"> <li>• Product development typically ad-hoc and often undocumented</li> <li>• Consistency and repeatability may not be possible</li> </ul>
2	Managed	Managed	<ul style="list-style-type: none"> <li>• Product development managed using written policies</li> <li>• Personnel have expertise and are trained to follow procedures</li> <li>• Processes are defined but some may not be in practice</li> </ul>
3	Defined	Defined (Practiced)	<ul style="list-style-type: none"> <li>• All processes are repeatable across the organization</li> <li>• All processes are in practice with documented evidence</li> </ul>
4	Quantitatively Managed	Improving	<ul style="list-style-type: none"> <li>• CMMI Levels 4 and 5 are combined</li> <li>• Process metrics are used control effectiveness and performance</li> <li>• Continuous improvement</li> </ul>
5	Optimizing		

# ISA/IEC 62443 4-2

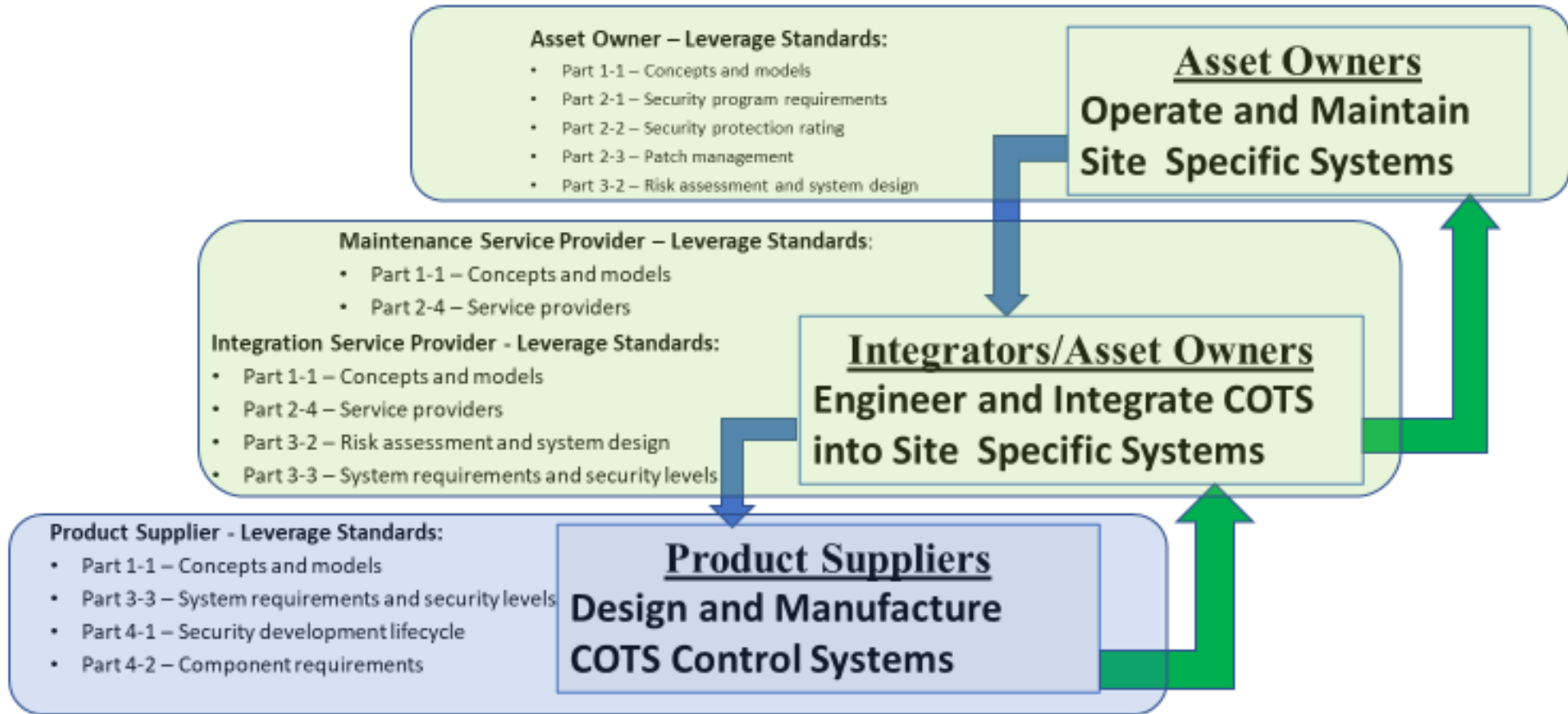
## Security Capability Levels in Automation Components and Systems

 No attack resistance
 Low attack resistance
 Medium attack resistance
 High attack resistance

Security Level	Attack Type			
	Violation type	Means type	Resources level	Motivation
SL-1	Coincidental	N/A	N/A	N/A
SL-2	Intentional	Simple	Low	Low
SL-3	Intentional	Sophisticated	Moderate	Moderate
SL-4	Intentional	Sophisticated	Extended	High

# IEC 62443 Security Standard – Roles based

## ISA/IEC 62443 Automation Security Lifecycle and Shared Stakeholder Responsibility for Cybersecurity

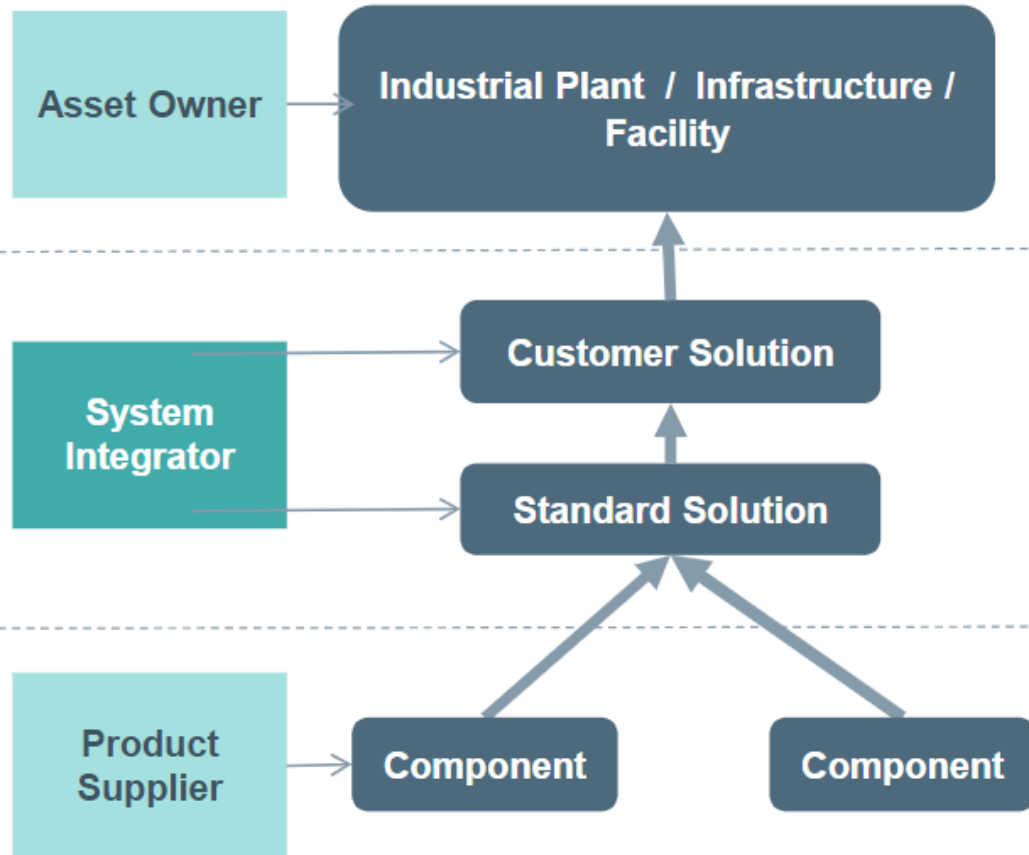




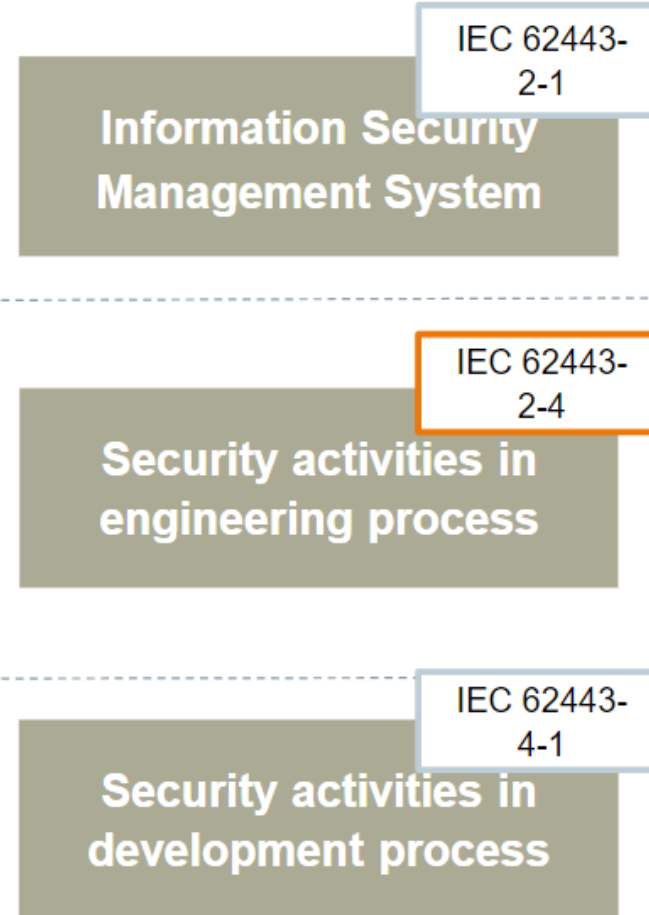
# IEC 62443 Security Standard

- Addresses different roles, their processes and interactions
- Covers full range of technical security measures

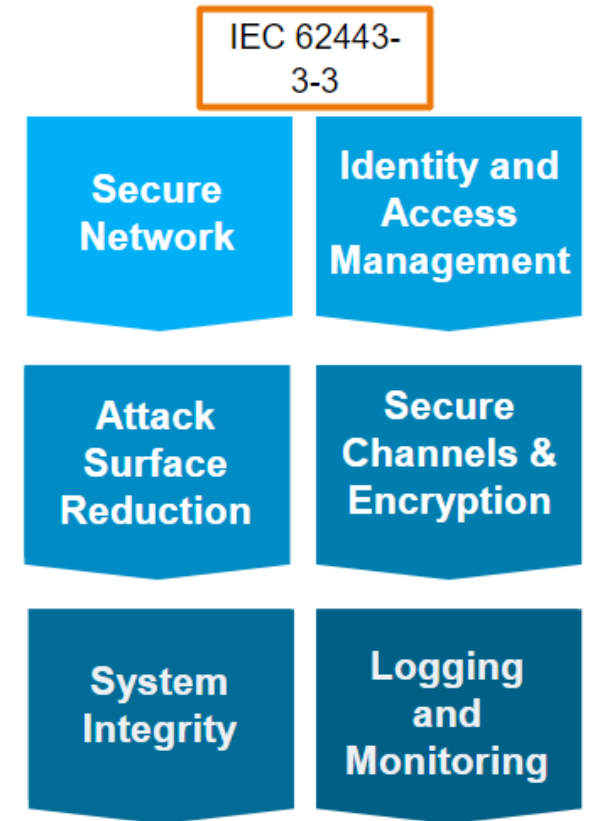
## Roles



## Processes



## Technical security measures



# Benefits of Certification to an international standard

- Automation suppliers sell products globally in many countries. Suppliers seek a single security assessment and certificate of conformance to an international standard. This reduces barriers to trade and reduces supplier's cost with one certification mark that is globally recognized.
- Asset owners with international operations desire to use a single engineering specification and an internationally accepted standard for securing their operations.
- Certification provides transparency about a products security capabilities and assurances that it meets the requirements specified in the published security standards.
- Securing automation ultimately:
  - Reduces risk of endangerment of public or employee safety or health
  - Protects industrial automation and control systems from security breaches
  - Reduces risk of violation of legal or regulatory requirements
  - Advocates a holistic approach - not all risks are technology-based & maintains a security culture
- **ISA 62443 Quick Start Guide:** <https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf>

# Asset Owners use of certifications in security programs (using ISA/IEC 62443 COTS product certifications as an example)

- Have your OT security team study the certification specification to ensure it is applicable to your industry and use-case.
- Ensure that the certification scheme is consistent in applying all requirements from a standard to all products that are assessed (ensures 'apples to apples' comparison of products).
- Be sure to understand what security dimensions the certification covers and what it does not cover
- Add any policy language and/or other requirements not covered in the certification to your procurement document.
- Ensure that the certification specification team included asset owners so that your important requirements are properly represented in the certification specification.
- Ensure that the certification body is ISO 17065 accredited.
- Ensure that the certification has policies and procedures for maintaining the certification over time.
- Include the selected certification in your procurement requirements; for example *ISASecure CSA SAL-2* or *ISASecure CSA SAL-3*

# Standards and Regulation

## Driving Cyber Security in products, solutions, environments

### Following Key-Guidelines

Describing 'What' should be done



NERC



NIST Cyber Security Framework



Cyber Resiliency Act

### Compliant with Key-Standards

Describing 'How' should it be done



ISO/IEC 62443 (System Security)



ISO/IEC 62351 (Communication Security)

ISO/IEC 27001/27019 (Security Management)

### Conform to regulatory requirements

Describing what 'must' be done



Bundesministerium  
des Innern

**IT Security Law**



- Follow industry standard, i.e. bdew
- Report on incidents
- Implementation and Certification of an Information Security Management System (ISMS)
- Cryptographic requirements for Smart Metering



Bundesnetzagentur

**Security Catalogue**



Bundesamt  
für Sicherheit in der  
Informationstechnik



- Assessment and certification of ICS systems

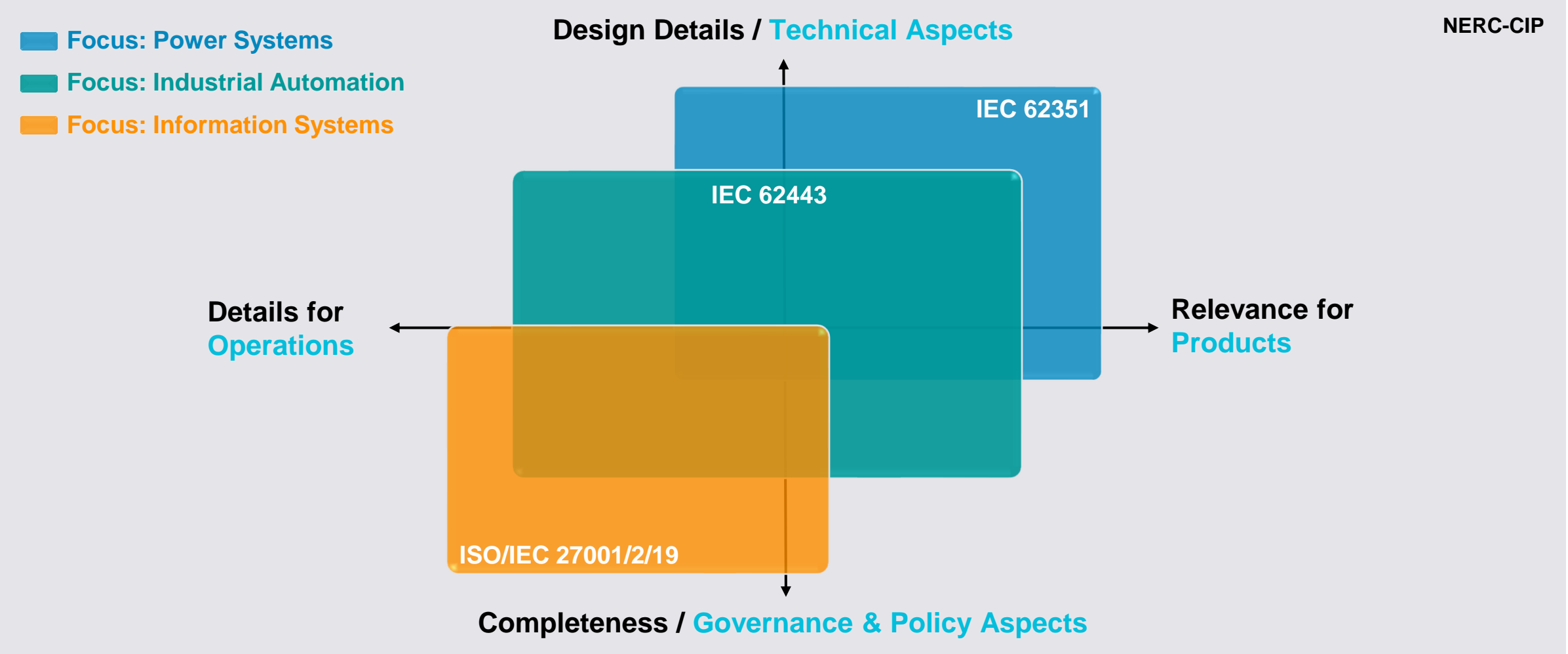


- Auditable compliance (NERC) is required for bulk power systems by regulation



# Standards and Regulation

## Overlapping with different focus areas



# ISO 27001:2022 - Information Security Standard

- ISO/IEC 27001:2022 standard published Oct, 2022. This marks the beginning of the 3-year transition period.
- Last date for initial/re-certification audits according to former ISO 27001:2013 is 18 months after publication of ISO/IEC 27001:2022 (April 2024)
- Transition of existing certificates to ISO/IEC 27001:2022 is 3 years. (October 2025)

# ISO 27001 Annex A Overview

Annex A	Objective
A.5 Information security policies	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
A.6 Organization of information security	To establish a management framework to initiate and control the implementation and operation of information security within the organization.
A.7 Human resource security	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
A.8 Asset management	To identify organizational assets and define appropriate protection responsibilities.
A.9 Access control	To limit access to information and information processing facilities.
A.10 Cryptography	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
A.11 Physical and environmental security	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.
A.12 Operations security	To ensure correct and secure operations of information processing facilities.
A.13 Communications security	To ensure the protection of information in networks and its supporting information processing facilities.
A.14 System acquisition, development and maintenance	To ensure that information security is an integral part of information systems across the entire lifecycle.
A.15 Supplier relationships	To ensure protection of the organization's assets that is accessible by suppliers.
A.16 Information security incident management	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
A.17 Information security aspects of business continuity management	Information security continuity shall be embedded in the organization's business continuity management systems.
A.18 Compliance	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

# ISO 27001:2022

The former 14 clauses of Annex A are now focused on the 4 following topics:

- A.5 Organizational controls (with 37 controls)
- A.6 Personal controls (with 8 controls)
- A.7 Physical controls (with 14 controls )
- A.8 Technical controls (with 34 controls)



# ISO 27001:2022

Annex A of the new ISO/IEC 27001:2022 version includes 93 security controls. The following 11 controls are new:

- A.5.7 Threat Intelligence
- A.5.23 Information security for the use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring
- A.8.9 Configuration management
- A.8.10 Deletion of information
- A.8.11 Data masking
- A.8.12 Data leak prevention
- A.8.16 Activity monitoring
- A.8.23 Web filtering
- A.8.28 Secure coding

# Cybersecurity Program Development Approach

## Current State



Maturity level unknown

Not documented

## Determine Security Posture/Maturity Level



- Perform assessment
  - NIST CSF
  - ISO/IEC 62443
  - NIST800-82
- Identify gaps
- Recommendations

## Develop Security Program



- Develop security strategy
- Develop roadmap
- Provide budget estimation

## Implement Security Program



- Program management of security strategy and project
- Risk management
- Security services planning

## Desired state



- Initial
- Developing
- Defined
- Managed
- Optimized

# | Questions?

# Cloud Security

Kristine Martz

Industry Specialist – Energy & Utilities

Amazon Web Services



# Cloud Security for Energy & Utilities

Kristine Martz (she/her)

Security Industry Specialist, Energy & Utilities

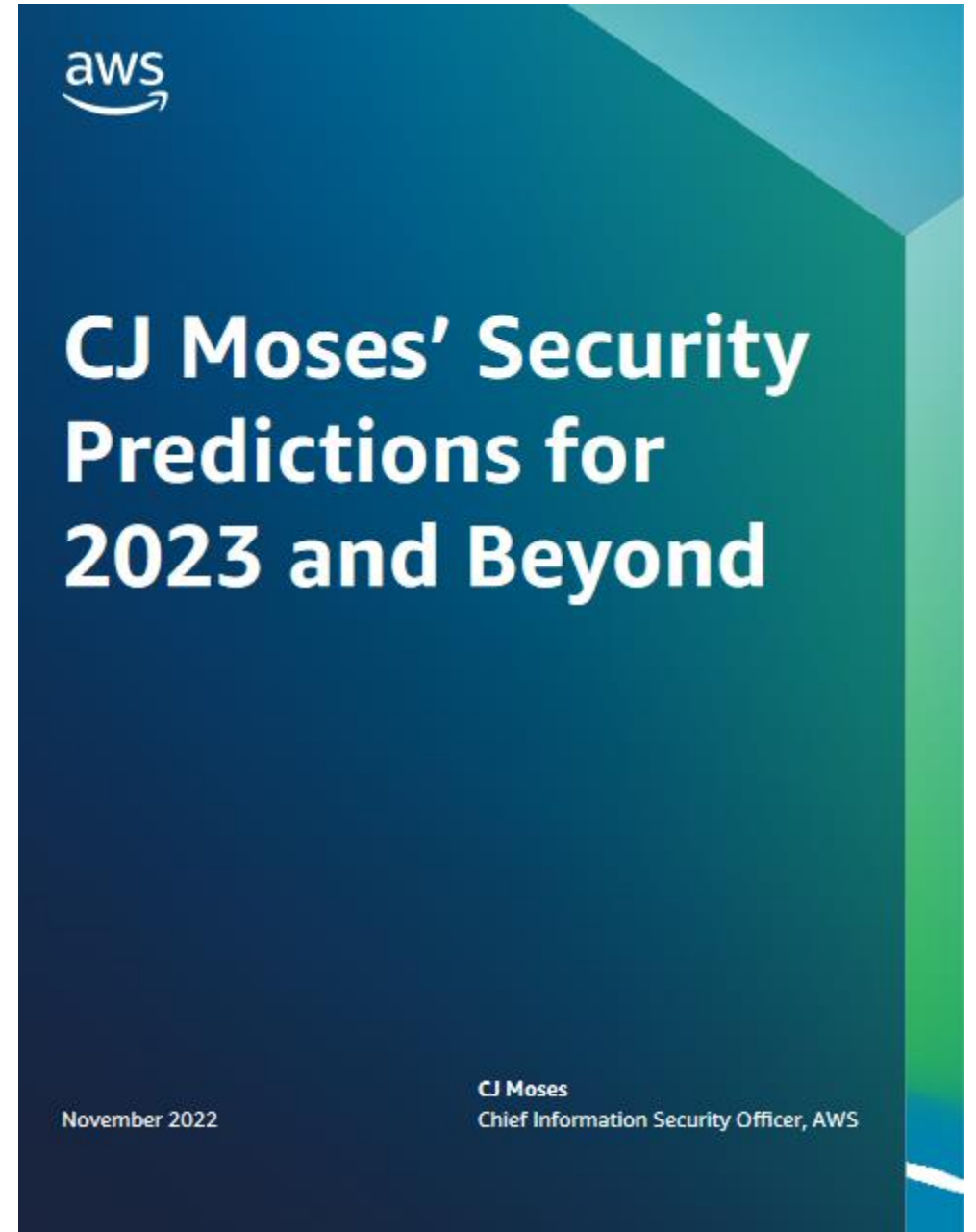
Security Assurance

Amazon Web Services



# AWS CISO Security Predictions for 2023 and Beyond

1. Security Will Be Integral to Everything Organizations Do
2. Diversity Will Help Address the Continued Security Talent Gap
3. Automation Driven by AI/ML Will Enable Stronger Security
4. People Will Drive Greater Data Protection Investment
5. More Advanced Forms of Multi-Factor Authentication Will Become Pervasive
6. Quantum Computing Will Benefit Security



# Energy & Utilities customers face unique risk and regulatory challenges

- In its shift to the cloud, the Energy & Utilities industry is
  - confronting a range of familiar and emerging issues



Constantly evolving regulatory requirements



Requirements that vary significantly across regions



Highly dynamic security threat landscape



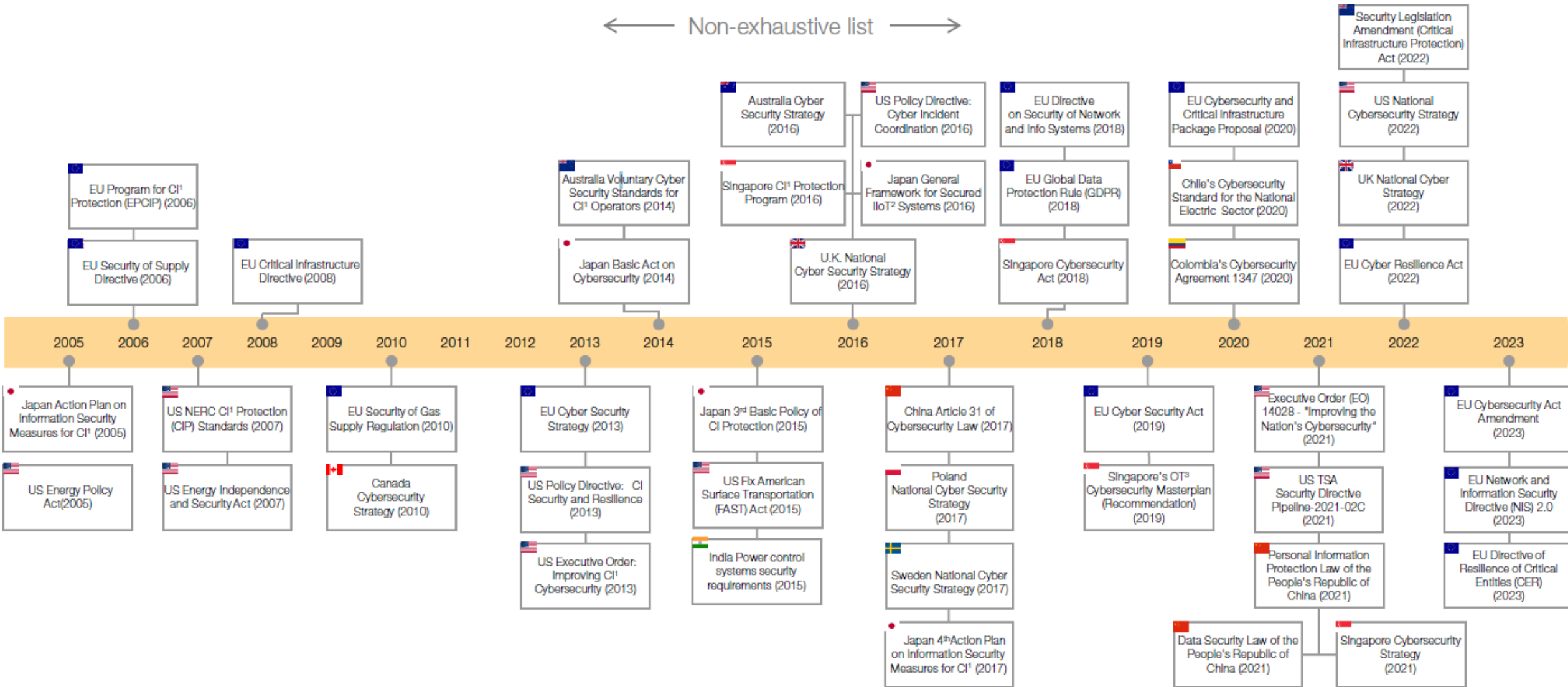
Stringent reporting and documentation requirements



Limited cloud security & compliance specialists

# Rise in Cybersecurity Policies and Regulations

← Non-exhaustive list →





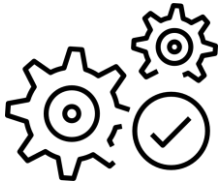
# Customer Questions

- Where is my data when I put it in the cloud?
- Who owns my data in the cloud?
- What resilience does cloud provide?
- How are connected systems protected over the internet?
- How reliable are workloads in the cloud?
- How is my data secured in the cloud?
- What are the latency impacts of failing over to another Region?
- How much time does failover take for hot standby vs cold standby?
- What contingency plans are in place for multi-Region loss of power?



# Tools and guidance to enable compliance

Compliance,  
Security Tools  
& Services



Services and assets to automate controls, collect evidence and manage audits demands

---

Industry  
Frameworks  
and Assets



Deep Industry  
Expertise



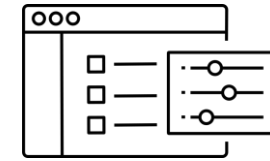
Mechanisms to advocate for and share best practices with customers

---

Regulatory  
Engagement



Terms &  
Conditions



Agreements and third-party audit reports to support energy & utilities compliance objectives

---

Transparency



# We engage with global regulatory bodies on an ongoing basis

## Ongoing engagement with regulators in the U.S. and around the world serves two purposes



### To assess and explain policy

Regulatory policy evaluations to assess the potential impact of regulations

Country-by-country impact assessments to map how energy & utilities customers and partners need to operate

Region- and country-specific compliance guides to document key policy changes and responses








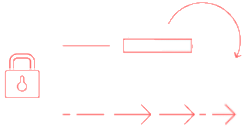
### To share our approach and tools

Educate regulators to help examiners audit AWS environments

Help shape the regulatory landscape to reflect changes in technology

Facilitate dialogue between the industry and its regulators

# AWS security, identity, and compliance solutions

 <p><b>Identity &amp; access management</b></p>	 <p><b>Detection</b></p>	 <p><b>Infrastructure protection</b></p>	 <p><b>Data protection</b></p>	 <p><b>Incident response</b></p>	
<ul style="list-style-type: none"> <li>AWS Identity &amp; Access Management (IAM)</li> <li>AWS Single Sign-On</li> <li>AWS Organizations</li> <li>AWS Directory Service</li> <li>Amazon Cognito</li> <li>AWS Resource Access Manager</li> </ul>	<ul style="list-style-type: none"> <li>AWS Security Hub</li> <li>Amazon GuardDuty</li> <li>Amazon Inspector</li> <li>Amazon CloudWatch</li> <li>AWS Config</li> <li>AWS CloudTrail</li> <li>VPC Flow Logs</li> <li>AWS IoT Device Defender</li> </ul>	<ul style="list-style-type: none"> <li>AWS Firewall Manager</li> <li>AWS Network Firewall</li> <li>AWS Shield</li> <li>AWS WAF – Web application firewall</li> <li>Amazon Virtual Private Cloud (VPC)</li> <li>AWS PrivateLink</li> <li>AWS Systems Manager</li> </ul>	<ul style="list-style-type: none"> <li>Amazon Macie</li> <li>AWS Key Management Service (KMS)</li> <li>AWS CloudHSM</li> <li>AWS Certificate Manager</li> <li>AWS Secrets Manager</li> <li>AWS VPN</li> <li>Server-Side Encryption</li> </ul>	<ul style="list-style-type: none"> <li>Amazon Detective</li> <li>CloudEndure DR</li> <li>AWS Config Rules</li> <li>AWS Lambda</li> </ul>	<ul style="list-style-type: none"> <li>AWS Artifact</li> <li>AWS Audit Manager</li> </ul>

# Inherit global security and compliance

## Certifications / Attestations

C5	DE ✓
Cyber Essentials Plus	GB ✓
DoD SRG	US ✓
FedRAMP	US ✓
FIPS	US ✓
HITRUST	US ✓
IRAP	AU ✓
ISO 9001	🌐 ✓
ISO 27001	🌐 ✓
ISO 27017	🌐 ✓
ISO 27018	🌐 ✓
K-ISMS	KR ✓
MTCS	SG ✓
PCI DSS Level 1	🌐 ✓
SEC Rule 17-a-4(f)	US ✓
SOC 1, SOC 2, SOC 3	🌐 ✓

## Laws / Regulations / Privacy

Argentina Data Privacy	✓
CISPE	EU ✓
EU Model Clauses	EU ✓
FERPA	US ✓
GDPR	EU ✓
GLBA	US ✓
HIPAA	US ✓
HITECH	🌐 ✓
IRS 1075	US ✓
ITAR	US ✓
My Number Act	JP ✓
UK DPA - 1988	GB ✓
VPAT/Section 508	US ✓
Data Protection Directive	EU ✓
Privacy Act [Australia]	AU ✓
Privacy Act [New Zealand]	NZ ✓
PDPA—2010 [Malaysia]	MY ✓
PDPA—2012 [Singapore]	SG ✓
PIPEDA [Canada]	CA ✓
Spanish DPA Authorization	ES ✓
Spanish DPA Authorization	ES ✓

## Alignments / Frameworks

CIS (Center for Internet Security)	🌐 ✓
CJIS (US FBI)	US ✓
CSA (Cloud Security Alliance)	🌐 ✓
ENS High	ES ✓
EU-US Privacy Shield	EU ✓
FFIEC	US ✓
FISC	JP ✓
FISMA	US ✓
G-Cloud	GB ✓
GxP (US FDA CFR 21 Part 11)	US ✓
ICREA	🌐 ✓
IT Grundschutz	DE ✓
MITA 3.0 (US Medicaid)	US ✓
MPAA	US ✓
NIST	US ✓
PHR	US ✓
Uptime Institute Tiers	🌐 ✓
Cloud Security Principles	GB ✓

🌐 = industry or global standard

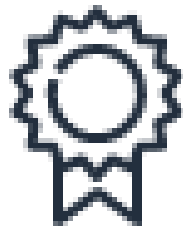
# AWS Partners Lead with Innovation

WE'RE IN THIS TOGETHER



## Innovation

- Innovative Vision
- Innovative Culture
- Structure and tools to innovate



## Expertise

- Cloud Technology
- Cloud Governance
- Training as you Build



## Global Reach

- Drawing on insights from other settings & experience
- Bringing together stakeholders

# Informational Resources

## Energy & Utilities Security Assurance Resources

[The Utility Executive's Guide to Cloud Security](#)

[Utility Executive's Guide to AWS Security](#)

[Control Domains](#)

[Power and Utility Path to Production in the AWS Cloud](#)

[How Dragos Uses AWS to Empower Collective Defense for Industrial](#)

[Control Systems \(ICS\) and Operational Technology \(OT\)](#)

[How energy and utility companies can recover from ransomware and other disasters using infrastructure as code on AWS](#)

[Modernize your Utility's SOC and build better security with Splunk Cloud Platform on AWS](#)

[How to securely extend utility OT data to the cloud](#)

[Is FUD \(Fear, Uncertainty & Doubt\) Holding You Back From Adopting the Cloud?](#)

[Secure and resilient Distribution SCADA on AWS](#)

[Regulatory Developments in the Oil & Gas Pipeline Industry: Digital](#)

[Transformation & OT Cybersecurity Best Practices](#)

[Securing Water Utilities with AWS](#)

## NERC CIP Thought Leadership Resources

[AWS User Guide to Support Compliance with North American Electric Reliability Corporation \(NERC\) Critical Infrastructure Protection \(CIP\) Standards](#)

[Practical Adoption of Cloud Computing in Power Systems—Drivers, Challenges, Guidance, and Real-World Use Cases](#)

[Enabling Security and Resilience with Cloud Technology: AWS Cloud security and architecture for power and utilities](#)

## NERC CIP BES Cyber System Information (BCSI)

[NERC CIP Standards for BES Cyber System Information on AWS](#)

[BES Cyber System Information \(BCSI\) on AWS](#)

[Operational Best Practices for NERC CIP BCSI](#)

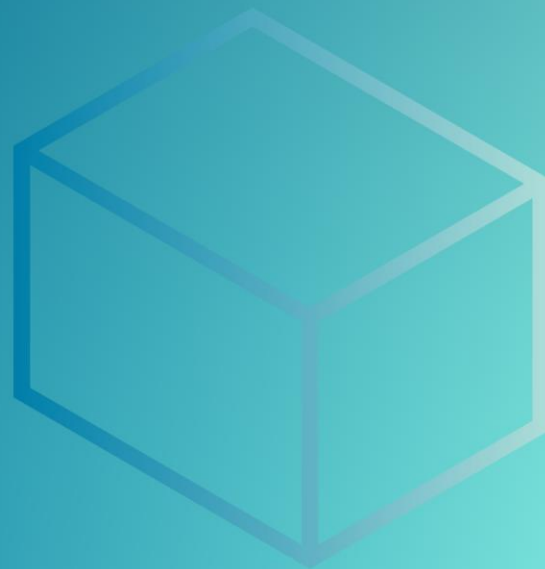
[Operational Best Practices for NERC CIP BCSI example](#)



# Thank you!

Kristine Martz

[KriMartz@amazon.com](mailto:KriMartz@amazon.com)







Frank Harrill

VP, Security, SEL

# Closing Remarks

Frank Harrill  
VP, Security Schweitzer Engineering (SEL)

# Thank you for attending!

[supplychain@natf.net](mailto:supplychain@natf.net)

[dearley@natf.net](mailto:dearley@natf.net)

[vagnew@natf.net](mailto:vagnew@natf.net)

## Links from the webinar chat:

**OSCAL FYI <https://pages.nist.gov/OSCAL/>**

**Reference for the machine-readable controls question <https://pages.nist.gov/OSCAL/>**

**<https://www.nerc.com/comm/RSTC/Pages/SITES.aspx>**