



Supply Chain Standards

Cybersecurity and Digitalization:
Supply Chain Risks in the Electricity Sector

Frances Cleveland

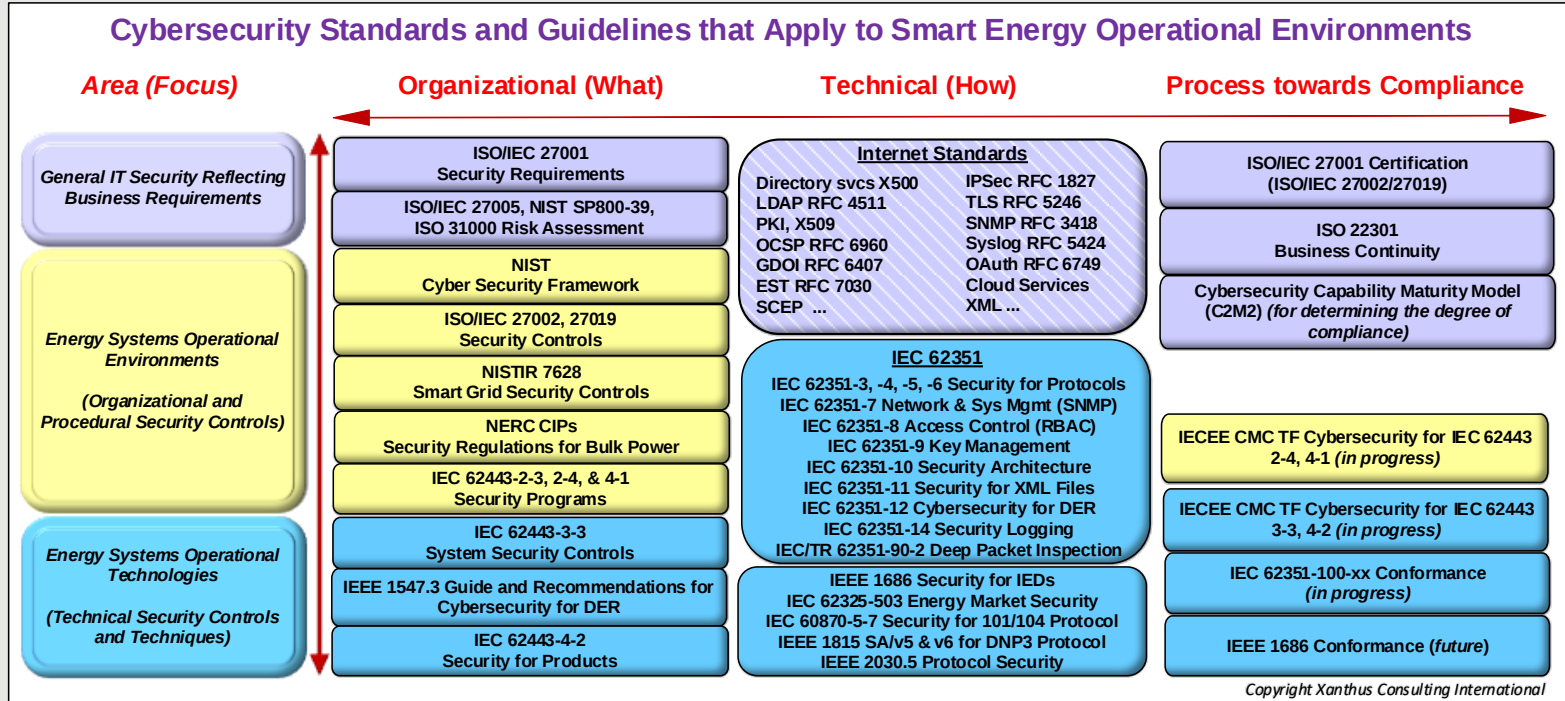
Gian Luigi Pugni

Agenda: Supply Chain Standards for Electric Power Utilities

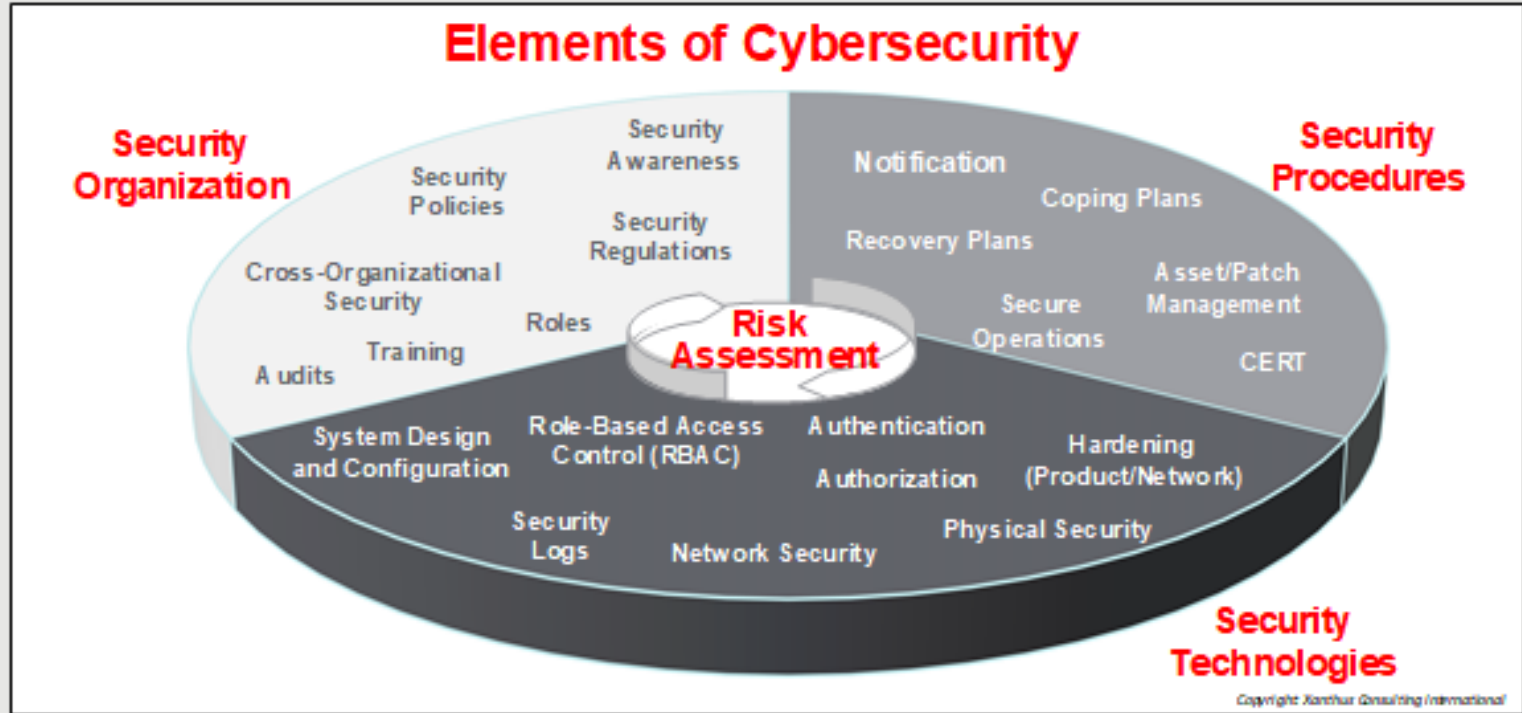
- Focus on Electric Power Utility supply chain issues in the operational environment
- Cover internationally accepted standards and guidelines relevant to identifying and managing cybersecurity risks associated with the supply chain risk from third-parties / suppliers and will provide a survey of these documents (e.g., the U.S. National Institute of Standards and Technology [NIST] Cybersecurity Framework, NIST SP800-161, ISO/IEC 27036-1:2021, NISTIR 8276).
- Address different approaches and considerations that utilities should take into account based on their context (e.g., generation, transmission, distribution, DER aggregators).

Overview of Cyber Security Standards and Guidelines

The key IEC, ISO, IEEE, NIST, NERC, and IETF cyber security standards and best practices are shown in the diagram, organized by type (**What**, **How**, Process towards **Compliance**) and by Focus Area (**High general level**, **High energy-specific level**, **Detailed technical level**).

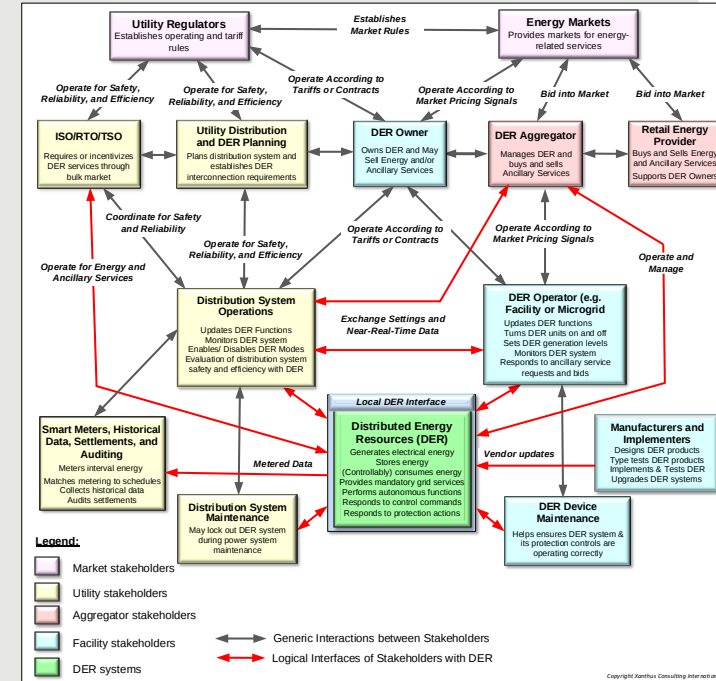


Elements of Cybersecurity: Organization, Procedures, and Technologies, based on Risk Assessment



What is Unique about Supply Chain Standards?

- Most cybersecurity standards focus on what a **single organization** needs to do to secure their own people, systems, and operations.
- Supply Chain security issues, by definition, involve **multiple organizations**
 - Procurement of products from other organizations.
 - Utilization of external communication networks and services, such as markets and cloud services.
 - Interactions with personnel from other organizations: vendors, plant operators, aggregators, and customers.
 - Incorporation of equipment from other organizations into power system operations, such as generating plants and distributed energy resources.



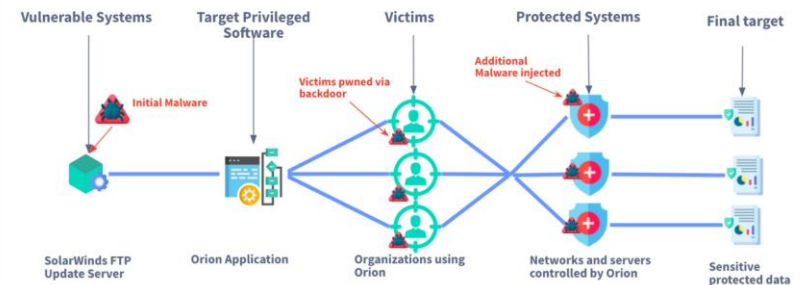
What are the Supply Chain Risks?

- Utility purchases energy management products from vendors who have deliberately or accidentally incorporated malicious code into their systems.
- Utility interfaces to 3rd party products which contain malicious code.
- Utility develops software using code from compromised sources.
- Utility installs 2 software/firmware patches with malicious code that is undetected: only detectable with both patches applied.
- 3rd parties connect to utility operations without adequate access control, authentication, or authorization.
- Supplier cannot provide products to utility in a timely manner due to their supply chain problems.
- Supplier provides lower quality or even counterfeit products due to their supply chain problems.
- Natural disasters physically disrupt the development and/or delivery of products.
- Regulatory changes affect delivery of systems – timing and/or quality.
- Cloud services experience cyber attacks, impacting sensitive data and power system operations.

Malicious code impacts:

- Allows sensitive information to be stolen.
- Affects power system operations, causing power outages, frequency or voltage problems, equipment failures, or even safety issues.
- Affects power markets so that subtle changes allow one market participant to gain more than the rules permit.
- Affects customer's appliances, causing utility loss of reputation even if they pay for damaged appliances.

Attack through trusted system with privileged access



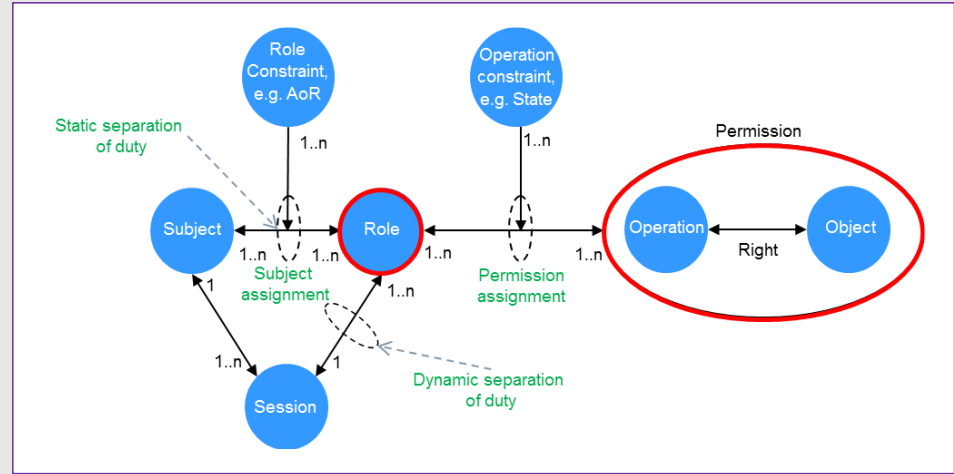
What are the Supply Chain Vulnerabilities?

- Utility fails to have comprehensive Security Policies for their OT systems (ISO/IEC 27019, IEC 62443, NIST CSF, NERC CIPs, etc.)
- Utility fails to have a supply chain policy for their procurements
- Utility fails to check on their vendors' supply chain policies
- Utility fails to test vendor products for common malware
- Utility fails to request the vendor to validate software systems and patches
- Utility fails to test the cybersecurity of vendor products including interfaces with utility equipment
- Utility fails to have multiple vendors able to supply similar products
- Utility fails to use multifactor authentication for access to critical systems
- Utility fails to require 3rd party owners and operators of generating plants and distributed energy resources (DER) to implement cybersecurity before connecting to the power system
- Utility fails to have cybersecurity contractual agreements on responsibilities and actions with 3rd party aggregators and DER owner/operators
- Utility fails to have plans for operations during natural disasters and recovering after such events



What are Some Key Actions to Address these Supply Chain Vulnerabilities?

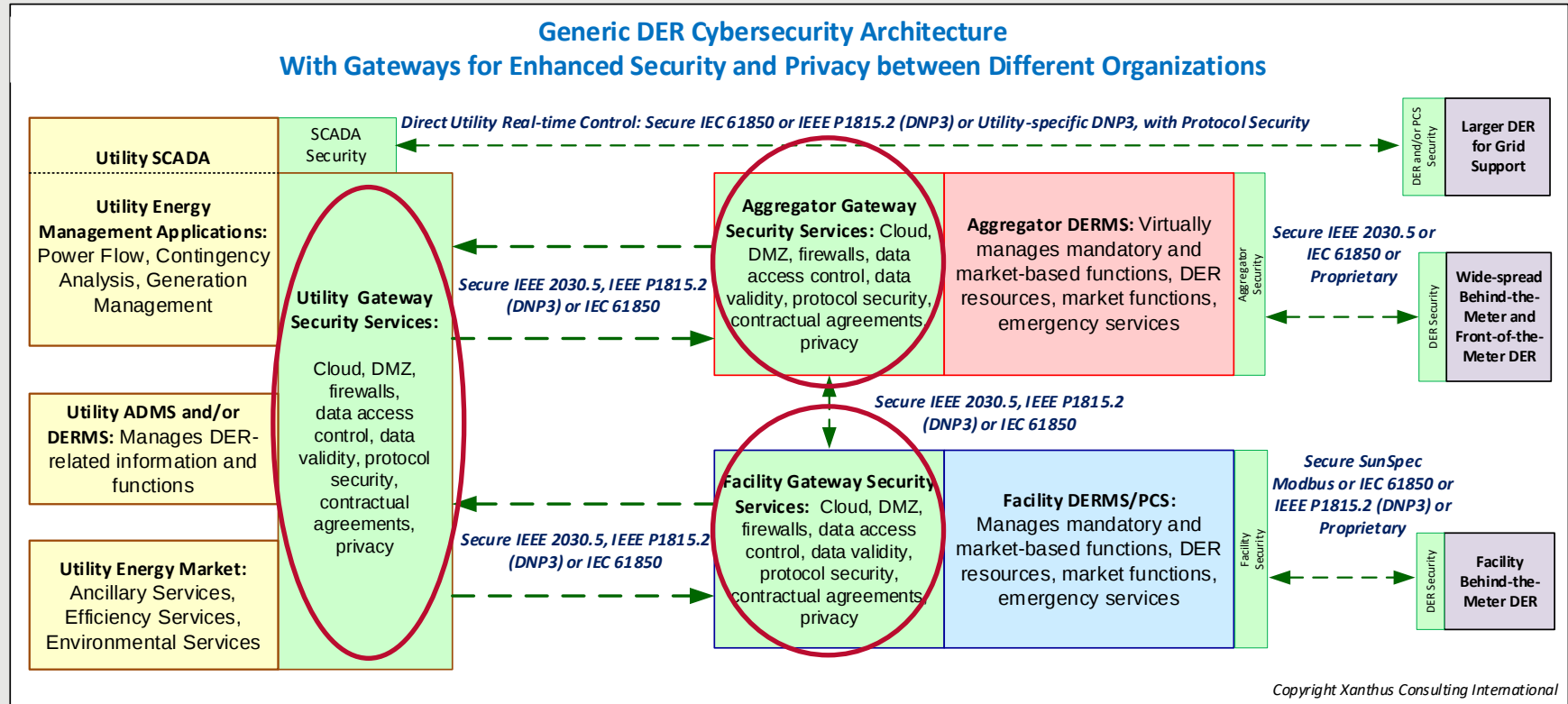
- Risk Assessment (see later slides)
- Use of power system monitoring to detect and log possible cyber attacks
- Cybersecurity requirements and testing certification for all interconnecting systems and personnel
- Cross-organizational contractual agreements on responsibilities and actions of all parties
- Role-Based Access Control (IEC 62351-8) for all external parties
- Gateways with strong security (next slide)



Example: Role-Based Access Control

What are Some Key Actions to Address these Supply Chain Vulnerabilities?

- Example DER architecture with gateways





NIST Cybersecurity Framework 2.0 (draft)

- **GOVERN (GV)** – Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy.
- **IDENTIFY (ID)** – Help determine the current cybersecurity risk to the organization.
- **PROTECT (PR)** – Use safeguards to prevent or reduce cybersecurity risk.
- **DETECT (DE)** – Find and analyze possible cybersecurity attacks and compromises.
- **RESPOND (RS)** – Take action regarding a detected cybersecurity incident.
- **RECOVER (RC)** – Restore assets and operations that were impacted by a cybersecurity incident.

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Standards on Third-Party Risk Management and Cyber Risk Assessment Methodologies

Gian Luigi Pugni



START4.0

Competence Center START 4.0

Enti Pubblici



Imprese



CYBERSECURITY



SAFETY



SECURITY



ENERGIA

Strategie di cybersecurity per le infrastrutture di distribuzione dell'energia



TRASPORTI

Information security management nell'ambito del trasporto



IDRICO

Soluzioni per recovery e monitoraggio degli invasi e della rete di distribuzione



PRODUZIONE

Digitalizzazione e aumento livelli di maturità tecnologica dei processi industriali



PORTO

Sicurezza delle merci e delle persone, data management flussi correlati

Topics

- Risk assessment for **Energy Systems** with the goal of **Business Continuity**
- Adoption of company policy and guidelines in Supply Chain management:
Cybersecurity Supply Chain Risk Management (C-SCRM)

NIST 2.0 Framework draft perspective

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Cybersecurity Supply Chain Risk Management (GV.SC):
Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)

GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (formerly ID.SC-01)

GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally (formerly ID.AM-06)

GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (formerly ID.SC-03)

GV.SC-04: Suppliers are known and prioritized by criticality

GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (formerly ID.SC-03)

GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04)

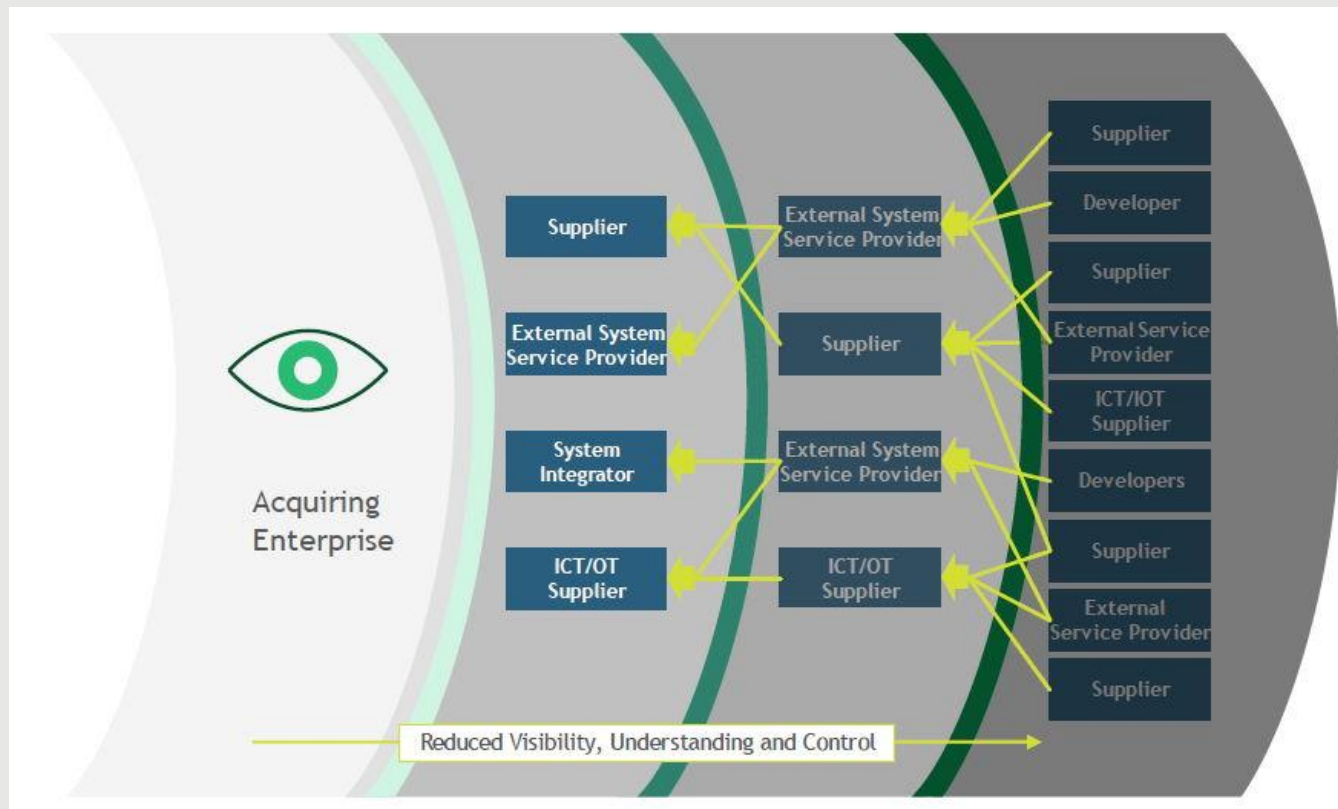
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities (formerly ID.SC-05)

GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle

GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

Source: Public Draft: The NIST Cybersecurity Framework 2.0 – NIST - August 8, 2023 <https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd>

Enterprise supply chain



Source: NIST SP 800-161r1

Enterprise supply chain

The **Supply Chain** is a set of complex, globally distributed and interconnected resources and processes.

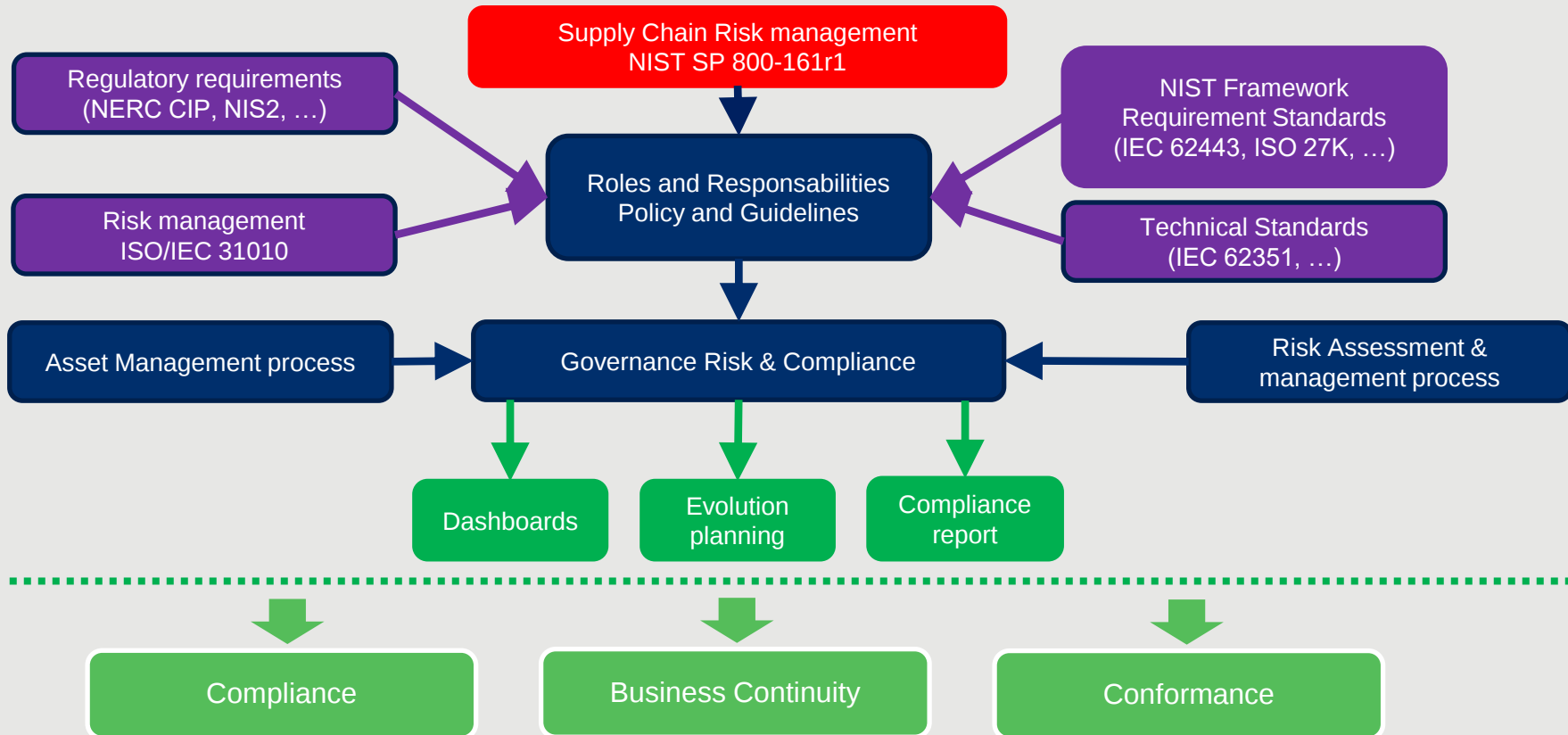
Cyber SCRM is the set of activities necessary to manage the **Cyber Security** risk associated with external parties.

This is needed to:

- **Determine** Cyber Security Requirements for Suppliers
- **Implement** requirements through formal agreements (e.g. contracts)
- **Communicate** to suppliers how these requirements will be verified and validated
- **Verify** that cybersecurity requirements are met through a variety of assessment methodologies
- **Maintain and improve continuously** this process as part of cyber security process

Source: NIST SP 800-161r1

Governance Risk & Compliance management



Policy and Guidelines – concept and examples

Global Policy

- Identity and Access Management
- Role Based Access Control
- Physical Security
- Network Security
- Asset management
- Security Monitoring
- Business Continuity requirements
- Data Classification

Specifications on context requirements

- Authentication requirements
- Data protection and encryption
- Physical monitoring for Substations
- PKI Systems requirements
- Monitoring of OT networks
- OT/IoT Cyber Security requirements
- Network Segregation in OT environments
- IaaS cloud security requirements

Specific context technical specifications & guidelines

- AD architecture structure and procedures
- IEC 62351 implementation guide
- Monitoring of OT networks
- Firewall configuration profiles
- Certification Authority CP and CPS
- Monitoring of OT networks
- IaaS Security zones configuration and management

Policy and Guidelines – concept and examples

Context requirements and technical specifications will feed the afterward supply chain processes and can incorporate controls from requirement standards (e.g., IEC 62443) or technical standard (e.g., IEC 62351).

Each control responsibility should be clearly assigned to specific actors of the supply chain (client, integrator, manufacturer, service provider)

Specifications on
context requirements



Specific context technical
specifications & guidelines

- Authentication requirements
- Data protection and encryption
- Physical monitoring for S
- PKI Systems requirements
- Monitoring of OT network

- AD architecture structure and procedures
- IEC 62351 implementation
- Monitoring of OT network

It must be defined and well communicated
Who is responsible of issuing, maintenance
and deployment

These are “the rules of the game” that must
be valid for the whole supply chain (both for
suppliers or clients)

Policy and guidelines are guided by:
Regulatory requirements
Standard and best practices
yet must reflect the company reality

Must be shared, agreed and adopted in the
product/service procurement phase
and in internal solution development

Represent the basis for certification and
Audit processes

• IaaS cloud security requirements

• Certification Authority CP and CPS

C-SCRM Lifecycle – Agree with suppliers on...

Manufacturer/provider
Qualification

- **Certifications**
- **Competences and contribution on Cybersecurity standards and best practices**
- **Better to share at this stage policy and guidelines**
- **Share the expected standard compliance (e.g. IEC 62443, ISO 27K)**

Purchase (tender) for
product/service

- **Risk assessment**
- **Technical standard periodical Audit clause**
- **HR requirement**
- **Vulnerability and event notification**
- **Lifecycle clauses (patching, maintenance, decommissioning)**
- **SLA with attention to Business Continuity**
- **Info sharing agreement**

Development and
deployment of the
solution

- **Security by design, standard based development or integration**
- **Vulnerability Assessment on development and pre deployment**
- **At this stage Policy, and technical specification based on standard (e.g IEC 62351) must be commonly adopted**

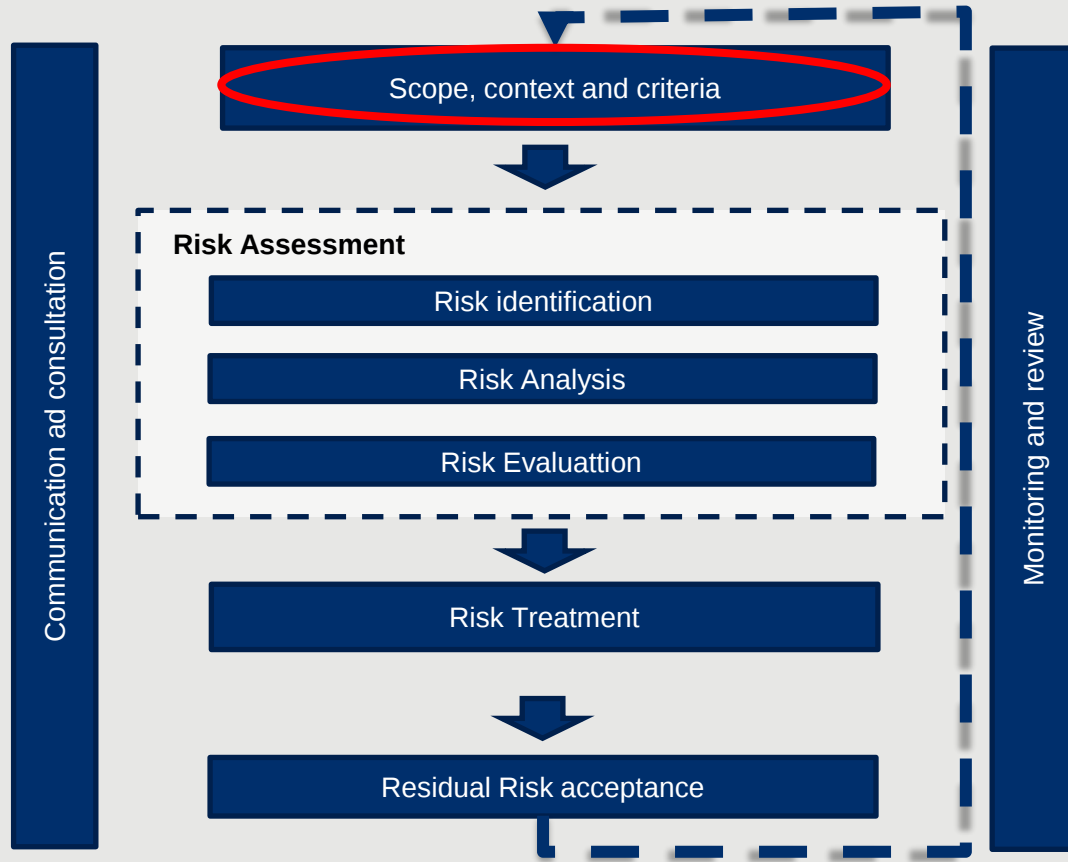
Maintenance

- **Business Continuity process regular testing**
- **Patching / maintenance process**
- **Regular Audit on product / systems and services**
- **Monitoring of events -> incident detection**
- **Asset management**
- **CERT/CSIRT process with asset responsibility**

Decommissioning

- **Secure Information back transfer**
- **Cleanup of devices and supplier data base**

Risk management ISO 31000 process and supply chain



Enterprise Policies must consider Business process relationship with supplier, customers and all stakeholders

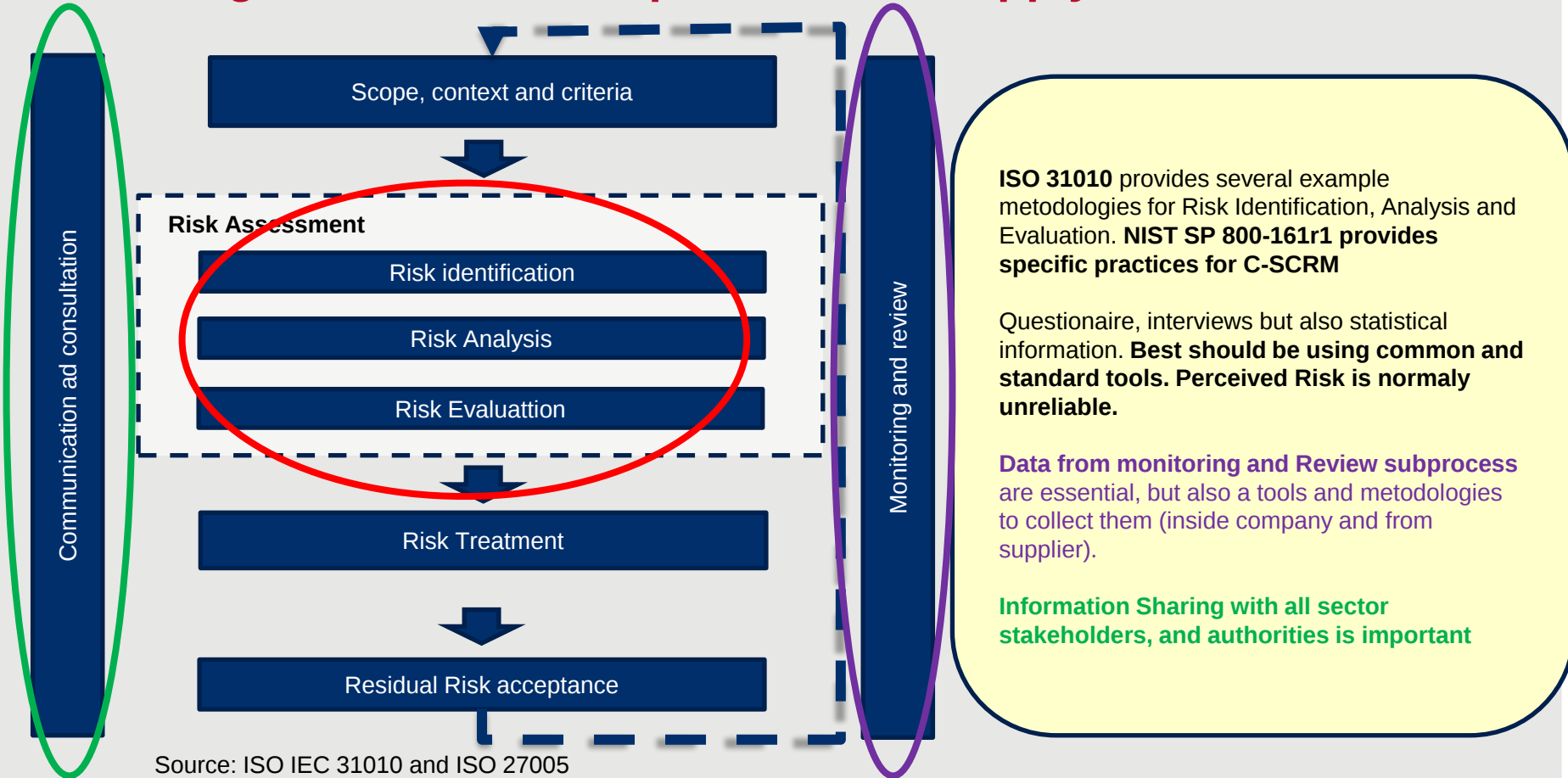
Since vendor qualification stage the context will enrich

For every new product, system, service the context will change

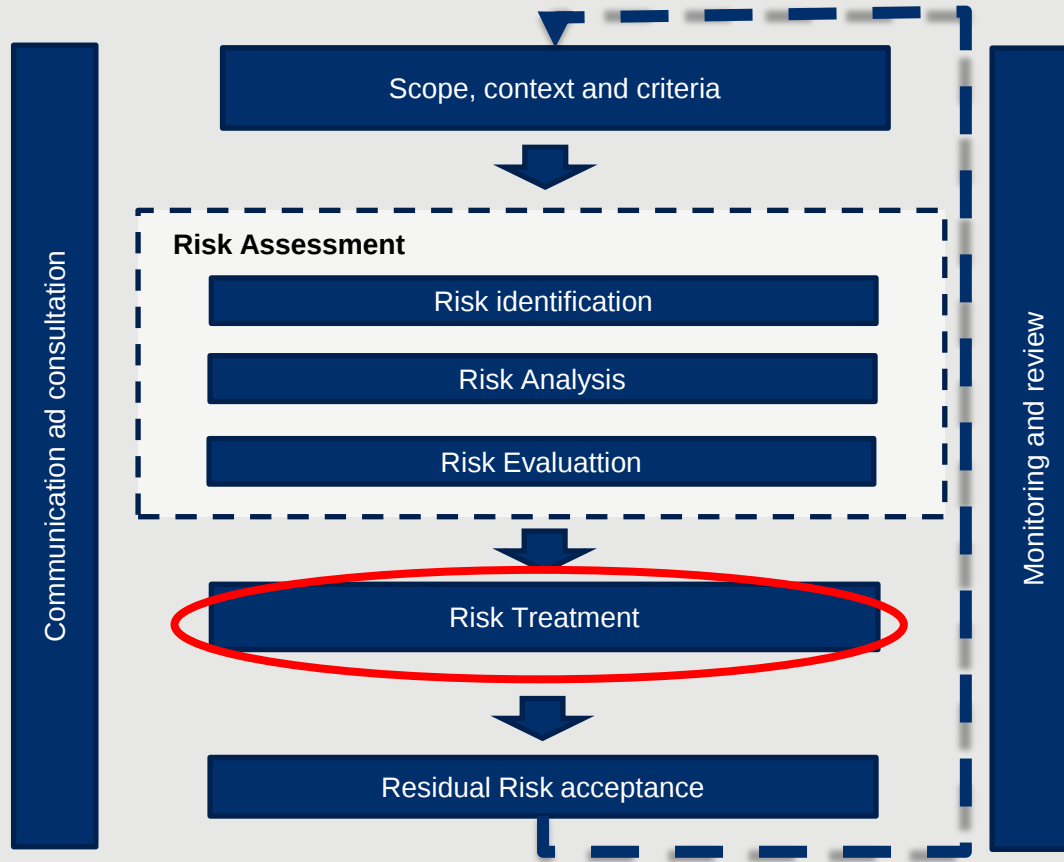
New Business processes will change the scope

At this stage the reference contacts for afterwards steps must be agreed

Risk management ISO 31000 process and supply chain



Risk management ISO 31000 process and supply chain



Source: ISO IEC 31010 and ISO 27005

Risk Assessments results may require to be: Avoid, Transfer, Mitigate or Accept every specific Risk.

In a multilevel SC Risk Transfer is needed and must be specified in the contract agreement: Policy and Technical specification must be clear in defining roles between parties (e.g. CERT relationships).

Requirement and Technical standard are fundamental to build Company technical specifications

Product, maintenance and Service supply require quite different approach.

C-SCRM additional elements

Regulatory compliance requirements:

NERC-CIP
NIS, NIS2
GDPR
RED directive
EC Cyber Resilience Act (upcoming)
...

OT environment specific complexity:

- extended solution lifecycle (15-20y) compared with IT systems
- Very distributed environment
- Relationship

Strict requirements for services and products:

- Notification timing for discovered vulnerabilities and incidents
- Product/service 3party certification
- Lifecycle duration for maintenance
- ...

Difficult to comply and be aware of everything especially for small companies. To overcome this problem is possible :

- adopt collaborative model based on Competence Centers
- enter Information Sharing groups like EE-ISAC

Open source based solutions, responsibilities, and compliance to upcoming regulations.
Information Sharing

References and contacts

- NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, May 2023, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>
- NIST CSF v2.0, https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf, <https://www.nist.gov/news-events/events/2023/09/journey-nist-cybersecurity-framework-csf-20-workshop-3>
- EE-ISAC, European Energy Information Sharing & Analysis Centre: <https://www.ee-isac.eu/>

Thank You

Frances Cleveland, Xanthus Consulting International
fcleve@xanthus-consulting.com

Gian Luigi Pugni, Competence Center START 4.0
glpugni@gmail.com



USAID
FROM THE AMERICAN PEOPLE

