Oil & Natural Gas Third Party Collaboration IT Security NIST Profile

API ITSS Third Party Collaboration IT Security Workgroup

Version 1.0

12/16/2016

Contents

1 Introduction

This document provides a profile for the use of the NIST Framework for Improving Critical Infrastructure for Cybersecurity (v1.0) for collaboration between Oil and Natural Gas (ONG) Industry Companies and other external parties. This profile provides cybersecurity requirements that should be considered as part of granting third parties (i.e., any non-employees) access to company assets (e.g., your company's network and information).

This profile has been established to assist in promoting greater efficiency in successfully establishing Joint Ventures and Major Capital Projects in the industry. However, the NIST Cybersecurity Framework also provides a common foundation for working across industries. Therefore, collaboration between Oil and Natural Gas Industry Companies and external partners used for consultancy or managed service providers is also within the scope of this document.

Both Information Technology and Operational Technology are in the scope of this profile. For example, this profile may be used when allowing access by a Third Party to Oil and Natural Gas Company IT Infrastructure/Systems for collaborating on documents. This profile may also be used for Process Control Systems, when working on and sharing processes which run the business. This profile provides a common understanding for how this may be done.

Suppliers are considered third parties, and this document is intended to be used in collaborating with the suppliers. However, it is not meant to be a specification for supplier products.

Many companies in the energy sector have begun to align with the NIST Framework for Improving Critical Infrastructure for Cybersecurity (v1.0), heretofore referred to as the NIST Framework or Framework. This NIST Framework was created through the collaboration between industry and government to provide consistent standards, guidelines and practices to promote the protection of critical infrastructure. In this document, the Framework has been analyzed from an Oil and Natural Gas Industry perspective. This may be considered a Framework profile with reference augmentation, but it does not dictate specific use cases or guidance for use. This profile is not intended to be used in implementing the Framework internally within an Oil and Natural Gas company.

While this profile has been developed to promote consistency across the industry in successfully establishing collaboration between ONG companies and external parties, the appropriate contractual agreements will still be required. All of the NIST functions may require information, reporting or consent from the Third Party, and the requirements of this information sharing and evidence collection should be noted in the contracts. (The American Petroleum Institute (API) IT Security Subcommittee is unable to provide contractual language.)

2 Approach

This section documents the approach taken to develop the Third Party Collaboration IT Security NIST Profile.

2.1 Relevant NIST Categories

The NIST Framework Core is shown in Table 1 providing an overview of the Functions and Categories within the Framework.

For this Profile, the API IT Security Subcommittee reviewed the NIST Categories and selected those that contained controls relevant to Third Party collaboration. These controls are highlighted in Table 2 with a "Controls" in the "Relevant to Third Party" column. The controls relevant to a company's risk profile should be verified before entering into an agreement with Third Parties.

There are some categories with specific controls that are not relevant to Third Party collaboration, but the category in the broader sense is relevant to this collaboration. For example, a company should be sure that Third Parties have a Risk Management Strategy, but it does not need to examine the details of the strategy. Therefore, the **Identify.Risk Management Strategy** category is marked as "Checklist" in the "Relevant to Third Party" column.

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
PR	Protect	PR.AC	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

Table 1. NIST Framework Function and Category Unique Identifiers

Function	Category	Relevance to Third Party
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Controls
	Business Environment (ID.BE): 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.	Checklist
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Controls
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Controls
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Checklist
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	Controls
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	Controls
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Controls
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Controls
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	Controls
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Controls
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	Controls
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	Controls
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	Controls

Function	Category	Relevance to Third Party
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**Controls**
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**Controls**
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**Controls**
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**Controls**
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**Checklist**
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**Controls**
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**Checklist**
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**Controls**

Table 2. NIST Framework noting Categories Relevant to Third Party Collaboration

2.2 Informative Reference Review

In the NIST Framework, each of the Categories has one or more Subcategories. Each Subcategory has associated Informative References. To illustrate this, consider the “Communications” category within the “Recover” function (as shown in Table 3). The Communications Category has three Subcategories, and each Subcategory has at least one informative reference. Some Subcategories have as many as six references. The References were reviewed and gaps (missing elements) were identified at the Subcategory level.

Function	Category	Subcategory	Informative References
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	· **CCS CSC** 8 · **COBIT 5** DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	· **COBIT 5** BAI05.07 · **ISA 62443-2-1** 4.4.3.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	· **COBIT 5** BAI07.08 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	· **COBIT 5** EDM03.02
		RC.CO-2: Reputation after an event is repaired	· **COBIT 5** MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· **NIST SP 800-53 Rev. 4** CP-2, IR-4

Table 3. NIST Framework Recover Function

2.3 Selection of Baseline Informative Reference

As a result of the Informative Reference review, it was determined that the most comprehensive reference for Third Party Collaboration in a business IT environment is the NIST SP 800-53 Rev 4, which is freely available. The other references were compared to NIST SP 800-53 Rev 4 and any relevant additional Informative References were documented in Section 3.

If the system to be protected is a process control environment rather than a business IT environment, IEC 62443-3-3 should be used in addition to NIST SP 800-53 Rev 4, but it is not a free reference.

As the references were reviewed, gaps in the content were documented. Supplemental References were then selected to bridge these gaps. These Supplemental References are also discussed in Section 3.

2.4 Additional References for Industrial Control Systems

When Joint Ventures and Major Capital Projects are implementing Industrial Control Systems (ICS), all parties should agree that security controls must be implemented as part of the design. The following reference discusses the importance of security on automation projects, emphasizing "'Secure by Design' rather than 'Secure by Default.'"
Cyber Security and Execution of Automation Projects
Joel Langill
http://www.eandcspoton.co.za/resources/docs/Control/Secure_IACS_projects.pdf

Although not mentioned in the NIST Cybersecurity Framework, the following standards should be used to provide for common terminology when discussing process control network security:

ISA 62443-1-1
Security for industrial automation and control systems - Models and Concepts
October 29, 2007
(ISA 99 is currently working on a second edition of this standard.)
http://isa99.isa.org/ISA99%20Wiki/WP-1-1.aspx
http://isa99.isa.org/Public/Documents/ISA-62443-1-1-EX.pdf

ISA 62443-1-2
Security for industrial automation and control systems – Glossary of Terms and Abbreviations
http://isa99.isa.org/ISA99%20Wiki/WP-1-2.aspx
http://isa99.isa.org/Public/Documents/ISA-62443-1-2-WD.pdf
(Readers should note that this is still a draft. Until it is approved, please use the ISA99 Master Glossary of Terms.
http://isa99.isa.org/ISA99%20Wiki/Master-Glossary.aspx.)

In addition, NIST SP 800-82 - Guide to Industrial Control System (ICS) Security contains a list of the relevant NIST SP 800-53 references for industry control systems.
http://dx.doi.org/10.6028/NIST.SP.800-82r2

In Appendix B, the NIST SP 800-53 references that are contained in the NIST Cybersecurity Framework for Critical Infrastructure and, according to NIST SP 800-82, are relevant to ICS are highlighted.

2.5 Profile Usage

The flowchart below provides an overview of how this profile may be used by ONG organizations when entering into agreements or collaborative efforts with external parties.

Section 3 walks through each Function and Category combination and notes whether it a Checklist or Controls approach should be taken. If the Checklist approach is required, a company should determine if the Category is executed in the broad sense. If the Controls approach is required, the company should confirm that the controls relevant to its risk profile are in place in working with third parties.

Appendix A contains the list of Informative References for each Subcategory. If the collaboration is an Information Technology Collaboration, the NIST SP 800-53 standard should be used. If the collaboration is an Operational Technology collaboration, NIST SP 800-53 and IEC 62443-3-3 should be used. Appendix B can be used to determine the specific references in NIST SP 800-53 references that are relevant to Operational Technology. For both Information Technology and Operational Technology collaborations, the Additional References for each Function and Category combination should be examined, as well as the Supplemental References that address the NIST Framework gaps.

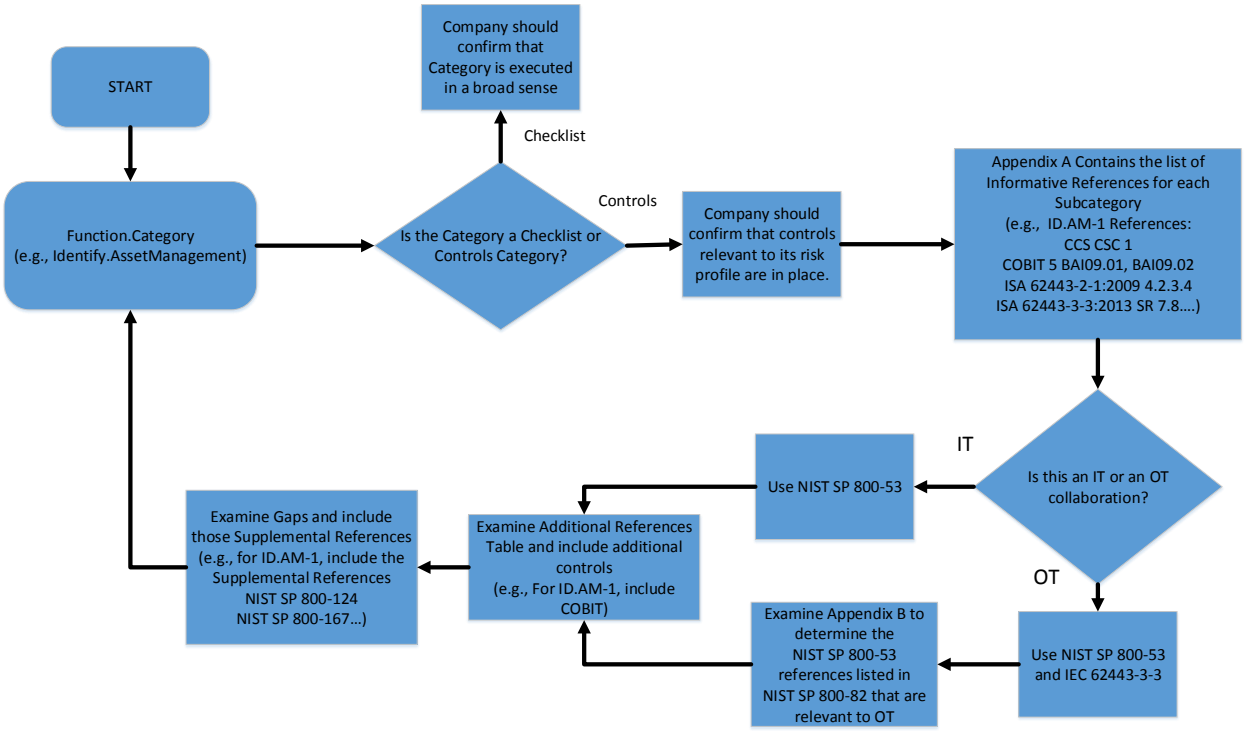

Figure 1. Profile Usage Flow Chart

3 Informative Reference Recommendations and Gaps

3.1 Identify

3.1.1 Identify.Asset Management (ID.AM)

Third Party Relevance: Controls

Rationale: A company's assets should be well-managed and tracked so that they can be adequately protected. This would be expected of any Oil and Natural Gas company.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments/Rationale
Identify.Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried		NIST 800-53 is more specific than ISA 62443.
Identify.Asset Management	ID.AM-2: Software platforms and applications within the organization are inventoried		NIST 800-53 is more specific than ISA 62443.
Identify.Asset Management	ID.AM-3: Organizational communication and data flows are mapped		No additional references
Identify.Asset Management	ID.AM-4: External information systems are catalogued		No additional references
Identify.Asset Management	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value		Both NIST 800-53 and ISA 62443 discuss prioritizing assets.

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments/Rationale
Identify.Asset Management	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	COBIT	Include COBIT 5 BAI09.01, BAI09.02 COBIT is more detailed than NIST 800-53.

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.1.1.a	Identify.Asset Management	Corporate vs. Non-corporate devices is not addressed for asset management.	NIST SP 800-124: Guidelines for Managing the Security of Mobile Devices in the Enterprise Workgroup Recommendation
3.1.1.b	Identify.Asset Management	Need clarity on whitelisting. Higher level of maturity would include whitelisting.	1)NIST SP 800-167: Guide to Application Whitelisting October 2015 2) National Cybersecurity Communications Integration Center Appendix to “Seven Steps to Defend Industrial Control Systems”
3.1.1.c	Identify.Asset Management	No specification for how often asset management activities are to occur. "On a regular basis" is not descriptive enough.	Workgroup recommendation

Gap#	Function.Category	Gap	Recommended Reference
3.1.1.d	Identify.Asset Management	Need detailed discussion of responsibilities	NERC CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments on page 41 under Requirement R4:
3.1.1.e	Identify.Asset Management	Additional information for Security Asset Management, both Business Network and Process Control Network assets, would be helpful.	1) ARC Advisory Group http://www.arcweb.com/ 2) NIST SP 1800-5b IT Asset Management October, 2015

Gap 3.1.1.a:
The NIST Framework References for Asset Management do not address Bring-Your-Own-Device (BYOD).

Workgroup Recommendation:
A non-Company asset would not be registered in the Company Asset register. From the Company point of view, all assets accessing Company IT infrastructure/IT systems should be registered and managed, irrespective of who owns them.

Supplemental Reference 3.1.1.a:
NIST SP 800-124: Guidelines for Managing the Security of Mobile Devices in the Enterprise
June 2013
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Highlights:

- Summary
  - Enforce security policies
  - Implement user and device authentication
  - Restrict which app stores may be used and which applications may be installed
- Section 2.2.2 discusses the use of untrusted mobile devices.
- Section 3.1 discusses sandboxes/containers for BYOD.
- Section 4.1.1 discusses access restrictions for BYOD.

Gap 3.1.1.b:
Need clarity on whitelisting. The NIST Framework references provide insufficient information on application whitelisting.

Supplemental Reference 3.1.1.b:

1) NIST SP 800-167: Guide to Application Whitelisting – October 2015

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

- Consider using application technologies that are already built into the Operating System.
- Use products that support sophisticated application attributes.
- Take a staged approach to application whitelisting.

2) National Cybersecurity and Communications Integration Center Appendix to "Seven Steps to Defend Industrial Control Systems"

The National Cybersecurity and Communications Integration Center (NCCIC) published an appendix to "Seven Steps to Defend Industrial Control Systems, " which provides conceptual guidance on application whitelisting for Industrial Control Systems. Links to both documents are listed below.

Seven Steps to Defend Industrial Control Systems
https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Whitelisting Appendix:
https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf

Gap 3.1.1.c:

No specification is provided in the Identify Function and Access Management Category references for how often asset management activities are to occur. References suggest, "on a regular basis," which is not descriptive enough.

Workgroup Recommendation:

The frequency should be based on risk and documented.

Supplemental Reference 3.1.1.c:

None

Gap 3.1.1.d:

Need more detailed discussion of responsibilities.

Supplemental Reference 3.1.1.d:

NERC CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments

CIP-010-2 - Attachment 1 and Requirement 4 Attachment 1 Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors

- Provides examples of roles for assets managed by vendors or contractors that are not given in NIST 800-53

http://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/CIP-010-2_CLEAN_09032014.pdf

Gap 3.1.1.e:
Additional information for Industrial Control System Asset Management would be helpful.

Supplemental References 3.1.1.e:
1) ARC Advisory Group (http://www.arcweb.com/)
The ARC Advisory Group site provides market research related to asset management in ICS maintenance and operations. Registration is required for free newsletters. It contains articles related to the Industrial Internet of Things and Asset Management. They also have technology selection guides for Asset Lifecycle Management.

2) NIST SP 1800-5b
IT Asset Management
October 2015
NIST SP 1800-5b is specific to the approach, architecture and security characteristics of IT Asset Management. It focuses on continuous management of assets https://nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5b-draft.pdf. This is becoming a more formal process for security assets with an emphasis on a cycle of continuous management.

3.1.2 Identify.Business Environment (ID.BE)

Third Party Relevance: Checklist
Rationale: While ensuring the organization's mission, stakeholders and activities are understood and prioritized is important, the specific controls are not required for Third Party Collaboration.

However, as part of the contractual processes in engagements with Third Parties, the Third Party organization should confirm that these profiles, strategies and cybersecurity elements are established and used by the organization. This is more of a checklist item that a list of controls that need to be implemented.

3.1.3 Identify. Governance (ID.GV)

Third Party Relevance: Controls

Rationale: Any company should be managing and monitoring its risk.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments/Rationale
Identify.Governance	ID.GV-1: Organizational information security policy is established		No additional references
Identify.Governance	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners		ISO27001 does not address alignment of internal roles with external entities. Recommend NIST.
Identify.Governance	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed		No additional references

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments/Rationale
Identify.Governance	ID.GV-4: Governance and risk management processes address cybersecurity risks		No additional references

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.1.3	Identify.Governance	Relevant external parties/third parties is not defined.	Definition developed by workgroup

Gap 3.1.3:
Relevant external parties or third parties is not defined.

Supplemental Reference 3.1.3: N/A

Workgroup Definition:
Third Parties are external, semi-trusted organizations including vendors, contractors, cloud providers and other service providers.

3.1.4 Identify. Risk Assessment (ID.RA)

Third Party Relevance: Controls
Rationale: Any company should be conducting risk assessments to identify risks.
Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments/Rationale
Identify.Risk Assessment	None	NIST references are much more detailed than ISA62443 references.	

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.1.4	Identify.RiskAssessment	Risk Assessments for the Cloud environment are not discussed	1) Cloud Security Alliance 2) API ITSS Cloud Risk Assessment Committee will be publishing additional guidelines

Gap 3.1.4:

Risk Assessments for the Cloud environment are not discussed

Supplemental References 3.1.4:

The NIST Framework references do not specifically discuss cloud connectivity or cloud providers.

Recommended Guidelines:

The Cloud Security Alliance (https://cloudsecurityalliance.org/) provides the Security Trust and Assurance Registry (STAR) (https://cloudsecurityalliance.org/star/) . STAR certification validates the security posture of cloud offerings. There are three STAR assurance ratings:

- Level 1 - Self-Assessment
- Level 2 - Third Party Assessment-Based Certification
- Level 3 - Continuous Monitoring-Based Certification

The Cloud providers should utilize the Cloud Security Alliance assurance ratings. The Level would be dependent on the use case and the criticality of the service provided.

3.1.5 Risk Management Strategy (ID.RM)

Third Party Relevance: Checklist

Rationale: The organization's priorities, constraints, risk tolerances, and assumptions, while important, are not directly related to Third Party Collaboration IT Security. Therefore, the specific controls are not required for Third Party Collaboration

However, as part of the contractual processes in engagements with Third Parties, the Third Party organization should confirm that these profiles/cybersecurity elements are established and used in risk management. This is more of a checklist item that a list of controls that need to be implemented.

3.2 Protect

3.2.1 Protect. Access Control (PR.AC)

Third Party Relevance: Controls

Rationale: Any company should implement Access Control mechanisms to secure and limit access to its assets to approved individuals, which include Third Parties.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments/Rationale
Protect. AccessControl	PR.AC-1: Identities and credentials are managed for authorized devices and users	IEC62443-3-3	NIST discusses account management. IEC 62443 discusses authentication (e.g., states that two factor authentication is needed for remote access).
Protect. AccessControl	PR.AC-2: Physical access to assets is managed and protected	IEC62443-3-3	NIST does not call out procedures for monitoring and alarming while IEC62443 3-3 does.

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments/Rationale
Protect. AccessControl	PR.AC-3: Remote access is managed	IEC62443-3-3	NIST states that ability to disable a connection is needed. IEC62443 states that some control systems or components may not allow sessions to be terminated.
Protect. AccessControl	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	IEC62443-3-3	IEC 62443 discusses supervisor override and emergency mechanisms for manual override, which are not in NIST.
Protect. AccessControl	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	IEC62443-3-3	IEC 62443 discusses session integrity and session ID. It also discusses cable exposure to elements (liquids, etc.) Meanwhile, NIST discusses VPNs and how to handle unsuccessful logins

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.1.4.a	Protect.AccessControl	No discussion of Federation or Federation architecture.	API ITSS Trust Framework

Gap#	Function.Category	Gap	Recommended Reference
3.1.4.b	Protect.AccessControl	A Network Protection/VPN-Firewall Reference Architecture is needed.	1) Trusted Internet Connections Reference Architecture Document v2.0 October 1, 2013 2) NIST SP 800-47: Security Guide for Interconnecting Information Technology Systems August, 2002 3) NIST SP 800-82: Guide to Industrial Control Systems Security June, 2011
3.1.4.c	Protect.AccessControl	No discussion of attestation of external identities requiring access to company infrastructure and systems.	NISTSP800-34A SA12(14) – Supply Chain Protection – Identity and Traceability Workgroup Recommendation

Gap 3.1.4.a:
Throughout the references, no information was provided regarding Federated Identity Management. The Federation Gap was documented in the Protect Function and Access Control Category.

Supplemental Reference 3.1.4.a:
The API ITSS Trust Framework should be referenced as energy industry companies are beginning to pursue federated identity management environments.

http://mycommittees.api.org/corporateaffairs/itsf/Shared%20Documents/Trust%20Framework%20Final%2007-15-2016.pdf

Gap 3.1.4.b: The Protect Function and Access Control Category section does not offer a Reference Architecture for Network Protection, Virtual Private Networks and Firewalls.

Supplemental References 3.1.4.b:
Trusted Internet Connections Reference Architecture Document v2.0
October 1, 2013
Published by the Department of Homeland Security

https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf

- This guide is geared towards Federal agencies but is applicable for business network third party connections
- Figure 4 on page 10 contains a security pattern for external connections. There are a range of security patterns starting on page 8. Connection scenarios are noted in the Appendices starting on page 37.

NIST SP 800-47: Security Guide for Interconnecting Information Technology Systems
August, 2002
http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

- This is a security guide for interconnecting IT Systems which provides two sample agreements in the Appendix:
    - An interconnection security agreement (page A.1)
    - A memorandum of understanding (page B.3)

NIST SP 800-82: Guide to Industrial Control System Security
June, 2011
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

- Section 5 – Network Architecture provides guidance on firewalls and network segregation. It also discusses business and process control network separation.

Gap 3.1.4.c:
No discussion of attestation of external identities requiring access to company infrastructure and systems.

Workgroup Recommendation:
Formal review and approval of external entities requiring access to company assets is recommended. Monitoring of access via an access reporting mechanism is also recommended.

Supplemental References 3.1.4.c:
NIST SP 900-53A Revision 4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations
Building Effective Assessment Plans
December 2014
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

- This NIST publication provides account management access controls as well as supply chain controls. SA-12(14) is applicable here for external parties:

- Establishes and retains unique identification of organization-defined supply chain elements, processes, and actors for the information system, system component, or information system service.

3.2.2 Protect. Awareness and Training (PR.AT)

Third Party Relevance: Controls

Rationale: This is relevant for 3rd parties, as the human element is the most fundamental of any IT Security program and the one with the biggest exposure, ensuring that any collaborating company that is accessing/sharing IT resources has a minimum standard & effective security awareness/training program is very important

Third Parties should contractually confirm that cybersecurity training is provided by their organizations. If the Third Parties have access into a corporation's environment, they should be trained on what the corporation's policies are and what is expected of them. For example, JVs and External Partners that will manage business information and have access to the network should receive security training.

3.2.3 Protect. Data Security (PR.DS)

Third Party Relevance: Controls

Rationale: The appropriate steps should be taken to protect company data.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Protect.Data Security	PR.DS-1: Data-at-rest is protected	CCS CSC 17; IEC62443	CCS CSC 17 discusses encryption and recommends that host-based/hard drive encryption and data leakage prevention techniques be used. IEC62443 provides more detail on integrity verification and automated notification of integrity violations.

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Protect.Data Security	PR.DS-2: Data-in-transit is protected	IEC62443-3-3	IEC 62443 is more detailed than NIST. IEC62443 discusses the potential for packet manipulation, session integrity, and purging data from memory.
Protect.Data Security	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition		No additional references
Protect.Data Security	PR.DS-4: Adequate capacity to ensure availability is maintained	IEC62443-3-3	IEC 62443 is more detailed than NIST for Denial of Service protection. NIST is a more detailed for resource management and allocation of resources to more critical jobs. NIST also discusses the need to understand storage capacity.
Protect.Data Security	PR.DS-5: Protections against data leaks are implemented		No additional references

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Protect.Data Security	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	ISO/IEC 27001; IEC62443-3-3	ISO 27001 discusses protection of application service transactions. IEC 62443 is more detailed than NIST. NIST focuses on software, firmware, and information integrity. IEC62443 focuses verification of security functionality and session integrity and communication integrity, as well as software integrity.
Protect.Data Security	PR.DS-7: The development and testing environment(s) are separate from the production environment	ISO/IEC 27001	NIST speaks to baseline configuration but provides little guidance on the separation of development and production environments. ISO addresses these areas.

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.2.3.a	Protect.DataSecurity	No discussion of encryption standards.	1) NSA Types provided 2) NIST SP 800-111: Guideline to Storage Encryption Technologies for End User Devices
3.2.3.b	Protect.DataSecurity	No discussion of key ownership.	1) Workgroup recommendation 2) NIST SP 800-57: Recommendation for Key Management – Part 1: General (Revision 3) July, 2012

Gap#	Function.Category	Gap	Recommended Reference
3.2.3.c	Protect.DataSecurity	No discussion of the controls needed to protect production data in a test environment in PR.DS-7.	1)Workgroup recommendation

Gaps 3.2.3.a and 3.2.3.b

The NIST Framework references do not provide encryption standards or key ownership recommendations.

NSA Types Provided:

Encryption Standards:

To provide some perspective on the encryption security levels, the National Security Agency (NSA) Types are provided here for reference. NSA provides encryption standards and guidelines for the U.S. government.

- Type 1 encryption is endorsed for Classified or U.S. government sensitive national security information.
- Type 2 encryption is endorsed for U.S. government sensitive national security information.
- Type 3 encryption is used for unclassified U.S. government information or commercial information.

The National Institute of Standards and Technology (NIST) has stated that AES encryption of all three key lengths (128-bit, 192-bit and 256-bit) provides adequate protection. The NSA has approved AES for Type 1 systems.

Workgroup Recommendation:

Key Ownership:

As a best practice, it is recommended that encryption keys be owned by the entity that owns the information, although they may be managed by another entity.

Supplemental References 3.2.3.a and 3.2.3.b:

Recommended Standard:

NIST SP 800-111: Guide to Storage Encryption Technologies for End User Devices

November, 2007

http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

- This document provides guidance for the encryption of data at rest: full disk encryption, volume and virtual disk encryption, and file/folder encryption.

Recommended Standard:
NIST SP 800-57: Recommendation for Key Management – Part 1: General (Revision 4)
January, 2016
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

- This document provides best practices associated with key management.

Gap 3.2.3.c

PR.DS-7, which focuses on development and test environments, does not discuss the controls needed to protect production data in development and test environments.

Workgroup Recommendation:
There may be occasions when sensitive data must be used in research, testing and training. A rigorous risk assessment should be performed to determine the necessity and the privacy risks. The appropriate mitigations, such as data masking, should be implemented.

3.2.4 Protect.Information Protection Processes and Procedures (PR.IP)

Third Party Relevance: Controls
Rationale: The appropriate processes and procedures should be implemented to protect company data. Best practices should be implemented for encryption as well as backup and recovery.
Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Protect. Information Protection	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained		No additional references

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Protect. Information Protection	PR.IP-2: A System Development Life Cycle to manage systems is implemented		No additional references
Protect. Information Protection	PR.IP-3: Configuration change control processes are in place	IEC62443-3-3	IEC62443-3-3 is complementary. NIST is focused on process. IEC62443 focuses on settings.
Protect. Information Protection	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	IEC62443-2-2	IEC 62443-2-2 is more detailed for control system backup and recovery. It discusses known states and patches for control system recovery.
Protect. Information Protection	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met		No additional references
Protect. Information Protection	PR.IP-6: Data is destroyed according to policy		No additional references
Protect. Information Protection	PR.IP-7: Protection processes are continuously improved		No additional references
Protect. Information Protection	PR.IP-8: Effectiveness of protection technologies is shared with		No additional references

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
	appropriate parties		
Protect. Information Protection	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed		No additional references
Protect. Information Protection	PR.IP-10: Response and recovery plans are tested	IEC 62443-3-3	NIST discusses testing and validation broadly. IEC 62443-3-3 is more specific. For example, IEC suggests IDS and anti-virus validation.
Protect. Information Protection	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	IEC62443-2-1	NIST does not specifically state that personnel should be screened on an ongoing basis, while IEC62443-2-1 does.

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.2.4.a	Protect.Information Protection	Cabling security discussion is incomplete.	1) ISO/IEC 27002, Section 11.2.3. 2) NIST SP 800-82: Guide to Industrial Control System Security

Gap#	Function.Category	Gap	Recommended Reference
			June, 2011 3) IEEE 1242: Guide for Specifying and Selecting Cable for Petrochemical Plants, 2005
3.2.4.b	Protect.Information Protection	Incomplete discussion of secure backups.	1) NIST SP 800-111: Guideline to Storage Encryption Technologies for End User Devices November, 2007 2) NIST SP 800-123: Guide to General Server Security July, 2008
3.2.4.c	Protect.Information Protection	Incomplete discussion of background checks and terminations.	1) Workgroup recommendation 2)NIST SP 800-82 Guideline to Industrial Control Systems Security June, 2011

Gaps 3.2.4.a

The cabling security discussion in the NIST Framework references is incomplete.

Standards are listed below. However, it should be noted that different automation vendors support implementations of proprietary and "near-standard" signaling and transmission protocols that will affect the specification of cables. In these instances, it is appropriate and required to adhere to the vendor-recommended cable (where often the vendor is the only supplier) so as to not violate warranty and support considerations.

Supplemental References 3.2.4.a

ISO/IEC 27002 provides additional guidance in Section 11.2.3 – Cabling Security.
http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf

- This standard recommends underground and segregated power and telecommunications lines.
- The standard also recommends the use of cables with electromagnetic shielding.

NIST SP 800-82 provides additional guidance in Section 6.2.2.3 – Cabling.
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

- Cabling recommendations for process control networks are discussed.

IEEE 1242: Guide for Specifying and Selecting Cable for Petrochemical Plants
Published in 2005

http://ieeexplore.ieee.org/Xplore/defdeny.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Farnumber%3D1470007&denyReason=-134&arnumber=1470007&productsMatched=null&userType=inst

The standard is available for a fee, but a summary from Mustang Engineering is available at the following link:

http://www.mustangeng.com/NewsandIndustryEvents/Publications/Publications/IEEESTANDARD1242.pdf

Gap 3.2.4.b
The Protection Function and Information Protection Processes and Procedures Category references do not provide a complete discussion of secure backups.

Supplemental References 3.2.4.b:

NIST SP 800-111 Rev 1: Guide to Storage Encryption Technologies for End User Devices
November, 2007
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

- This document discusses the protection of data at rest.
- Pages 2 and 3 suggest that backups should be protected at least as well as the original source.

NIST SP 800-123 Rev 1: Guide to General Server Security
July, 2008
http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

- This guide discusses the necessary activities performed to secure and maintain the security of servers.
- Section 6 discusses server security.

- Section 6.2.1 discusses server data backup policies.

Gap 3.2.4.c:
An incomplete discussion of background checks and terminations was provided.

Workgroup Recommendation:
Evidence of background checks for employees involved in collaboration efforts should be provided. In addition, parties should be notified of terminations of employees involved in collaboration.

Supplemental Reference 3.2.4.c:
NIST SP 800-82 – Guide to Industrial Control Systems Security
June, 2011
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

- Section 6.2.1 discusses personnel security, including hiring and terms and conditions of employment.

3.2.5 Protect.Maintenance (PR.MA)

Third Party Relevance: Controls
Rationale: The appropriate steps should be taken to protect the environment when maintenance steps are performed.
Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Protect. Maintenance	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	IEC62443-2-1	NIST states that strong authentication should be used, but does not elaborate. IEC62443-2-1 provides some details.
Protect. Maintenance	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	IEC62443-2-1	NIST states that strong authentication should be used, but does not elaborate. IEC62443-2-1 provides some details.

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.2.5.a	Protect.Maintenance	No maintenance reference architecture provided. For example, the need for protecting information in transit is not discussed.	1) Configuring and Managing Remote Access for Industrial Secure Systems November, 2010 2) PNNL-20776 Secure Data Transfer Guidance for Industrial Control and SCADA Systems September 2011 3) NIST 800-82 Rev2 Guide to Industrial Control System Security May, 2015
3.2.5.b	Protect.Maintenance	There is no mention of software versioning or patch management requirements.	NIST SP 800-40 Rev 4 Guide to Enterprise Patch Management Technologies July 2013

Gap 3.2.5.a:
The NIST Framework does not provide a reference architecture for securing infrastructure maintenance activities.

Supplemental Reference 3.2.5.a:

Configuring and Managing Remote Access for Industrial Control Systems
November, 2010
Published by the Department of Homeland Security and Center for the Protection of National Infrastructure
http://docplayer.net/15167503-Configuring-and-managing-remote-access-for-industrial-control-systems-november-2010-cpni-centre-for-the-protection-of-national-infrastructure.html

- This guide is geared towards the Industrial Control System network

- Page 29 provides guidance for improving security, and page 31 provides a diagram with security countermeasures implemented.
- Page 41 contains a topology diagram for VPN remote access.

PNNL-20776
Secure Data Transfer Guidance for Industrial Control and SCADA Systems
September 2011
http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

- This guide is geared towards ICS and SCADA
- Page B.3 shows a sample architecture, including external connections.
- The following components of the architecture are discussed: Security Zones, Demilitarized Zones, Firewalls and Intrusion Detection/Prevention Systems.

NIST 800-82 Rev2
Guide to Industrial Control System Security
May, 2015
A reference architecture is depicted in Figure 5-5, "CSSP Recommended Defense-in-Depth Architecture."

Gap 3.2.5.b:
There is no mention of software versioning or patch management requirements in the Protect.Maintenance references of the NIST Framework.

Supplemental Reference 3.2.5.b:

NIST SP 800-40 Rev 4
Guide to Enterprise Patch Management Technologies
July 2013
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

Summary:
This publication states that patches should be deployed to correct security problems in hardware and software. It discusses patch management challenges and technologies.

3.2.6 Protect.Protective Technology (PR.PT)

Third Party Relevance: Controls

Rationale: The appropriate protective technologies should be installed.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Protect. Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	IEC62443-3-3, ISO27001, CCS CSC	NIST does not address control system timestamps in as much detail as IEC62443. ISO references clock synchronization to a single reference time source for the integrity of event correlation. NIST does not cover this area. CCS CSC addresses many specific concerns related to logging and retention.
Protect. Protective Technology	PR.PT-2: Removable media is protected and its use restricted according to policy	IEC62443-3-3, CCS CSC	NIST does not address portable devices, while IEC 62443 does, stating that portable devices should not be used with control systems NIST addresses asset management, lifecycle management, and physical controls of removable media, where CCS addresses technical controls such as monitoring, scanning, and disabling auto-run.

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Protect. Protective Technology	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	IEC62443-3-3	IEC62443-3-3 discusses two-factor authentication and PKI.
Protect. Protective Technology	PR.PT-4: Communications and control networks are protected	IEC62443-3-3	IEC62443 mentions areas specific to control systems like failing closed and restriction on person-to-person communication like email.

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.2.6.a	Protect.Protective Technology	Additional discussion on the importance of timestamps would be useful.	NIST 800-82 Rev2 Guide to Industrial Control System Security May, 2015
3.2.6.b	Protect.Protective Technology	More information on the management of removable media for the Industrial Control System is needed.	NIST 800-82 Rev2 Guide to Industrial Control System Security May, 2015

Gap 3.2.6.a

More details on the importance of timestamps would be helpful.

Supplemental Reference 3.2.6.a

NIST 800-82 Rev2
Guide to Industrial Control System Security
May 2015

Page 6-14 states that, “The system should provide reliable, synchronized time stamps in support of the audit tools.”

Gap 3.2.6.b

More information on the management of removable media is needed.

Supplemental Reference 3.2.6.b

NIST 800-82 Rev2
Guide to Industrial Control System Security
May 2015

Page 6-27 states that the use of unauthorized removable media should not be permitted.

3.3 Detect

3.3.1 Detect. Anomalies and Events (DE.AE)

Third Party Relevance: Controls

Rationale: The ability to detect anomalous events, which could become incidents, is recommended in working with Third Parties.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Detect. Anomalies Events	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed		No additional references

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Detect. Anomalies Events	DE.AE-2: Detected events are analyzed to understand attack targets and methods	IEC62443-3-3; CCS CSC	IEC62443 provides detail on audit logs and discusses monitoring device placement. NIST is very detailed, but CCS provides detail on specific logs to capture.
Detect. Anomalies Events	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	IEC62443-3-3; CCS CSC	IEC62443 provides detail on audit logs. CCS provides a better understanding of SIEM functionality.
Detect. Anomalies Events	DE.AE-4: Impact of events is determined		No additional references
Detect. Anomalies Events	DE.AE-5: Incident alert thresholds are established		No additional references

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.3.1.a	Detect.AnomaliesEvents	Need to ensure an agreement is made between parties to share information.	NERC CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments
3.3.1.b	Detect.AnomaliesEvents	No thresholds for triggering alerts were documented.	NIST 800-53A provides additional guidance for monitoring alerts.

Gap 3.3.1.a

There is a need to ensure the appropriate agreements are made between parties to share information.

Supplemental References 3.3.1.a
There must be a joint expectation for this type of service (Incident response, Alerts and Breach Notification) formally set forth in negotiations and engagement with third parties, in writing and backed up with some sort of indemnification.

Recommended Standard:

NERC CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments
Page 41 under Requirement R4:
Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Gap 3.3.1.b
Thresholds for triggering alerts are needed.

Supplemental References 3.3.1.b (Same as 3.3.2)
While standards did not provide specific information for security alert thresholds or breach notifications, the NIST 800-53A Rev 4 standard provided some additional broad guidance for both areas. This standard also discussed incident handling, reporting and response. Meanwhile, NIST 800-61 Rev 2 provides information on incident notification and the indicators of an incident.

NIST 800-53A Revision 4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations
Building Effective Assessment Plans
December 2014
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

- IR-4(8) - Incident Handling - Correlation With External Organizations
    - This section requires defining the information to be correlated and shared with external organizations.

- IR-6 - Incident Reporting
    - This section states that an organization should report incidents within a defined time period.

- IR-7(2) - Incident Response Assistance - Coordination With External Providers

- This section requires establishing relationships between a company's incident response teams and the external providers.

- SI-4(5) - Information System Monitoring - System-Generated Alerts
- SI-4(7) - Information System Monitoring - Automated Response To Suspicious Events
- SI-7(8) - Software, Firmware, And Information Integrity - Auditing Capability For Significant Events
- SI-4(12) - Information System Monitoring - Automated Alerts
  - These sections state that personnel or roles to be alerted should be defined for indicators of compromise, suspicious events, integrity violations and inappropriate or unusual activities.

- SI-5 - Security Alerts, Advisories, And Directives
  - This section states that a company should receive information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.

- SI-5(1) - Security Alerts, Advisories, And Directives - Automated Alerts And Advisories
  - This section discusses having an understanding of the automated mechanisms available to the organization for security alerts and advisories.

- SI-4(22) - Information System Monitoring - Unauthorized Network Services
  - This standard requires that organizations define personnel or roles to be alerted upon the detection of unauthorized or unapproved network services.

NIST SP 800-61 Rev 2
Computer Security Incident Handling Guide
August 2012
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- 3.2.7 - Incident Notification
  - This section provides a suggested list of individuals to be notified which includes external providers.

3.3.2 Detect. Security Continuous Monitoring (DE.CM)

Third Party Relevance: Controls
Rationale: Security monitoring is recommended when working with Third Parties.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Detect.SecurityContinuous Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events	IEC62443-3-3, CCS CSC	Control system monitoring is more detailed in IEC62443, while NIST discusses account management and monitoring. CSC addresses log management and log retention requirements. However, NIST does a better job addressing network monitoring and different networks in which logging is needed (wireless, external to internal, etc.).
Detect.SecurityContinuous Monitoring	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	IEC62443-3-3	Control system monitoring is more detailed in IEC62443. Physical access control is in NIST.
Detect.SecurityContinuous Monitoring	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	IEC62443-3-3	IEC62443 is more detailed for control system monitoring. NIST discusses account management and monitoring.
Detect.SecurityContinuous Monitoring	DE.CM-4: Malicious code is detected	IEC62443-3-3, CCS CSC	IEC62443 provides some detail on malicious code that is not in NIST. CSC addresses technical controls for malware protection and detection.

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Detect.SecurityContinuous Monitoring	DE.CM-5: Unauthorized mobile code is detected	IEC62443-3-3	Mobile code is discussed in more detail in IEC 62443-3-3. It provides some examples.
Detect.SecurityContinuous Monitoring	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events		No additional references
Detect.SecurityContinuous Monitoring	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events		No additional references
Detect.SecurityContinuous Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed		No additional references
Detect.SecurityContinuous Monitoring	DE.CM-8: Vulnerability scans are performed	CCS CSC	NIST and CSC both address technical recommendations for vulnerability scanning.

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.3.2	Detect.SecurityContinuous Monitoring	No discussion of breach notifications from third parties.	NIST 800-53A provides additional guidance for breach notifications. NIST 800-61r2 provides information on incident notification.

Gap 3.3.2:
There is no discussion of breach notifications from third parties.

Supplemental References 3.3.2 (Same as 3.3.1)
While standards did not provide specific information for security alert thresholds or breach notifications, the NIST 800-53A Rev 4 standard provided some additional broad guidance for both areas. This standard also discussed incident handling, reporting and response. Meanwhile, NIST 800-61 Rev 2 provides information on incident notification and the indicators of an incident.

NIST 800-53A Revision 4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations
Building Effective Assessment Plans
December 2014
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

- IR-4(8) - Incident Handling - Correlation With External Organizations
    - This section requires defining the information to be correlated and shared with external organizations.

- IR-6 - Incident Reporting
    - This section states that an organization should report incidents within a defined time period.

- IR-7(2) - Incident Response Assistance - Coordination With External Providers
    - This section requires establishing relationships between a company's incident response teams and the external providers.

- SI-4(5) - Information System Monitoring - System-Generated Alerts
- SI-4(7) - Information System Monitoring - Automated Response To Suspicious Events

- SI-7(8) - Software, Firmware, And Information Integrity - Auditing Capability For Significant Events
- SI-4(12) - Information System Monitoring - Automated Alerts
    - These sections state that personnel or roles to be alerted should be defined for indicators of compromise, suspicious events, integrity violations and inappropriate or unusual activities.

- SI-5 - Security Alerts, Advisories, And Directives
    - This section states that a company should receive information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.

- SI-5(1) - Security Alerts, Advisories, And Directives - Automated Alerts And Advisories
    - This section discusses having an understanding of the automated mechanisms available to the organization for security alerts and advisories.

- SI-4(22) - Information System Monitoring - Unauthorized Network Services
    - This standard requires that organizations define personnel or roles to be alerted upon the detection of unauthorized or unapproved network services.

NIST SP 800-61 Rev 2
Computer Security Incident Handling Guide
August 2012

- 3.2.7 - Incident Notification
    - This section provides a suggested list of individuals to be notified which includes external providers.

3.3.3 Detect. Detection Processes (DE.DP).

Third Party Relevance: Controls
Rationale: The appropriate processes and procedures should be implemented to ensure monitoring is appropriately executed.
Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Detect. Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability		No additional references
Detect. Detection Processes	DE.DP-2: Detection activities comply with all applicable requirements	ISO27001 NIST 800-53 Rev 4	Privacy regulations are discussed in the ISO standard. NIST 800-53 Rev 4 includes a Privacy Controls Catalog.
Detect. Detection Processes	DE.DP-3: Detection processes are tested	IEC62443-3-3	Security functionality verification is included in IEC62443, but not in NIST.
Detect. Detection Processes	DE.DP-4: Event detection information is communicated to appropriate parties	IEC62443-3-3	An application programming interface (API) provided by control system for access to logs is discussed in IEC62443-3-3.

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.3.3.a	Detect.DetectionProcesses	How privacy regulations apply to third parties is not discussed.	Workgroup Recommendation API Trust Framework NIST 800-53 – Control UL-2

3.3.3.b	Detect.DetectionProcesses	There is no discussion regarding setting a formal expectation of privacy between the parties.	NERC CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments

Gap 3.3.3.a:
How privacy regulations apply to third parties is not discussed.

Workgroup Recommendation:
As privacy is a regulatory concern, corporate law must be consulted be consulted. Handling of data that falls under privacy regulations should be assessed and documented as part of third party contracts. One must be cognizant of privacy laws when managing third party personal data. Privacy laws vary from one country to the next.

Baker and McKenzie publishes a global privacy handbook yearly which covers privacy law across the world. One can request the handbook or access the online tool from this URL: http://bakerxchange.com/cv/36363bd2dcf09d18a30203b0dd39af54003fb6d1 .

DLA Piper provides an interactive online handbook and color-coded map, which can be useful when comparing the privacy regulations of different countries.
https://www.dlapiperdataprotection.com/#handbook/world-map-section/c1_AR/c2_AU

Privacy is also generally covered within the API Trust Framework.
http://mycommittees.api.org/corporateaffairs/itsf/Shared%20Documents/Trust%20Framework%20Final%2007-15-2016.pdf

NIST 800-53 r4
Control UL-2
This is the primary privacy control in 800-53, Appendix J. It is intended to address requirements definition and documentation for sharing Personally Identifiable Information (PII) between parties.

Supplemental Reference 3.3.3.b
The appropriate expectations must be set for this privacy between the third parties. The following standard contains examples for establishing privacy expectations.

NERC CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments on page 41 under Requirement R4:
Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

3.4 Respond

3.4.1 Respond. Response Planning (RS.RP)

Third Party Relevance: Controls
Rationale: Response processes and procedures must be executed and maintained when collaborating with third parties.
Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations
None

Gaps
None

3.4.2 Respond. Communications (RS.CO)

Third Party Relevance: Controls
Rationale: Companies should ensure that communication channels are determined for incident response.
Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Respond. Communications		None	

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.4.2.a	Respond.Communications	No discussion of Information Sharing and Analysis Centers.	Workgroup Recommendation
3.4.2.b	Respond.Communications	Inadequate discussion of guidelines for response communications with third parties. They are adequate for an internal response function.	NIST 800-53A provides additional guidance for breach notifications. NIST 800-61r2 provides information on incident notification. NIST 800-150 provides recommendations for information sharing and handling

Gap 3.4.2.a:
The references did not discuss the Information Sharing and Analysis Centers.

Workgroup Recommendation:
To enhance and facilitate collaboration, companies involved in Third Party Collaboration (Joint Ventures or Major Capital Projects) should be to become members of the ONG-ISAC.

Gap 3.4.2.b:
The standards provide inadequate discussion of guidelines for response communications with third parties. They are also adequate for an internal response function.

Supplemental References 3.4.2.b (Same as 3.3.1, 3.3.2, 3.5.3; Additional NIST 800-150 reference)
While standards did not provide specific information for security alert thresholds or breach notifications, the NIST 800-53A Rev 4 standard provided some additional broad guidance for both areas. This standard also discussed incident handling, reporting and response. Meanwhile, NIST 800-61 Rev 2 provides information on incident notification and the indicators of an incident.
NIST 800-53A Revision 4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations
Building Effective Assessment Plans

December 2014
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

- IR-4(8) - Incident Handling - Correlation With External Organizations
    - This section requires defining the information to be correlated and shared with external organizations.

- IR-6 - Incident Reporting
    - This section states that an organization should report incidents within a defined time period.

- IR-7(2) - Incident Response Assistance - Coordination With External Providers
    - This section requires establishing relationships between a company's incident response teams and the external providers.

- SI-4(5) - Information System Monitoring - System-Generated Alerts
- SI-4(7) - Information System Monitoring - Automated Response To Suspicious Events
- SI-7(8) - Software, Firmware, And Information Integrity - Auditing Capability For Significant Events
- SI-4(12) - Information System Monitoring - Automated Alerts
    - These sections state that personnel or roles to be alerted should be defined for indicators of compromise, suspicious events, integrity violations and inappropriate or unusual activities.

- SI-5 - Security Alerts, Advisories, And Directives
    - This section states that a company should receive information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.

- SI-5(1) - Security Alerts, Advisories, And Directives - Automated Alerts And Advisories
    - This section discusses having an understanding of the automated mechanisms available to the organization for security alerts and advisories.

- SI-4(22) - Information System Monitoring - Unauthorized Network Services
    - This standard requires that organizations define personnel or roles to be alerted upon the detection of unauthorized or unapproved network services.

NIST SP 800-61 Rev 2
Computer Security Incident Handling Guide
August 2012
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- 3.2.7 - Incident Notification
    - This section provides a suggested list of individuals to be notified which includes external providers.

NIST 800-150
Guide to Cyber Threat Information Sharing
October 2016
Table 3-2 provides recommendations for handling sensitive data
Table 3-3 provides the traffic light protocol for disclosure ratings.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

3.4.3 Respond. Analysis (RS.AN)

Third Party Relevance: Controls
Rationale: Companies should ensure the appropriate analysis is performed on incidents and provided to another company as agreed.
Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Respond.Analysis	RS.AN-1: Notifications from detection systems are investigated	IEC62443-3-3	Providing an Application Programming Interface (API) for log access is recommended in IEC62443-3-3.

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Respond.Analysis	RS.AN-2: The impact of the incident is understood		No additional references
Respond.Analysis	RS.AN-3: Forensics are performed	IEC62443-3-3	IEC62443 discusses the need for timestamps and the ability to track whether a human performed a certain action (non-repudiation).

Gaps

Gap#	Function.Category	Gap	Recommended Reference
N/A	Respond.Analysis	No Gaps	

3.4.4 Respond. Mitigation (RS.MI)

Third Party Relevance: Controls

Rationale: In collaborating with third parties, it is important to ensure that, should an incident occur, the appropriate processes and activities are in place to prevent the expansion of an event, mitigate its effects, and eradicate the incident.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Respond. Mitigation		None	

Gaps

Gap#	Function.Category	Gap	Recommended Reference

N/A	Respond.Mitigation	No Gaps	

3.4.5 Respond. Improvements (RS.IM)

Third Party Relevance: Checklist

Rationale: Improving organizational response activities is important, but the detailed controls do not need to be monitored and reviewed for secure Third Party Collaboration.

However, as part of the contractual processes in engagements with Third Parties, the Third Party organization should confirm that improvement processes are in place. This is more of a checklist item than a list of controls that need to be implemented.

3.5 Recover

3.5.1 Recover. Recovery Planning (RC.RP)

Third Party Relevance: Controls

Rationale: Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments
Respond. Communications		None	

Gaps

Gap#	Function.Category	Gap	Recommended Reference
N/A	Respond.Communications	No Gaps	

3.5.2 Recover. Improvements (RC.IM)

Third Party Relevance: Checklist

Rationale: Improving recovery planning and processes are important, but the detailed controls do not need to be monitored and reviewed for third party collaboration.

However, as part of the contractual processes in engagements with Third Parties, the Third Party organization should confirm that improvement processes are in place. This is more of a checklist item than a list of controls that need to be implemented.

3.5.3 Recover. Communications (RC.CO)

Third Party Relevance: Controls

Rationale: Companies should ensure that communication channels are determined and coordinated as a company recovers from an incident.

Baseline References: NIST SP 800-53(business technologies), ISA 62443-3-3:2013 (operational technologies)

Additional Recommended Informative References and Observations

Function. Category	Subcategory	Reference Recommendation in addition to NIST	Comments/Rationale
Recover. Communications	None		

Gaps

Gap#	Function.Category	Gap	Recommended Reference
3.5.3	Recover.Communications	No mention of incident coordination with a third party.	NIST 800-53A provides additional guidance for breach notifications. NIST 800-61r2 provides information on incident notification. NIST 800-150 provides recommendations for information sharing and handling

Supplemental References 3.5.3 (Same as 3.3.1, 3.3.2, 3.4.2 Additional NIST 800-150 reference)
While standards did not provide specific information for security alert thresholds or breach notifications, the NIST 800-53A Rev 4 standard provided some additional broad guidance for both areas. This standard also discussed incident handling, reporting and response. Meanwhile, NIST 800-61 Rev 2 provides information on incident notification and the indicators of an incident.
NIST 800-53A Revision 4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations
Building Effective Assessment Plans
December 2014
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

- IR-4(8) - Incident Handling - Correlation With External Organizations
    - This section requires defining the information to be correlated and shared with external organizations.

- IR-6 - Incident Reporting
    - This section states that an organization should report incidents within a defined time period.

- IR-7(2) - Incident Response Assistance - Coordination With External Providers
    - This section requires establishing relationships between a company's incident response teams and the external providers.

- SI-4(5) - Information System Monitoring - System-Generated Alerts
- SI-4(7) - Information System Monitoring - Automated Response To Suspicious Events
- SI-7(8) - Software, Firmware, And Information Integrity - Auditing Capability For Significant Events
- SI-4(12) - Information System Monitoring - Automated Alerts
    - These sections state that personnel or roles to be alerted should be defined for indicators of compromise, suspicious events, integrity violations and inappropriate or unusual activities.

- SI-5 - Security Alerts, Advisories, And Directives
    - This section states that a company should receive information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.

- SI-5(1) - Security Alerts, Advisories, And Directives - Automated Alerts And Advisories

- This section discusses having an understanding of the automated mechanisms available to the organization for security alerts and advisories.

- SI-4(22) - Information System Monitoring - Unauthorized Network Services
  - This standard requires that organizations define personnel or roles to be alerted upon the detection of unauthorized or unapproved network services.

NIST SP 800-61 Rev 2
Computer Security Incident Handling Guide
August 2012
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- 3.2.7 - Incident Notification
  - This section provides a suggested list of individuals to be notified which includes external providers.

NIST 800-150
Guide to Cyber Threat Information Sharing
October 2016
Table 3-2 provides recommendations for handling sensitive data
Table 3-3 provides the traffic light protocol for disclosure ratings.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

4 Contractual Language and Legal Review

API ITSS is unable to make specific contractual language recommendations. Some areas that should be addressed in a contract include:

1) Commercially Sensitive Information
2) Data privacy
3) Indemnity
4) Intellectual property
5) Service agreement terms and conditions
6) Trade Controls.

In addition, contracts should include IT Security Standards as a baseline reference into contracts with Third Parties with access to Company infrastructure and/or IT systems needs. This profile may be used as input into the baseline standards for contracts.

Standards are available for the language to be used for the procurement of control system technology.

Cybersecurity Procurement Language for Energy Delivery Systems
April 2014
Energy Sector Control Systems Working Group (ESCSWG)
http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Cyber Security Procurement Language for Control Systems
Version 1.8
Sponsor: Department of Homeland Security,
National Cyber Security Division
Contributors: Idaho National Laboratory, State of New York
Multi-State Information Sharing Analysis Center (MSISAC),
System Audit Network Security (SANS)
February 2008
http://energy.gov/oe/downloads/cyber-security-procurement-language-control-systems-version-18

The planning/assessment, governance, and communications efforts should include a thorough review by appropriate company-level law functions. These include:

1) ID.RA – Identify.Risk Assessment
2) ID. GV – Identify.Governance
3) RS.RP – Respond.Response Planning
4) RS.CO – Respond.Communications
5) RC.RP – Recover.Recovery Planning
6) RC.CO – Recover.Communications

Companies will work to establish their own protocols within this NIST profile, and companies should ensure that they are not violating any antitrust guidelines.

Appendix A. List of NIST Framework References

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-2: Software platforms and applications within the organization are inventoried	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
IDENTIFY (ID)	Asset Management	ID.AM-3: Organizational communication and data flows are mapped	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
IDENTIFY (ID)	Asset Management	ID.AM-4: External information systems are catalogued	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
IDENTIFY (ID)	Asset Management	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
IDENTIFY (ID)	Business Environment (ID.BE): 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.	ID.BE-1: The organization's role in the supply chain is identified and communicated	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-5: Resilience requirements to support delivery of critical services are established	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all families
IDENTIFY (ID)	Governance (ID.GV)	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Governance (ID.GV)	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· COBIT 5 MEA03.01, MEA03.04 · ISA 62443-2-1:2009 4.4.3.7 · ISO/IEC 27001:2013 A.18.1 · NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
IDENTIFY (ID)	Governance (ID.GV)	ID.GV-4: Governance and risk management processes address cybersecurity risks	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 PM-9, PM-11
IDENTIFY (ID)	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	· CCS CSC 4 · COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.6.1.4 · NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-3: Threats, both internal and external, are identified and documented	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-4: Potential business impacts and likelihoods are identified	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· COBIT 5 APO12.02 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-6: Risk responses are identified and prioritized	· COBIT 5 APO12.05, APO13.02 · NIST SP 800-53 Rev. 4 PM-4, PM-9
IDENTIFY (ID)	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	· COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · ISA 62443-2-1:2009 4.3.4.2 · NIST SP 800-53 Rev. 4 PM-9
IDENTIFY (ID)	Risk Management Strategy (ID.RM)	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.2.6.5 · NIST SP 800-53 Rev. 4 PM-9

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Risk Management Strategy (ID.RM)	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	· CCS CSC 16 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family
PROTECT (PR)	Access Control (PR.AC)	PR.AC-2: Physical access to assets is managed and protected	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	· COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISA 62443-3-3:2013 SR 1.13, SR 2.6 · ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20

Function	Category	Subcategory	Informative References
PROTECT (PR)	Access Control (PR.AC)	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · ISA 62443-3-3:2013 SR 2.1 · ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16
PROTECT (PR)	Access Control (PR.AC)	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, SC-7
PROTECT (PR)	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	· CCS CSC 9 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13

Function	Category	Subcategory	Informative References
PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-2: Privileged users understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-3, PM-13
PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.03, APO10.04, APO10.05 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 PS-7, SA-9
PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-4: Senior executives understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-5: Physical and information security personnel understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13

Function	Category	Subcategory	Informative References
PROTECT (PR)	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	· CCS CSC 17 · COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28
PROTECT (PR)	Data Security (PR.DS)	PR.DS-2: Data-in-transit is protected	· CCS CSC 17 · COBIT 5 APO01.06, DSS06.06 · ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SC-8
PROTECT (PR)	Data Security (PR.DS)	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.4.3.3.3.9, 4.3.4.4.1 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
PROTECT (PR)	Data Security (PR.DS)	PR.DS-4: Adequate capacity to ensure availability is maintained	· COBIT 5 APO13.01 · ISA 62443-3-3:2013 SR 7.1, SR 7.2 · ISO/IEC 27001:2013 A.12.3.1 · NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5

Function	Category	Subcategory	Informative References
PROTECT (PR)	Data Security (PR.DS)	PR.DS-5: Protections against data leaks are implemented	· CCS CSC 17 · COBIT 5 APO01.06 · ISA 62443-3-3:2013 SR 5.2 · ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PROTECT (PR)	Data Security (PR.DS)	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 · ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SI-7
PROTECT (PR)	Data Security (PR.DS)	PR.DS-7: The development and testing environment(s) are separate from the production environment	· COBIT 5 BAI07.04 · ISO/IEC 27001:2013 A.12.1.4 · NIST SP 800-53 Rev. 4 CM-2

Function	Category	Subcategory	Informative References
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	· CCS CSC 3, 10 · COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-2: A System Development Life Cycle to manage systems is implemented	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.3 · ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-3: Configuration change control processes are in place	· COBIT 5 BAI06.01, BAI01.06 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10

Function	Category	Subcategory	Informative References
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-6: Data is destroyed according to policy	· COBIT 5 BAI09.03 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · NIST SP 800-53 Rev. 4 MP-6
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-7: Protection processes are continuously improved	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6

Function	Category	Subcategory	Informative References
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	· ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· COBIT 5 DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 · NIST SP 800-53 Rev. 4 CP-2, IR-8
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-10: Response and recovery plans are tested	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.17.1.3 · NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 · NIST SP 800-53 Rev. 4 PS Family

Function	Category	Subcategory	Informative References
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-12: A vulnerability management plan is developed and implemented	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
PROTECT (PR)	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.3.3.7 · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 · NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
PROTECT (PR)	Maintenance (PR.MA)	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 · NIST SP 800-53 Rev. 4 MA-4
PROTECT (PR)	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· CCS CSC 14 · COBIT 5 APO11.04 · ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family

Function	Category	Subcategory	Informative References
PROTECT (PR)	Protective Technology (PR.PT)	PR.PT-2: Removable media is protected and its use restricted according to policy	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7
PROTECT (PR)	Protective Technology (PR.PT)	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · ISO/IEC 27001:2013 A.9.1.2 · NIST SP 800-53 Rev. 4 AC-3, CM-7
PROTECT (PR)	Protective Technology (PR.PT)	PR.PT-4: Communications and control networks are protected	· CCS CSC 7 · ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7

Function	Category	Subcategory	Informative References
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-2: Detected events are analyzed to understand attack targets and methods	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· ISA 62443-3-3:2013 SR 6.1 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-4: Impact of events is determined	· COBIT 5 APO12.06 · NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-5: Incident alert thresholds are established	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.2.3.10 · NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

Function	Category	Subcategory	Informative References
DETECT (DE)	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	· CCS CSC 14, 16 · COBIT 5 DSS05.07 · ISA 62443-3-3:2013 SR 6.2 · NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· ISA 62443-2-1:2009 4.3.3.3.8 · NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· ISA 62443-3-3:2013 SR 6.2 · ISO/IEC 27001:2013 A.12.4.1 · NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-4: Malicious code is detected	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.3.4.3.8 · ISA 62443-3-3:2013 SR 3.2 · ISO/IEC 27001:2013 A.12.2.1 · NIST SP 800-53 Rev. 4 SI-3
DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-5: Unauthorized mobile code is detected	· ISA 62443-3-3:2013 SR 2.4 · ISO/IEC 27001:2013 A.12.5.1 · NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44

Function	Category	Subcategory	Informative References
DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· COBIT 5 APO07.06 · ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 · NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-8: Vulnerability scans are performed	· COBIT 5 BAI03.10 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-5
DETECT (DE)	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.4.3.1 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
DETECT (DE)	Detection Processes (DE.DP)	DE.DP-2: Detection activities comply with all applicable requirements	· ISA 62443-2-1:2009 4.4.3.2 · ISO/IEC 27001:2013 A.18.1.4 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4

Function	Category	Subcategory	Informative References
DETECT (DE)	Detection Processes (DE.DP)	DE.DP-3: Detection processes are tested	· COBIT 5 APO13.02 · ISA 62443-2-1:2009 4.4.3.2 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
DETECT (DE)	Detection Processes (DE.DP)	DE.DP-4: Event detection information is communicated to appropriate parties	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.4.5.9 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
DETECT (DE)	Detection Processes (DE.DP)	DE.DP-5: Detection processes are continuously improved	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RP)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1:2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8

Function	Category	Subcategory	Informative References
RESPOND (RP)	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 · NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
RESPOND (RP)	Communications (RS.CO)	RS.CO-2: Events are reported consistent with established criteria	· ISA 62443-2-1:2009 4.3.4.5.5 · ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
RESPOND (RP)	Communications (RS.CO)	RS.CO-3: Information is shared consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.2 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RESPOND (RP)	Communications (RS.CO)	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.5 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RESPOND (RP)	Communications (RS.CO)	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· NIST SP 800-53 Rev. 4 PM-15, SI-5

Function	Category	Subcategory	Informative References
RESPOND (RP)	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated	· COBIT 5 DSS02.07 · ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RESPOND (RP)	Analysis (RS.AN)	RS.AN-2: The impact of the incident is understood	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4
RESPOND (RP)	Analysis (RS.AN)	RS.AN-3: Forensics are performed	· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · ISO/IEC 27001:2013 A.16.1.7 · NIST SP 800-53 Rev. 4 AU-7, IR-4
RESPOND (RP)	Analysis (RS.AN)	RS.AN-4: Incidents are categorized consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.6 · ISO/IEC 27001:2013 A.16.1.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
RESPOND (RP)	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained	· ISA 62443-2-1:2009 4.3.4.5.6 · ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4

Function	Category	Subcategory	Informative References
RESPOND (RP)	Mitigation (RS.MI)	RS.MI-2: Incidents are mitigated	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 · ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
RESPOND (RP)	Mitigation (RS.MI)	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
RESPOND (RP)	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RESPOND (RP)	Improvements (RS.IM)	RS.IM-2: Response strategies are updated	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
RECOVER (RC)	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	Improvements (RC.IM)	RC.IM-2: Recovery strategies are updated	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

Function	Category	Subcategory	Informative References
RECOVER (RC)	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	· COBIT 5 EDM03.02
RECOVER (RC)	Communications (RC.CO)	RC.CO-2: Reputation after an event is repaired	· COBIT 5 MEA03.02
RECOVER (RC)	Communications (RC.CO)	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· NIST SP 800-53 Rev. 4 CP-2, IR-4

Appendix B. NIST 800-82r2 Recommendations for NIST SP 800-53 Framework References

The column called "NIST SP 800-53 References in NIST Framework" contains the NIST 800-53 references listed in the NIST Cybersecurity Framework. The column "NIST 800-82 Recommendations for ICS" contains the references from the 800-53 list that pertain to Industrial Control Systems, as recommended in NIST 800-82.

Subcategory	NIST SP 800-53 References in NIST Framework	NIST SP 800-82 Recommendations for ICS
ID.AM-1: Physical devices and systems within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8	NIST SP 800-53 Rev. 4 CM-8
ID.AM-2: Software platforms and applications within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8	NIST SP 800-53 Rev. 4 CM-8
ID.AM-3: Organizational communication and data flows are mapped	NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8	NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
ID.AM-4: External information systems are catalogued	NIST SP 800-53 Rev. 4 AC-20, SA-9	NIST SP 800-53 Rev. 4 AC-20, SA-9
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14	NIST SP 800-53 Rev. 4 CP-2, RA-2
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11	NIST SP 800-53 Rev. 4 CP-2, PS-7
ID.BE-1: The organization's role in the supply chain is identified and communicated	NIST SP 800-53 Rev. 4 CP-2, SA-12	NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	NIST SP 800-53 Rev. 4 PM-8	None

Subcategory	NIST SP 800-53 References in NIST Framework	NIST SP 800-82 Recommendations for ICS
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	NIST SP 800-53 Rev. 4 PM-11, SA-14	None
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14	NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11
ID.BE-5: Resilience requirements to support delivery of critical services are established	NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14	NIST SP 800-53 Rev. 4 CP-2
ID.GV-1: Organizational information security policy is established	NIST SP 800-53 Rev. 4 -1 controls from all families	
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	NIST SP 800-53 Rev. 4 PM-1, PS-7	NIST SP 800-53 Rev. 4 PS-7
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)	
ID.GV-4: Governance and risk management processes address cybersecurity risks	NIST SP 800-53 Rev. 4 PM-9, PM-11	None
ID.RA-1: Asset vulnerabilities are identified and documented	NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5	NIST SP 800-53 Rev. 4 SI-5
ID.RA-3: Threats, both internal and external, are identified and documented	NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	NIST SP 800-53 Rev. 4 RA-3, SI-5

Subcategory	NIST SP 800-53 References in NIST Framework	NIST SP 800-82 Recommendations for ICS
ID.RA-4: Potential business impacts and likelihoods are identified	NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14	NIST SP 800-53 Rev. 4 RA-2, RA-3
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16\	NIST SP 800-53 Rev. 4 RA-2, RA-3
ID.RA-6: Risk responses are identified and prioritized	NIST SP 800-53 Rev. 4 PM-4, PM-9	None
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	NIST SP 800-53 Rev. 4 PM-9	None
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	NIST SP 800-53 Rev. 4 PM-9	None
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14	None
PR.AC-1: Identities and credentials are managed for authorized devices and users	NIST SP 800-53 Rev. 4 AC-2, IA Family	NIST SP 800-53 Rev. 4 AC-2, Some IA
PR.AC-2: Physical access to assets is managed and protected	NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
PR.AC-3: Remote access is managed	NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20	NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16	NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	NIST SP 800-53 Rev. 4 AC-4, SC-7	NIST SP 800-53 Rev. 4 AC-4, SC-7
PR.AT-1: All users are informed and trained	NIST SP 800-53 Rev. 4 AT-2, PM-13	NIST SP 800-53 Rev. 4 AT-2

Subcategory	NIST SP 800-53 References in NIST Framework	NIST SP 800-82 Recommendations for ICS
PR.AT-2: Privileged users understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13	NIST SP 800-53 Rev. 4 AT-3
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	NIST SP 800-53 Rev. 4 PS-7, SA-9	NIST SP 800-53 Rev. 4 PS-7, SA-9
PR.AT-4: Senior executives understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13	NIST SP 800-53 Rev. 4 AT-3
PR.AT-5: Physical and information security personnel understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13	NIST SP 800-53 Rev. 4 AT-3
PR.DS-1: Data-at-rest is protected	NIST SP 800-53 Rev. 4 SC-28	NIST SP 800-53 Rev. 4 SC-28
PR.DS-2: Data-in-transit is protected	NIST SP 800-53 Rev. 4 SC-8	NIST SP 800-53 Rev. 4 SC-8
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16	NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
PR.DS-4: Adequate capacity to ensure availability is maintained	NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5	NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
PR.DS-5: Protections against data leaks are implemented	NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PS-3, PS-6, SC-7, SC-8, SC-13, SI-4
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	NIST SP 800-53 Rev. 4 SI-7	NIST SP 800-53 Rev. 4 SI-7
PR.DS-7: The development and testing environment(s) are separate from the production environment	NIST SP 800-53 Rev. 4 CM-2	NIST SP 800-53 Rev. 4 CM-2
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

Subcategory	NIST SP 800-53 References in NIST Framework	NIST SP 800-82 Recommendations for ICS
PR.IP-2: A System Development Life Cycle to manage systems is implemented	NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8	NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
PR.IP-3: Configuration change control processes are in place	NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10	NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
PR.IP-4: Backups of information are conducted, maintained, and tested periodically	NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9	NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
PR.IP-6: Data is destroyed according to policy	NIST SP 800-53 Rev. 4 MP-6	NIST SP 800-53 Rev. 4 MP-6
PR.IP-7: Protection processes are continuously improved	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4	NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	NIST SP 800-53 Rev. 4 CP-2, IR-8	NIST SP 800-53 Rev. 4 CP-2, IR-8
PR.IP-10: Response and recovery plans are tested	NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14	NIST SP 800-53 Rev.4 CP-4, IR-3
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	NIST SP 800-53 Rev. 4 PS Family	NIST SP 800-53 Rev. 4 PS Family (some PS)
PR.IP-12: A vulnerability management plan is developed and implemented	NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2

Subcategory	NIST SP 800-53 References in NIST Framework	NIST SP 800-82 Recommendations for ICS
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5	NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	NIST SP 800-53 Rev. 4 MA-4	NIST SP 800-53 Rev. 4 MA-4
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	NIST SP 800-53 Rev. 4 AU Family	NIST SP 800-53 Rev. 4 Some AU Family
PR.PT-2: Removable media is protected and its use restricted according to policy	NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7	NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	NIST SP 800-53 Rev. 4 AC-3, CM-7	NIST SP 800-53 Rev. 4 AC-3, CM-7
PR.PT-4: Communications and control networks are protected	NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7	NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4	NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: Impact of events is determined	NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4	NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
DE.AE-5: Incident alert thresholds are established	NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

Subcategory	NIST SP 800-53 References in NIST Framework	NIST SP 800-82 Recommendations for ICS
DE.CM-1: The network is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20	NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-10, CM-11
DE.CM-4: Malicious code is detected	NIST SP 800-53 Rev. 4 SI-3	NIST SP 800-53 Rev. 4 SI-3
DE.CM-5: Unauthorized mobile code is detected	NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44	NIST SP 800-53 Rev. 4 SC-18, SI-4
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4	NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, SI-4
DE.CM-8: Vulnerability scans are performed	NIST SP 800-53 Rev. 4 RA-5	NIST SP 800-53 Rev. 4 RA-5
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14	NIST SP 800-53 Rev. 4 CA-2, CA-7
DE.DP-2: Detection activities comply with all applicable requirements	NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4	NIST SP 800-53 Rev. 4 CA-2, CA-7, SI-4
DE.DP-3: Detection processes are tested	NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4
DE.DP-4: Event detection information is communicated to appropriate parties	NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4

Subcategory	NIST SP 800-53 References in NIST Framework	NIST SP 800-82 Recommendations for ICS
DE.DP-5: Detection processes are continuously improved	NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4,
RS.RP-1: Response plan is executed during or after an event	NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8	NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
RS.CO-1: Personnel know their roles and order of operations when a response is needed	NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8	NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
RS.CO-2: Events are reported consistent with established criteria	NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8	NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
RS.CO-3: Information is shared consistent with response plans	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	NIST SP 800-53 Rev. 4 PM-15, SI-5	NIST SP 800-53 Rev. 4 SI-5
RS.AN-1: Notifications from detection systems are investigated	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: The impact of the incident is understood	NIST SP 800-53 Rev. 4 CP-2, IR-4	NIST SP 800-53 Rev. 4 CP-2, IR-4
RS.AN-3: Forensics are performed	NIST SP 800-53 Rev. 4 AU-7, IR-4	NIST SP 800-53 Rev. 4 AU-7, IR-4
RS.AN-4: Incidents are categorized consistent with response plans	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
RS.MI-1: Incidents are contained	NIST SP 800-53 Rev. 4 IR-4	NIST SP 800-53 Rev. 4 IR-4
RS.MI-2: Incidents are mitigated	NIST SP 800-53 Rev. 4 IR-4	NIST SP 800-53 Rev. 4 IR-4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5	NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5

Subcategory	NIST SP 800-53 References in NIST Framework	NIST SP 800-82 Recommendations for ICS
RS.IM-1: Response plans incorporate lessons learned	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RS.IM-2: Response strategies are updated	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RC.RP-1: Recovery plan is executed during or after an event	NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8	NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
RC.IM-1: Recovery plans incorporate lessons learned	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RC.IM-2: Recovery strategies are updated	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RC.CO-1: Public relations are managed	None	None
RC.CO-2: Reputation after an event is repaired	None	None
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	NIST SP 800-53 Rev. 4 CP-2, IR-4	NIST SP 800-53 Rev. 4 CP-2, IR-4

Appendix C. NIST Framework References

If the various standards organizations approve including the NIST Framework References that were reviewed to establish these guidelines, they will be included in this Appendix.