

Pipeline Control Systems Cybersecurity

API STANDARD 1164
THIRD EDITION, AUGUST 2021

ERRATA 1, AUGUST 2021



Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed. The use of API publications is voluntary. In some cases, third parties or authorities having jurisdiction may choose to incorporate API standards by reference and may mandate compliance.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

All rights reserved. No part of this work may be reproduced, translated, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001-5571.

Copyright © 2021 American Petroleum Institute

Foreword

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

The verbal forms used to express the provisions in this document are as follows.

Shall: As used in a standard, “shall” denotes a minimum requirement in order to conform to the standard.

Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the standard.

May: As used in a standard, “may” denotes a course of action permissible within the limits of a standard.

Can: As used in a standard, “can” denotes a statement of possibility or capability.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 200 Massachusetts Avenue, Suite 1100, Washington, DC 20001. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

The American Petroleum Institute maintains this standard under continuous maintenance procedures. These procedures establish a documented program for regular publication of addenda or revisions, including timely and documented consensus action on requests for revisions to any part of the standard. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 200 Massachusetts Avenue, Suite 1100, Washington, DC 20001.

Suggested revisions are invited and should be submitted at any time to the Standards Department, API, 200 Massachusetts Avenue, Suite 1100, Washington, DC 20001, standards@api.org.

Contents

	Page
1 Scope	1
1.1 Purpose	1
1.2 Intended Audience	2
1.3 How to Read This Standard	2
2 Normative References	4
3 Terms, Definitions, Acronyms, and Abbreviations	4
3.1 Terms and Definitions	4
3.2 Acronyms	9
4 ONG Pipeline IAC Cybersecurity Profiles	10
4.1 IAC Cybersecurity Profile-Introduction	10
4.2 IAC Cybersecurity Profile-Common Constraints	10
4.3 IAC Cybersecurity Profile-Threat Protection Objectives	11
4.4 IAC Cybersecurity Profile-Business and Mission Objectives	12
4.5 IAC Cybersecurity Profile-Objectives Impact to Threat Protection Mapping	13
5 ONG IAC Cybersecurity Policy, Plan, and Program	13
5.1 IAC Cybersecurity Plan-Development	15
5.2 IAC Cybersecurity Plan-Risk Management Foundation	15
5.3 IAC Cybersecurity Plan-Operationalizing an IAC Cybersecurity Program	17
5.4 IAC Cybersecurity Plan-Selecting Cybersecurity Profiles	18
5.5 IAC Cybersecurity Plan-Customizing Selected Profile Requirements	27
6 ONG IAC Cybersecurity Profile Requirements-Identify (ID)	28
6.1 Governance (ID.GV)	28
6.2 Risk Management Strategy (ID.RM)	32
6.3 Business Environment (ID.BE)	35
6.4 Supply Chain Risk Management (ID.SC)	39
6.5 IAC Risk Assessment (ID.RA)	42
6.6 Asset Management (ID.AM)	49
7 ONG IAC Cybersecurity Profile Requirements-Protect (PR)	55
7.1 Access Control (PR.AC)	56
7.2 IAC Cybersecurity Awareness and Training (PR.AT)	63
7.3 Data Security (PR.DS)	67
7.4 Information Protection Processes and Procedures (PR.IP)	75
7.5 Maintenance (PR.MA)	89
7.6 Protective Technology (PR.PT)	92
8 ONG IAC Cybersecurity Profile Requirements-Detect (DE)	97
8.1 Anomalies and Events (DE.AE)	97
8.2 Security Continuous Monitoring (DE.CM)	100
8.3 Detection Processes (DE.DP)	106
9 ONG IAC Cybersecurity Profile Requirements-Respond (RS)	110
9.1 Response Planning (RS.RP)	110
9.2 Communications (RS.CO)	111
9.3 Analysis (RS.AN)	114
9.4 Mitigation (RS.MI)	118
9.5 Improvements (RS.IM)	120

Contents

	Page
10 ONG IAC Cybersecurity Profile Requirements-Recover (RC)	122
10.1 Recovery Planning (RC.RP):	122
10.2 Improvements (RC.IM)	122
10.3 Communications (RC.CO)	124
Annex A (informative) API Standard 1164 Construction and Mapping	126
Annex B (informative) Plan-Do-Check-Act Model	129
Annex C (informative) Recurring Actions	131
Bibliography	132
Figures	
1 API 1164 Security Level Threat Protection Objectives	12
2 API 1164 Business Objective Impact Mapping to Threat Protection Profiles	13
3 API 1164 CSF Sources for IAC Cybersecurity Policy and Plan	14
4 IAC Cybersecurity Plan Development Participation	15
A.1 TSA Cybersecurity Measures to CSF Core Mapping	126
A.2 CSF Core Mapping to Pipeline Target Profile Requirements	127
A.3 NIST CSF Informative References	128
A.4 API 1164 Content Creation Mapping	128
B.1 Plan-Do-Check-Act (PDCA) Cycle	130
Tables	
C.1 Recurring Action Requirements	131

Background

This standard was developed using U.S. Transportation Security Administration's (TSA) *Pipeline Security* Guidelines (March 2018), especially Section 7, "Pipeline Cyber Asset Security Measures." This standard is based on the U.S. National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (CSF) (April 16, 2018), addressing all functions, categories, and subcategories. Activities were selected from the CSF core, with a focus and scoping of industrial automation and control (IAC) environments for the oil and natural gas (ONG) pipeline industry. Special attention was given to common risk management considerations, legal and regulatory requirements (e.g., TSA, FERC, DOT, PHMSA, etc.), and shared business/mission objectives.

This document is specifically written to provide an industry targeted IAC cybersecurity standard for the owner/operators of pipelines regulated under *Code of Federal Regulations (CFR) Title 49 for Transportation, Volume 2, Chapter I, Pipeline and Hazardous Materials Safety Administration (PHMSA), Department of Transportation, Part 192 – Transportation of Natural and Other Gas by Pipeline: Minimum Federal Safety Standards or Part 195 - Transportation of Hazardous Liquids by Pipeline*. This targeted standard specifies the framework, practices, and requirements needed to develop, implement, maintain, test, and constantly improve a robust IAC security program as part of the TSA's required Corporate Security Program. References to these regulations were incorporated at the time of this document's publication. Users are responsible for conforming to current and applicable regulations.

Pipeline Control Systems Cybersecurity

1 Scope

1.1 Purpose

This standard provides requirements and guidance for managing cyber risk associated with industrial automation and control (IAC) environments to achieve security, integrity, and resiliency objectives. Within this standard, this is accomplished through proper isolation of IAC environments from non-IAC environments to help IAC operational continuity.

Even with proper isolation of IAC environments from IT environments, both play a part in overall business continuity. IAC operational continuity and IT system continuity are often developed and implemented jointly as part of the overall business continuity plan.

The scope of this standard is limited to only the IAC cybersecurity aspects that can influence overall business continuity.

This standard is tailored for the oil and natural gas (ONG) pipeline industry, which includes, but is not limited to, natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems, liquefied natural gas (LNG) facilities, propane air facilities, and others involved in these industries.

This standard was developed to provide an actionable approach to protect IAC essential functions by managing cybersecurity risk to IAC environments. IAC environments can include, but are not limited to, supervisory control and data acquisition (SCADA), local control, and industrial internet of things (IIoT) solutions. This standard should be used in the context of developing, implementing, maintaining, and improving an IAC cybersecurity program, which includes the policies, processes, and procedural and technical controls for IAC cyber environments.

This standard is a set of requirements that should be customized prior to implementation using the company's risk management processes. The outcome is a customized, company-specific set of requirements for an IAC cybersecurity program to help manage the cybersecurity posture and any resulting residual risk to its IAC environments in alignment with the company's mission, objectives, and risk strategy, and in accordance with its policies and procedures.

While identification of threats and impacts is critical to the development of the IAC cybersecurity program, a risk-based evaluation of each will ensure the program is appropriately implemented, executed, and sustained consistent with an organization's desired risk posture. This standard focuses on desired cybersecurity outcomes by defining requirements for specific business objective impact protection levels.

Although the principles defined in this standard could be applied to safety instrumented systems (SIS), they are out of scope of this document. The security requirements specified within this standard do not attempt to address potential impacts to SIS safety integrity level (SIL) selection or determination. Any use of this standard in SIS environments is at the implementer's discretion and risk.

For companies that already have an IAC cybersecurity program, including one or more approved program policies and a documented IAC cybersecurity plan or plans implemented or being implemented, this standard should be considered an augmentation to their existing cybersecurity program elements. In these situations, a process of mapping this standard to current IAC cybersecurity program elements will determine any API 1164 requirements not currently in the existing program. The implementation of any missing elements should be tailored and prioritized using the company's risk management processes. The tailoring process for API 1164 cybersecurity requirements is described in 5.5.

This standard is not intended to preclude the implementation or use of any current or emerging technologies as long as applicable requirements specified herein are properly implemented, risk appropriate, and consistent with the company's risk management strategy.

1.2 Intended Audience

This document covers details specific to pipeline systems. Readers of this document should be acquainted with operational technology, general computer security concepts, and communication protocols such as those used in networking. The intended audience is varied and includes the following:

- senior managers who are trying to understand implications and consequences as they justify and implement a pipeline system's cybersecurity program to mitigate impact on business functionality;
- managers who are responsible for pipeline systems;
- system administrators, engineers, and information technology (IT) professionals who administer, patch, or secure pipeline systems;
- control engineers, integrators, and architects who design or implement secure pipeline systems;
- software manufacturers;
- products and services vendors;
- regulators responsible for pipeline cybersecurity;
- other government stakeholders who are trying to understand the unique pipeline security needs;
- researchers, academic institutions, and analysts who are trying to understand the unique security needs of pipeline systems.

1.3 How to Read This Standard

In the context of this document, the terms "industrial automation and control system(s)," "industrial control system(s)," or "control system(s)" refer to supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and local control systems used in the oil and natural gas industries. They do not refer to safety instrumented systems (SIS), unless explicitly mentioned. The term SCADA or DCS refers to SCADA or DCS systems respectively at the exclusion of local control systems. When the term "local control" is used, it is distinguished from a SCADA or DCS system with which it may interact.

This standard specifies elements for a robust IAC cybersecurity program in the form of cybersecurity requirements. It is not intended that each requirement specify or even necessitate an individual cybersecurity control; rather, it defines a requisite cybersecurity capability, feature, or a procedural and technical control attribute. Often, multiple requirements can be combined into the creation, implementation, or testing of a single IAC cybersecurity control. If or to what extent this combining occurs is left up to the implementer as long as the requirements are met.

The security requirements in this standard align to a "target profile" for each business objective impact level. A "current profile" is represented by the outcomes specified in this standard that are currently implemented by a company and being achieved in its IAC cybersecurity program. This target profile and the current profile can be compared by identifying opportunities for improving the current cybersecurity posture and influencing process improvement priorities of the IAC cybersecurity program.

Prioritizing the mitigation of the gap between current and target profiles is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. The following are examples of how the target profile may be used:

- An operator can use it as its IAC cybersecurity program baseline.
- A pipeline industry member can extend it to build a more risk-based tailored industrial cybersecurity program.
- A pipeline industry member can utilize the target profile to express industrial cybersecurity risk management requirements to an external service provider.
- A pipeline industry member can express a system's cybersecurity state through a current profile to report results relative to the target profile.
- A pipeline industry member, having identified an external partner upon whom its infrastructure depends, can use the target profile to convey required cybersecurity outcomes.

To further understand the construction of this standard and how it maps to TSA Pipeline Security Guidelines, NIST CSF, and other IAC cybersecurity standards, refer to Annex A.

1.3.1 Document Structure

- **Section 2: Normative References**

- **Section 3: Terms, Definitions, Acronyms, and Abbreviations**

Provides definitions for terms, definitions, acronyms, and abbreviations used in this standard or that are relevant to understanding the background, context, or a concept covered by this standard.

- **Section 4: ONG Pipeline IAC Cybersecurity Profiles**

This section sets the foundation of pipeline IAC cybersecurity. It introduces the concept of three different security profiles mapped to three levels of threat protection objectives. This section also sets the foundational concepts of IAC cybersecurity common constraints of IAC essential functions and safety instrumented systems (SIS) considerations. Also defined in this section are six common pipeline business objectives and a mapping of those business objectives to each NIST CSF function, category, and subcategory. Lastly, this section maps the business objective impacts to threat protection objectives, then maps those threat protection objectives to security profiles.

- **Section 5: ONG IAC Cybersecurity Policy, Plan, and Program**

This section defines how to implement this standard. It builds on the foundation set in Section 4 by defining an IAC cybersecurity management system mandated by a company policy and documented in an IAC cybersecurity plan. The IAC cybersecurity plan has a cornerstone of risk management, including a risk strategy, risk assessment processes, and risk responses aligned to the risk strategy. The IAC cybersecurity policy and the IAC cybersecurity plan elements are defined as a set of requirements based on applicable security profiles. This section also defines the concepts of segregating IAC cyber assets into cybersecurity zones and connecting those zones using cybersecurity conduits. It also defines how to perform business objective impact assessments to select applicable security profile requirements for the IAC cybersecurity zones and IAC cybersecurity conduits.

- **Sections 6–10: ONG IAC Cybersecurity Profile Requirements**

These sections specify the cybersecurity requirements for the three cybersecurity profiles that are to be applied to the IAC security zones and IAC security conduits based on their business impact severity level.

- **Annex A: API Standard 1164 Construction and Mapping**

This section details the use and mapping of TSA Pipeline Security Guidelines, NIST CSF, and other IAC cybersecurity standards by API 1164.

- **Annex B: Plan-Do-Check-Act Model**

This annex describes the PDCA model, which may assist planning, implementing, monitoring, and improving an IAC cybersecurity program

— Annex C: Recurring Actions

This annex consolidates all recurring actions that have a definitive time frame or periodic frequency.

2 Normative References

The following referenced document is indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

U.S. Transportation Security Administration¹, *Pipeline Security Guidelines*, March 2018

3 Terms, Definitions, Acronyms, and Abbreviations

3.1 Terms and Definitions

3.1.1

asset

An object represented either physically, logically, or virtually that is owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization.

3.1.1

attack vector

A path or a means by which unauthorized access can be gained to a device or a network for malicious purposes.

3.1.2

boundary device

A communication asset residing in either a security zone or security conduit that provides an interface between a zone and the conduit.

3.1.3

critical infrastructure

Public or private assets, systems, and networks, whether physical or virtual, that are considered so vital to a nation's operations that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

3.1.4

critical services

Services provided or consumed that are necessary to strengthen and maintain a nation's reliable, functioning, and resilient critical infrastructure.

3.1.5

current profile

The "as is" state of an environment's cybersecurity.

3.1.6

cyber asset

A physical or virtual device with the following minimum resources: 1) digital logic processing capability (e.g., CPU, ASIC); 2) memory (volatile or permanent); 3) one communications port, which is used in IT or industrial automation control solutions.

¹ Transportation Security Administration, 601 South 12th Street, Arlington, Virginia 22202, www.tsa.gov.

3.1.7**cybersecurity plan**

One or more formal documents that specify all the requirements and outcomes of a cybersecurity program.

3.1.8**cybersecurity policy**

A high-level document that describes the overall security goals and defines requirements for “what” is done by “whom” to effectively manage cybersecurity risks.

3.1.9**cybersecurity program**

An operationalized cybersecurity plan that includes the people operating in the context of their roles and responsibilities, processes that drive cybersecurity outcomes (including the effectiveness and performance measurements of those outcomes), and the technologies that support the people and processes all intended to manage the cybersecurity risk.

3.1.10**digital technology**

The branch of scientific or engineering knowledge that deals with the creation and practical use of computerized (digital logic processing capability) devices, systems, methods, and processes.

3.1.10**external IAC transport service**

A network segment that is part of an IAC internal conduit and that is responsible for delivering IAC data to the application processes on host computers, but is outside the purview of an IAC cyber environment and controlled and managed by a separate legal entity, partner, vendor, supplier, joint-venture entity, or another function within the organization.

3.1.11**external zone**

A network outside the purview of an IAC cyber environment that is controlled and managed by a separate legal entity, partner, vendor, supplier, joint-venture entity, or another function within the organization.

3.1.12**IAC audit record**

The evidentiary artifact of the occurrence of an IAC security audit event.

3.1.13**IAC cyber asset**

A cyber asset within the security perimeter of an IAC segregated environment.

3.1.14**IAC cyber environment**

Any combination of two or more IAC cyber assets, IAC cyber systems, IAC security zones, or IAC security conduits being considered collectively. The scope can be as large as enterprise-wide or as constrained as two IAC cyber assets under joint consideration.

NOTE Depending on the contextual use, the scope may refer to the organization’s entire IAC cyber environment as segmented and segregated; a subset of the organization’s IAC environment as segmented and segregated; or a single IAC segregated environment (a security zone or a security conduit, or a zone conduit pair).

3.1.15**IAC cyber solution**

One or more IAC cyber assets integrated collectively into a single solution deployed within an IAC security zone or IAC security conduit, providing essential functions.

3.1.16**IAC cyber system**

A single IAC cyber asset or a grouping of IAC cyber assets distinguished as a single entity, designed to perform a discernably separate set of IAC essential functions.

3.1.17**IAC cybersecurity plan**

A cybersecurity plan scoped exclusively for IAC cyber environments that addresses specific IAC cybersecurity and IAC operational requirements, constraints, and considerations when defining an IAC cybersecurity program.

3.1.18**IAC cybersecurity policy**

A cybersecurity policy that describes the overall IAC cybersecurity goals and objectives, is approved by organizational leadership, and authorizes, mandates, or otherwise mandates an IAC cybersecurity program to achieve those goals.

3.1.19**IAC cybersecurity profile**

A collection of defined IAC cyber activities and desired outcomes (functions, categories, subcategories, procedures, practices, and controls) that manages risk to mission/business objectives and is bound by the constraints and requirements of a particular scenario.

3.1.20**IAC cybersecurity program**

An operationalized IAC cybersecurity plan that includes people operating in the context of their roles and responsibilities; processes that drive cybersecurity outcomes (including the effectiveness and performance measurements of those outcomes); and the technologies that support the people and processes to manage the cybersecurity risk.

3.1.21**IAC essential function**

A function that provides a capability that is required to maintain health, safety, the environment, and availability for the process under control. Includes at least the following three categories: 1) protection: functions performed by a safety instrumented system (SIS); 2) control: functions controlling a process and/or equipment; and 3) view: the ability of the operator to view and manipulate the equipment under control.

NOTE All uses of the term “essential function,” where not otherwise qualified, should be assumed to refer to an IAC essential function.

3.1.22**IAC external conduit**

An IAC security conduit that connects an external zone and an IAC intermediate zone to provide security control and protection.

NOTE See 5.4.1 for clarification of security zones and security conduits.

3.1.23**IAC intermediate conduit**

An IAC security conduit that connects to an IAC intermediate zone and an IAC internal zone to provide security control and protection.

3.1.24**IAC intermediate zone**

An IAC security zone that connects to an external zone using an IAC external conduit and connects to an IAC internal zone using an IAC intermediate conduit to indirectly present IAC data and services and provides external controlled access to IAC services by external users to an IAC security zone.

3.1.25**IAC internal conduit**

A security conduit that connects an IAC internal zone to a separate IAC internal zone.

3.1.26**IAC internal zone**

A single IAC cyber asset or a grouping of IAC cyber assets that implements a single-level IAC cybersecurity profile and only communicates with other cyber assets not in the IAC security zone using an IAC security conduit.

3.1.27**IAC security audit event**

A security audit event generated from an IAC cyber asset, IAC security zone, or an IAC security conduit.

3.1.28**IAC security conduit**

A security conduit used in an IAC cyber environment, including (all) IAC external conduit(s), IAC intermediate conduit(s), and IAC internal conduit(s).

NOTE When defining or referencing security requirements, the term “IAC security conduit” is to be interpreted that the security requirements are applicable to all IAC conduit types listed in this definition.

3.1.29**IAC security zone**

A security zone used in an IAC segregated environment, including IAC internal zone(s) and IAC intermediate zone(s).

NOTE When defining or referencing security requirements, the term “IAC security zones” is to be interpreted that the security requirements are applicable to all IAC zone types listed in this definition.

3.1.30**IAC segregated environment**

An IAC security zone (IAC intermediate zone or IAC internal zone) or an IAC security conduit (IAC external conduit, IAC intermediate conduit, or IAC internal conduit), or a combination of any IAC security zone and IAC security conduit being considered collectively.

NOTE When defining or referencing security requirements, the terms “IAC segregated environment” and “IAC segregated environments” are to be interpreted as the security requirements applied to the IAC security zone and IAC security conduit types listed in this definition.

3.1.31**IAC support asset**

A cyber asset that is used in the maintenance, management, configuration, or administration of an IAC cyber asset, IAC cyber system, or IAC cyber environment.

3.1.32**impact**

A measure of the loss or harm associated with a consequence.

3.1.33**industrial automation and control**

A collective term for the domain within the realm of digital technology that is limited to only that which is used in or in direct support of operating industrial processes, which includes, but is not limited to, sensors, instrumentation, devices, systems, communications technologies, firmware, software, and logic and sequencing rules.

3.1.34 information technology

A collective term for the domain within the realm of digital technology that is limited to only that which is used in or in direct support of business information processing, which includes, but is not limited to, hardware, communications technologies, software, and related services.

3.1.35 need-to-know security principle

An information protection security principle that requires that access to sensitive information is necessitated by its connection with or use in official duties and/or for the performance of a concrete official task.

3.1.36 network segmentation

The process of partitioning a network into smaller networks.

3.1.37 network segregation

The process of defining different cybersecurity protection rulesets using risk-based criteria and implementing those rules to manage the security of a network segment and its cyber assets.

3.1.38 physical asset

An asset that has mass and that can be perceived through visual or tactile human senses.

3.1.39 nonlocal access

Human user communication with an IAC cyber asset using a network connection whether originating from within the same IAC security zone as the IAC cyber asset or a different security zone, including an external security zone.

3.1.40 risk management strategy

A documented declaration of an organization's risk priorities, constraints on the risk assessment, response and monitoring alternatives, risk tolerances, and assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time.

3.1.41 security audit event

Any observable occurrence in a cyber asset that is significant and relevant to the security of the cyber asset and the environment in which that asset operates to meet specific and ongoing audit needs.

3.1.42 security conduit

A security zone that is specific to communication processes and that contains a logical grouping of assets that are used in, perform, monitor, and defend communications between security zones.

3.1.43 security perimeter

A physical or logical boundary that is defined for a system, domain, or enclave, within which a particular security policy or security architecture is applied.

NOTE The security perimeter may mirror a physical boundary of a facility or site for convenience or practical implementation reasons, but that is coincidental to a security zone's purpose and use.

3.1.44 security zone

A grouping of cyber assets that adhere to the same security controls, whose security posture is managed collectively, and that only communicates with other cyber assets outside the security perimeter using a security conduit.

3.1.45 target profile

The desired outcome or “to be” state of cybersecurity implementation.

3.1.46 threat

Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

3.1.47 vulnerability

A flaw or weakness in a computer system’s security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy. [NIST SP 800-47].

NOTE From NIST SP 800-47.

3.2 Acronyms

CSF	NIST Cybersecurity Framework
CFR	Code of Federal Regulation
CSIRT	computer security incident response team
DOT	U.S. Department of Transportation
FERC	Federal Energy Regulatory Commission
HSE	health, safety, and environment
IAC	industrial automation and control
IIoT	industrial internet of things
IT	information technology
ISA	International Society of Automation
NIST	National Institute of Standards and Technology
ONG	oil and natural gas industry
PHA	Process Hazard Analysis
PHMSA	Pipeline and Hazardous Materials Safety Administration
TSA	Transportation Security Administration

4 ONG Pipeline IAC Cybersecurity Profiles

4.1 IAC Cybersecurity Profile—Introduction

NIST CSF defines a “profile” as a representation of the outcomes based on business needs that an organization has selected from the CSF categories and subcategories. It can be characterized as the alignment of the policies, procedures, and practices to the functions, categories, and subcategories for a particular scenario.

An API 1164 profile is a collection of selected cybersecurity activities and desired outcomes (functions, categories, subcategories, and security requirements) for a particular scenario. The selection is based on certain constraints and business/mission objectives.

API 1164 specifies multiple profiles for different scenarios. These profiles provide actionable approaches to managing IAC cybersecurity risk. They define a set of requirements and cyber activities that are designed to drive outcomes to manage the potential risk to business missions and objectives. They are customized for natural gas and hazardous liquid transmission pipelines, natural gas distribution pipeline systems, liquefied natural gas facilities, and others involved in these industries.

4.1.1 Scenario Profiles

This document defines the following three scenario profiles.

4.1.1.1 Baseline Profile

This profile covers IAC cybersecurity program-wide cyber activities and outcomes for all business objectives for the ONG pipeline industry. It also specifies IAC cybersecurity activities and outcomes for IAC segregated environments with the potential for low-level impact to pipeline industry business objectives. The baseline profile defines the minimum-security requirements for IAC cyber assets.

4.1.1.2 Enhanced Profile

This profile includes API 1164 baseline profile cyber activities and outcomes, plus the IAC cybersecurity activities and outcomes for IAC segregated environments, with the potential for a medium-level impact to pipeline industry business objectives.

4.1.1.3 Extended Profile

This profile includes the API 1164 enhanced profile cyber activities and outcomes, plus IAC cybersecurity activities and outcomes for IAC segregated environments, with the potential for the highest-level impact to pipeline industry business objectives.

4.2 IAC Cybersecurity Profile—Common Constraints

The IAC cybersecurity requirements detailed in Sections 0 through 10 have been developed based on common constraints applicable to cyber activities and outcomes for all API 1164 profiles. The IAC environment fits underneath the broad designation of operational technology (OT) rather than information technology (IT) despite the usage of elements that are often associated with traditional IT environments. This difference is not necessarily based on the technology deployed, but rather the intent of the environment and the impact of threats to the environment. IT environments are dynamic in function and generally serve business communication/decision-making purposes where threats to confidentiality and integrity are most significant.

OT environments, on the other hand, are often considered deterministic; specific control action results from a specific input and is always expected to produce the same action. Any security threat to an OT environment's ultimate availability threatens its basic design criteria. The IAC cybersecurity requirements outlined in this document are defined with the control system security attributes of availability first and integrity second, with confidentiality following. These security attributes are further prioritized through the lens of safety before

operational considerations. Correct prioritization of the protection and support of essential functions provided by the IAC is foundational to a holistic risk-based approach to IAC cybersecurity activities.

4.2.1 Prioritizing Control System Essential Functions

An IAC function is essential when the capability is required to maintain health, safety, the environment, and availability for the equipment under control. Essential functions include, but are not limited to, functions performed by a safety instrumented system (SIS), the functions controlling a process and/or equipment, and the ability of the operator to view/manipulate the equipment under control.

Prioritization of IAC security activities and outcomes should be in support of the IAC essential functions they are designed to protect. Any security activity or outcome that could result in the decrease of availability or integrity of an essential function, without a supporting risk assessment, is improperly prioritizing the security capability over the protection of essential functions and is thereby ill-conceived.

4.2.2 Safety Instrumented Systems Considerations

Although this standard does not include SIS nor address any potential impacts to SIS SIL selection or determination, the tenet of “safety first” mandates that consideration should be taken to avoid inadvertently impacting SIS functions.

Control system cybersecurity outcomes, processes, and cybersecurity controls should include considerations of potential impact to SIS functions. These include, but are not limited to:

- IAC risk assessments;
- cybersecurity control design;
- cybersecurity control implementation;
- cybersecurity control testing.

4.3 IAC Cybersecurity Profile—Threat Protection Objectives

The IAC cyber activities and outcomes defined for each of the three API 1164 profiles are designed to meet threat protection objectives.

These protection objectives are defined to defend against increasing levels of threat factors, including resourcing, sophistication, motivation, knowledge, and skill. These threat protection objectives are mapped to the different levels of potential impact to business missions and objectives. The higher the level of potential impact, the higher the profile for a higher level of protection against a higher level of threat factors.

The threat protection objective to API 1164 profile mapping is detailed in Figure 1.

API 1164 Profile	Threat Rating	Threat Protection	Threat Protection Objective
P3 Extended	T3	Advanced	Protect for a deliberate attack that is highly motivated, resourced, and sophisticated, leveraging industry specific or tech domain skills/knowledge.
P2 Enhanced	T2	Heightened	Protect for a deliberate attack that is moderately motivated, resourced, and sophisticated, leveraging industry specific or tech domain skills/knowledge.
P1 Baseline	T1	Basic	Protect for a deliberate attack that is simple, low resourced and motivated and does not leverage any specific skills. Protect for unintentional or coincidental security violation.

Figure 1—API 1164 Security Level Threat Protection Objectives

4.4 IAC Cybersecurity Profile—Business and Mission Objectives

The development of an IAC cybersecurity profile includes the identification of common business and mission objectives for that industry. These business and mission objectives provide the necessary context for identifying and managing applicable cybersecurity risk mitigation.

There are six shared business and mission objectives for the ONG pipeline sector identified within this standard. Other business and mission objectives can exist in individual companies, industry sectors, and/or industry subsectors, but they are left up to the stakeholder company to address as appropriate.

4.4.1 Maintain Human Health and Safety

Manage cybersecurity risks that can adversely impact human safety, including both accidental and deliberate hazards. Cybersecurity risk on the pipeline system can adversely affect human safety. Personnel should understand cybersecurity and safety interdependencies. The tenet of “safety first” mandates that cybersecurity measures be implemented such that they do not impact IAC essential functions, which could result in human safety consequences.

4.4.2 Maintain Environmental Safety

Manage cybersecurity risks that can adversely impact the environment. This includes both accidental and deliberate damage. Cybersecurity risk on the pipeline system can adversely affect environmental safety. Personnel should understand cybersecurity and environmental safety interdependencies. The tenet of “safety first” mandates that cybersecurity measures be implemented such that they do not impact IAC essential functions, which could result in environmental safety consequences.

4.4.3 Maintain Property Safety

Manage cybersecurity risks that can negatively impact the safety to property owned by the company and property owned by others. This includes both accidental and deliberate damage. Incidents from an IAC cybersecurity incident can adversely affect property safety. Personnel should understand cybersecurity and property safety interdependencies. The tenet of “safety first” mandates that cybersecurity measures be implemented such that they do not impact IAC essential functions, which could result in property safety consequences.

4.4.4 Maintain Operational Capability

Manage cybersecurity risks that can adversely affect delivery and other contractual commitments. Cybersecurity risk within the IAC cyber environment, including asset damage, can adversely affect IAC essential functions impacting commercial obligations. Personnel should understand cybersecurity and commercial interdependencies.

4.4.5 Maintain Compliance Posture

Manage cybersecurity risks that can adversely impact a compliant posture with regulatory, legal, and corporate policy requirements. There are some shared regulatory requirements between hazardous liquids and natural gas pipelines, but also unique requirements.

4.4.6 Maintain Reputation

Manage cybersecurity risks that can adversely affect the company's reputation or generate negative publicity. Reputation damage exposure can occur at international, national, regional, or local levels. The impact of the reputation damage can be with the public, governments, regulatory bodies, industry, or with one or more customers. Protect against compromise of the availability and integrity of the control process and associated data.

4.5 IAC Cybersecurity Profile—Objectives Impact to Threat Protection Mapping

For this standard to scope and prioritize the ONG pipeline IAC cybersecurity activities and outcomes into scenario-based profiles, it is essential that the potential impacts to pipeline business objectives are mapped to appropriate threat protection levels.

API 1164 categorizes the impact to pipeline business objectives from cybersecurity hazards into three levels: I1, I2, and I3. These three levels correspond to the three threat protection objectives.

Figure 2 details the profile to business objective impact severity mapping:

API 1164 Profile	Threat Protection	Threat Protection Objective	Impact Severity	Business Objective	Business Objective Impact
P3 Extended	T3 Advanced	Protect for a deliberate attack that is highly motivated, resourced, and sophisticated, leveraging industry specific or tech domain skills/knowledge.	I3 High	a) Health/Safety b) Environment c) Property d) Operations e) Compliance f) Reputation	Above Medium Impact threshold for one or more business objectives.
P2 Enhanced	T2 Heightened	Protect for a deliberate attack that is moderately motivated, resourced, and sophisticated, leveraging industry specific or tech domain skills/knowledge.	I2 Medium	a) Health/Safety b) Environment c) Property d) Operations e) Compliance f) Reputation	- Below High Impact threshold for all business objectives and - Above Low Impact threshold for one or more business objectives.
P1 Baseline	T1 Basic	Protect for a deliberate attack that is simple, low resourced, motivated and does not leverage any specific skills. Protect for unintentional or coincidental security violation.	I1 Low	a) Health/Safety b) Environment c) Property d) Operations e) Compliance f) Reputation	Below Medium threshold impact for all business objectives.

Figure 2—API 1164 Business Objective Impact Mapping to Threat Protection Profiles

The following section details the use of the business objective impact table and the selection of cybersecurity profile requirements.

5 ONG IAC Cybersecurity Policy, Plan, and Program

This standard is intended to be implemented using a building block approach. This approach requires that foundational elements be implemented first. The IAC cybersecurity baseline profile covers foundational IAC cybersecurity program-wide, elements, processes, and activities. Many of these program-wide elements are essential to a sustainable and maturable cyber program.

The successful implementation of this standard relies on having executive sponsorship to ensure sufficient resources are committed and activities receive appropriate priority. This sponsorship comes in the form of an approved IAC cybersecurity policy. An approved IAC cybersecurity policy may be a separate policy document or may be incorporated in an overarching corporate cybersecurity policy. Because the scope of this document is constrained to IAC environments, it is only concerned with the IAC elements of the cybersecurity policy. This document refers to IAC policy elements collectively as the IAC cybersecurity policy, whether implemented in a separate IAC document or incorporated in a larger-scoped policy document.

This IAC cybersecurity policy is the cornerstone and authorization for all other API 1164 IAC cybersecurity components and activities. The policy specifies the requirements for and mandates the implementation of a risk-based IAC cybersecurity program to manage the IAC cyber environment to a level of cyber risk deemed acceptable by the organizational leadership responsible for enterprise risk. The policy mandates that the program be defined by one or more formally documented plans, identified in this standard as the IAC cybersecurity plan.

The IAC cybersecurity plan may be a single document or set of documents covering IAC cybersecurity activities and outcomes separately or may be incorporated in one or more overarching corporate cybersecurity plan documents. Because the scope of this standard is constrained to IAC environments, it is only concerned with the IAC elements of the cybersecurity plans. This standard refers to the IAC plan elements collectively as the IAC cybersecurity plan, whether implemented in one or more separate IAC documents or incorporated in one or more larger-scoped documents.

The IAC cybersecurity plan specifies all the requirements, outcomes, and foundational building elements, including the processes, roles, and responsibilities of stakeholders, and technologies required to operationalize the IAC cybersecurity program.

The IAC cybersecurity program documentation hierarchy is depicted in Figure 3.

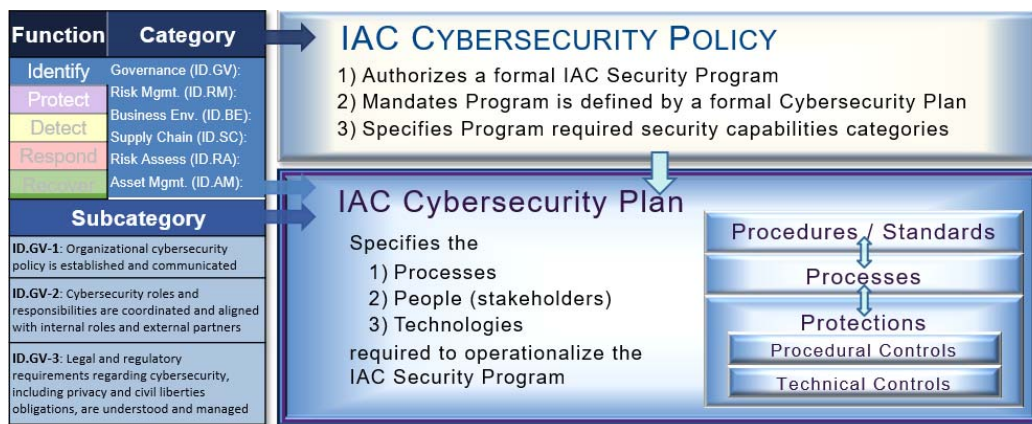


Figure 3—API 1164 CSF Sources for IAC Cybersecurity Policy and Plan

Within this standard, the IAC cybersecurity policy requirements are derived from the NIST CSF functions or category elements. The requirements for the IAC cybersecurity plan are derived from the NIST CSF categories, subcategories, informative references, and the extended references specified in A.3.

This approach is consistent with the NIST CSF mapping of the cyber section of TSA's Pipeline Security Guidelines. It is also consistent with the TSA Pipeline Security Guidelines mandate that the corporate security plan for each pipeline operator must include a cyber system security plan. Within this standard, the cyber plan is referred to as the IAC cybersecurity plan.

This standard promotes tailoring the requirements for selected impact profiles based on an implementer's unique risk factors. This is accomplished using the implementer's documented risk management processes, which consider alternate applicable mitigating controls and circumstances. This tailoring provides flexibility for easier implementation across the in-scope disparate IAC environments, resourcing constraints, and risk postures.

Implementers should not simply select specific profile requirements to address gaps in their current profile. The API 1164 cybersecurity policy is intended to drive the creation and maintenance of a risk-driven program. It is not intended to be implemented piecemeal. Without these underlying foundational elements, the ad hoc IAC cybersecurity activities will not be repeatable, measurable, or maintainable, and the IAC cybersecurity posture will likely erode.

5.1 IAC Cybersecurity Plan—Development

The IAC cybersecurity plan is developed by engaging all stakeholders. It is aligned with the organization's control system architecture and information security architecture. Stakeholders can be internal or external to an organization.

To develop the IAC cybersecurity plan, a cross-functional team should be established consisting of key stakeholders engaged in the IAC design, engineering, implementation, execution, security, management, maintenance, and operations, or have a technical or process interdependency with the IAC cyber environment. In some organizations, some personnel may perform multiple roles. See Figure 4 for an example of a cross-functional team. Stakeholders who provide or are involved in interfaces with the IAC cyber environment are members of the cross-functional team and should be consulted and informed regarding the Plan's impact to those interfaces.

All stakeholders should share their varied domain knowledge and experience so that the plan is comprehensive and considers the objectives, aspects, and constraints of the IAC cyber environment. The cross-functional cybersecurity team should consider the impacts between IAC safety, essential functions, and security interdependencies.

Figure 4 depicts the stakeholders that are either members of the cross-functional team or consulted during the creation or modification of the IAC cybersecurity plan.

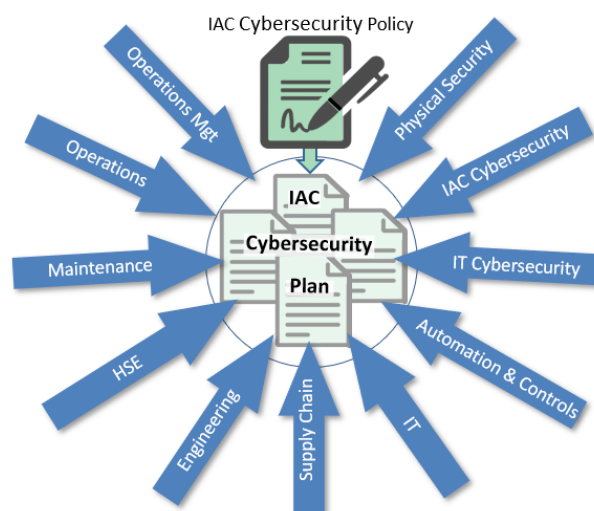


Figure 4—IAC Cybersecurity Plan Development Participation

5.2 IAC Cybersecurity Plan—Risk Management Foundation

Risk management is the process of applying resources in a measured and appropriate way. A risk management program is a collection of people, processes, and optional technology to systematically address risk, including cybersecurity risk, to organizational objectives, organizational assets, individuals, and other organizations. It is based on a risk strategy, formally and consistently assesses risk, and formally and consistently responds to risk according to the organization's risk tolerance.

The intent of an API 1164 IAC cybersecurity program is the management of risks associated with cybersecurity. While the identification of impacts and control mitigations is critical to the program's development, evaluation of

each from a risk perspective will ensure implementation of the program is appropriately executed and sustained consistent with an organization's risk posture.

A risk management process requires the organization to:

- 1) frame risk;
- 2) assess risk;
- 3) respond to risk once determined;
- 4) monitor risk on an ongoing basis.

Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decisions are integrated into every aspect of the organization. Established risk management program elements are documented in the IAC cybersecurity plan, agreed to by organizational stakeholders, and actively managed.

Input from a variety of organizational sources, such as leadership, operations, and support functions, helps identify risk from a balanced perspective and is tailored to meet the organization's specific cybersecurity needs.

An IAC cybersecurity risk management program has three foundational elements that are defined in the IAC cybersecurity plan:

- 1) risk strategy;
- 2) risk assessment process(es);
- 3) predetermined risk response matrix.

5.2.1 IAC Cybersecurity Plan—Risk Management Strategy

A risk management strategy is a formal element of a risk management program. It is a documented framework that addresses how the organization intends to assess, respond to, and monitor risk. The risk management strategy is used to make consistent decisions based on predefined risk responses to asset classifications and risk levels.

The risk strategy contains the organization's:

- 1) priorities (e.g., relative importance of business functions and trade-offs between varying types of risk);
- 2) constraints on the risk assessment;
- 3) response and monitoring alternatives;
- 4) risk tolerances (e.g., levels and types of risk, and degrees of risk uncertainty that are acceptable); and
- 5) assumptions about the impact and likelihood (threat and vulnerability factors) of occurrence that affect how risk is assessed, responded to, and monitored over time.

5.2.2 IAC Cybersecurity Plan—Risk Assessment

The purpose of the risk assessment process is to identify:

- 1) threats to operations, assets, or individuals;
- 2) vulnerabilities of cyber assets and IAC cyber assets;

- 3) the consequences/impact (i.e., harm) to the organization that may occur given the potential for threats exploiting vulnerabilities;
- 4) the likelihood that harm will occur.

The result is a determination of the cybersecurity risk's degree of harm and likelihood of harm occurring. This provides the organization with an understanding of the risk to operations, assets, individuals, the upstream and downstream supply chain ecosystem, and to critical infrastructure.

5.2.3 IAC Cybersecurity Plan—Risk Response

There are four generally accepted responses to a risk:

- 1) Tolerate: The identified risk is below a company's risk tolerance. No action is needed or taken.
- 2) Treat: Remediate the identified risk such that the residual risk after remediation is at an acceptable level.
- 3) Terminate: Remove the identified risk. The residual risk is zero.
- 4) Transfer: The identified risk is moved to a third-party reducing residual risk to an acceptable level.

5.3 IAC Cybersecurity Plan—Operationalizing an IAC Cybersecurity Program

When elements of the IAC cybersecurity plan are operationalized, they are considered elements of the IAC cybersecurity program. The IAC cybersecurity program may be separate or may be incorporated in one or more overarching corporate cybersecurity programs, including corporate IT. This document is only concerned with the IAC elements of the cybersecurity program. This document refers to the IAC program elements collectively as the IAC cybersecurity program, whether implemented separately or incorporated in one or more larger scoped cybersecurity programs.

The IAC cybersecurity plan is operationalized by implementing the procedures, processes, procedural controls, and technical controls. The stakeholders in their varying capacities perform activities to interact and operate the plan elements. Stakeholders execute procedures, processes, procedural controls, and technical controls assigned to those roles.

A subset of those activities test the effectiveness of the program, including both the design effectiveness and the operational effectiveness of the plan elements against program performance expectations and the outcomes aligned to the plan's documented element objectives.

Based on the program performance measures, improvements are recommended and prioritized. Often, the recommendation is to improve the design or operations of the IAC cybersecurity plan documented elements. In certain situations, it is possible that the policy requires modification to align to the operational reality of the IAC security program execution, a changing business environment, or both. Improvement recommendations are reviewed to align the IAC cybersecurity policy and the plan, allowing for modification of one or both. The API 1164 policy and plan-driven IAC cybersecurity program model is shown in Figure 5.



Figure 5—API 1164 Policy and Plan-driven IAC Cybersecurity Program

5.4 IAC Cybersecurity Plan—Selecting Cybersecurity Profiles

Figure 6 shows a high-level example of an API 1164 implementation process flow diagram that depicts how you could use this standard to define your IAC cybersecurity plan using three different cybersecurity profiles. These three cybersecurity profiles are based on three levels of threat protection objectives mapped to three business objective impact severity levels.

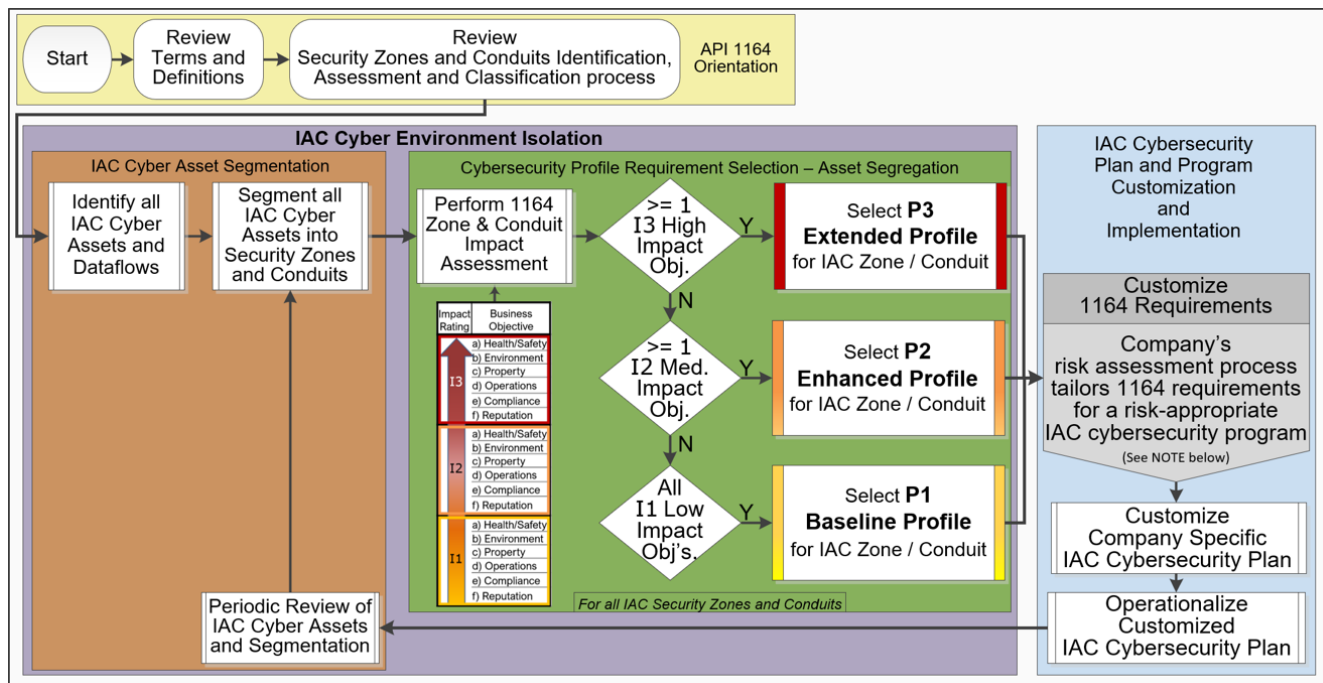


Figure 6—API 1164 Profile Selection, Customization, and Implementation

NOTE This document specifies the items and activities within the diagram above, with the exception of the “Customize 1164 Requirements” process in gray. It does provide guidance on the customization process, but relies on the company’s risk assessment process.

5.4.1 Defining IAC Segregated Environments: Security Zones and Conduits

5.4.1.1 Network Segmentation and Network Segregation

Protecting network integrity is a foundational element of defending interconnected systems within IAC cyber environments. A way to achieve this is through a defense-in-depth strategy that implements:

- 1) network segmentation: IAC network(s) are partitioned into smaller networks;
- 2) network segregation: Different protection rulesets are defined using risk-based criteria and implemented to manage the security of each segment.

The combination of network segmentation and segregation is a security countermeasure designed to compartmentalize IAC cyber assets where identified security practices are employed consistently to all cyber assets within the segment to achieve the desired cybersecurity target profile. This provides a segregated defense-in-depth approach to limit the attack surface of network interconnected IAC cyber assets from widespread horizontal and vertical expansion of a potential network intrusion.

ANSI/ISA-95/ISO/IEC-62264-1:2013 *Enterprise Control System Integration, Part 1: Models and Terminology* contains a reference model for computer integrated manufacturing based upon the Purdue Reference Model for CIM (hierarchical form). Although ISA-95-1's reference model is not a cybersecurity reference model, it depicts a high-level example of network segmentation, including IAC environments. While not endorsed or required by this standard, it can be used as the basis for the first layer in the segmentation of networks between IAC environments and non-IAC environments, and within IAC environments.

5.4.1.2 IAC Security Zones

An IAC security zone is a single IAC cyber asset, or a grouping of IAC cyber assets, identified as a single entity within a security perimeter. All IAC cyber assets within an IAC security zone implement shared security requirements distinguishing it from other cyber assets with which they communicate. An IAC security zone has a clear logical border with other zones. An IAC security zone is secured by a combination of mechanisms both at the zone edge and within the zone.

An IAC security zone shall have a clear logical or physical demarcation that may be defined by geographic boundaries, an organization's functional / departmental boundaries, common cyber functional capabilities or any other physical or logical grouping applicable to a given situation that will implement the common set of security controls on all assets within the zone's security perimeter.

The combination of network segmentation and security ruleset segregation defines an IAC security zone. The security zone protection ruleset implements all human, device, and process access to the zone, zone communications ingress and egress protections and security posture elements within the security zone.

Establishing security zones by grouping IAC and related cyber assets using risk-based criteria, including, but not limited to, shared risk profile, physical or logical location, criticality of assets, operational function, physical and logical access requirements, or responsible organization allows for risk-appropriate security measures to be applied. These measures are applied both within the security zone and to control and protect the communications into and out of the security zone.

This improves the IAC security posture by reducing attack surfaces, limiting exposure of critical production assets, and facilitating implementation of least privilege by restricting movement between security zones. Using a risk-based approach focuses security monitoring and controls on the zones where they are most effective and improves detection and response capabilities.

5.4.1.3 IAC Security Conduits

A rule of IAC security zones is that the IAC cyber assets contained within them shall only be allowed to communicate with IAC cyber assets outside their zone through an IAC security conduit. An IAC security conduit is

a special security zone that is specific to communication processes, containing logical grouping of assets that are used in, perform, monitor, and defend communications for the IAC security zones to which it connects.

IAC security conduits, usually consisting of one or more cyber assets, are security zones in and of themselves for access control and configuration management protection requirements. This is differentiated from what and how data traverses the conduit.

IAC cyber assets and the rules that govern the IAC security zone to which they belong determine what data will be communicated with other security zones. The IAC security conduit determines what data or services (e.g., communication protocols, TCP/IP ports, etc.) can traverse the conduit. The IAC security zone and the IAC security conduit work together to provide a layered defense-in-depth approach to IAC security zone data ingress and IAC security zone data egress.

The IAC security conduit may provide protection mechanisms in the form of access controls, data encryption, and the like while the data is traversing the IAC security conduit between the source IAC security zone and the target security zone. Edge and other network devices that create and manage the conduits create their own security zones that are risk-appropriately controlled on how they are managed and by whom.

Any boundary device of a security zone is an endpoint of a security conduit. Examples of devices that comprise a security conduit include, but are not limited to, managed switches, routers, firewalls, third-party circuits, IDS, IPS, and other communication devices.

5.4.1.4 IAC Zone and Conduit Taxonomy

The use of security zones and security conduits within this standard are organized into a structured taxonomy to support consistency and understanding of the specific contexts in which security zone and security conduit requirements are defined and used. This is detailed in Figure 7.

Non-IAC Environments		External Zone		Security Zones
IAC Segregated Environment	IAC Security Zone	IAC Intermediate Zone		
		IAC Internal Zone		
	IAC Security Conduit	IAC External Conduit		Security Conduits
		IAC Intermediate Conduit		
		IAC Internal Conduit		

Figure 7—API 1164 Security Zone and Security Conduit Taxonomy

- 1) Security zones:
 - a) External zone: A network segment outside the purview of an IAC cyber environment that could be in the purview of another function within the organization or outside the purview of the organization entirely.
 - b) IAC security zone: A security zone defined within an IAC cyber environment that requires the same security ruleset to be applied to all IAC cyber assets within its security perimeter. There are two subtypes of IAC security zones:
 - i) IAC intermediate zone: An IAC security zone that implements a single security ruleset for the purposes of indirectly presenting IAC data and services to an external zone and for providing external controlled access to IAC services by users from an external zone. IAC cyber assets within IAC intermediate zones do not perform IAC essential functions.

- ii) IAC internal zone: A single IAC cyber asset or a grouping of IAC cyber assets that implement a single security ruleset and only communicate with IAC cyber assets within the IAC internal zone, IAC cyber assets in another IAC internal zone, or IAC cyber assets in an intermediate zone.

2) Security Conduits: There are three subtypes of IAC security conduits:

- a) IAC external conduit: A security conduit that connects an external zone with an IAC intermediate zone.
- b) IAC intermediate conduit: A security conduit that connects an IAC intermediate zone with an IAC internal zone.
- c) IAC internal conduit: A security conduit that connects an IAC internal zone with another IAC internal zone.

NOTE The scope of this document only includes IAC security conduits, and within this document, security conduits and IAC security conduits are synonymous.

The IAC security conduit type (external, intermediate, internal) dictates what type of security zones can be connected. The IAC security conduit connectivity relationships are shown in Figure 8.



Figure 8—API 1164 IAC Security Conduit Connectivity Relationships

IAC security conduits may use third-party communications transport network provider services. This includes, but is not limited to, GEO, MEO, or LEO satellite providers, POTS/PSTN telco networks, terrestrial leased line, wide-area networks (WAN), metro-area networks (MAN), MPLS, VPLS, and cellular modems. Regardless of the medium, these services provide varying levels of “black-box” network infrastructure. In this regard, the user of these services has little to no visibility of network management and access control procedures.

This standard does not differentiate or subcategorize IAC security conduits between those that use third-party network infrastructure and those that use company-owned network infrastructure. Both are considered external IAC transport services when the management of those network segments and services are not in the purview of IAC personnel. This document includes additional requirements relative to the integrity of IAC networks, IAC baseline configurations, and IAC network and communication protections for IAC security conduits that use external IAC transport services.

5.4.1.5 IAC Zone and Conduit Example Implementation

Figure 9 provides a visual example of an implementation of IAC security zones and IAC security conduits. The diagram is for explanatory and reference purposes only.

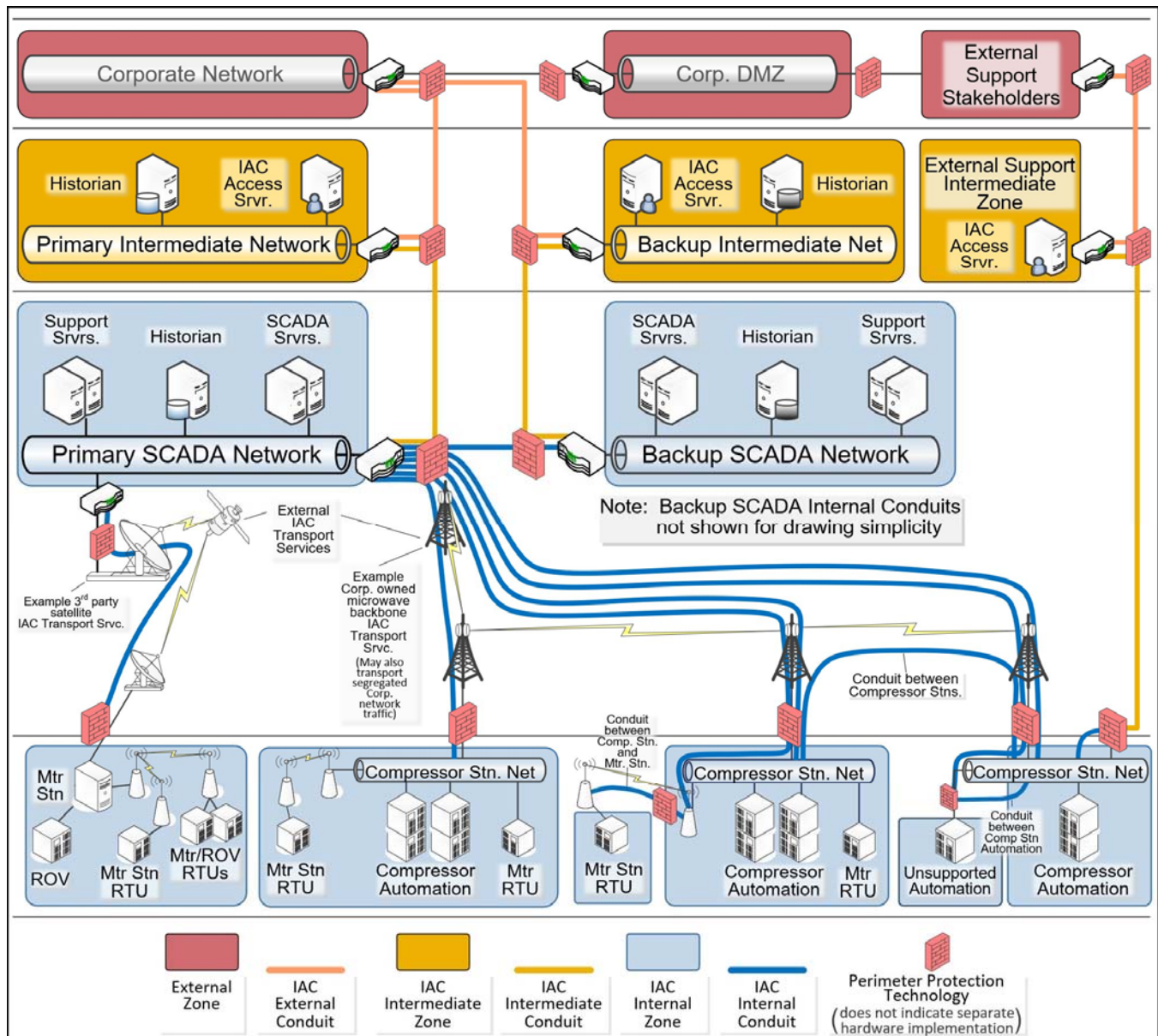


Figure 9—Example API 1164 IAC Security Zone and Conduit Implementation

5.4.1.6 IAC Security Zoning Overview

This standard gives complete autonomy to its implementers in defining the boundaries of IAC security zones. This flexibility allows them to meet the requirements of a virtually limitless number of company-specific considerations, architectures, and scenarios.

This flexibility stems from the premise that the reason why an asset is included within a given IAC security zone is not relevant. What is relevant and required is that the API 1164 profile selected for the security zone is based on the impact severity rating of the entire IAC security zone. This selected profile is then applicable to all IAC cyber assets within the zone, regardless of an individual IAC cyber asset's impact rating. That is, an IAC cyber asset that would have selected the baseline profile based on its isolated impact rating has to have its profile selected based on the impact rating of the entire zone it belongs to, which could be higher. This enforces the highest-level protection across all IAC cyber assets within the same zone to minimize a potential compromise of a lower-impact IAC cyber asset putting at risk an IAC cyber asset with a potential higher impact to business objectives.

5.4.1.7 IAC Security Zone Partitioning

The organization establishes zones and conduits by grouping IAC cyber assets. Grouping shall be based upon the results of the initial cybersecurity risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (e.g., least privilege principles), or responsible organization.

System inventory, architecture diagrams, network diagrams, and data flows can be used to determine and illustrate the IAC assets that are considered for zone segmentation.

5.4.1.7.1 Inventory Steps

- 1) Identify cyber asset inventory.
- 2) Identify functionality of assets, including communications, monitoring, command and control, and safety devices.
- 3) Disregard any cyber asset that is not used in the IAC resulting in the IAC cyber asset inventory.

NOTE External zones and management of cyber assets that are not within an IAC segregated environment boundary are outside the scope of this standard.

- 4) Identify all intra-company communications.
- 5) Identify all inter-company communications.

5.4.1.7.2 IAC Zone and Conduit Segmentation Rules

Organizations can create zones as they choose. IAC zone segmentation shall follow these rules:

- 1) All IAC assets within an IAC security zone must be on the same network segment or be able to be managed collectively as if on a single network segment.
- 2) All IAC cyber assets shall be a member of an IAC segregated environment and inherit the API 1164 profile of the IAC security zone or IAC security conduit to which it belongs.
- 3) An IAC segregated environment only contains IAC cyber assets. The inclusion of any cyber asset into an IAC segregated environment, by definition, makes it an IAC cyber asset governed by the rules of the IAC security zone or IAC security conduit to which it belongs.

NOTE For example, including a printer within the IAC security zone boundary makes the printer an IAC cyber asset.

- 4) All communication connections with IAC cyber assets within an IAC security zone shall be from other IAC cyber assets within the security zone or by an IAC security conduit interconnecting security zones.
- 5) An IAC security zone shall be connected to another security zone only through an IAC security conduit.
- 6) Where a dedicated development or test IAC security zone exists, it shall not be connected to any production IAC security zones, except through IAC security conduits when justified by a risk and cybersecurity assessment of connecting technologies and processes.
- 7) Communications between IAC cyber assets and an external zone shall only occur from an IAC intermediate zone traversing an IAC external conduit. (external ↔ intermediate).
- 8) IAC cyber assets that receive data or services from an external zone shall only do so through IAC intermediate conduit connected to an IAC intermediate zone (external ↔ intermediate ↔ IAC internal).
- 9) IAC cyber assets that provide data or services to an external zone shall only do so through an IAC intermediate conduit connected to an IAC intermediate zone (external ↔ intermediate ↔ IAC internal).

unless supported by a risk assessment that includes a cybersecurity assessment of the involved architectures, technologies, equipment, and life-cycle management and maintenance processes for potential impacts to essential services provided by the IAC segregated environment.

5.4.1.7.3 IAC Zone Segmentation Guidelines

Guidelines on how to create effective IAC security zones are listed below:

- 1) Group assets that contribute to a common function, location, or system.
- 2) Assets that have separate functions, locations, or systems can be grouped together into a common zone.
- 3) Wireless IAC cyber assets should be segregated into separate zones from IAC security zones containing wired IAC cyber assets.

NOTE Wireless includes Wi-Fi and other routable protocols that use radio frequency methods as a means of communications, not physical wires.

- 4) If an IAC security conduit is risk justified, between an IAC production security zone and dedicated development or test IAC security zone, its connection should be temporarily.
- 5) IAC cyber assets that can establish temporary zone conduit connections to an IAC security zone should be segregated into a separate zone or zones from IAC cyber assets that are intended to establish permanent zone conduit connections.
- 6) Not all assets within a zone need to directly communicate with each other.
- 7) Nesting of IAC security zones within other zones is permitted, but only if the zone and conduit rules and relevant IAC cybersecurity plan requirements are strictly followed. Specifics of these types of architecture are outside the scope of this document.

5.4.2 IAC Security Zone and Security Conduit Impact Assessment

Impact assessments are used to determine which API 1164 security profile is to be selected for IAC security zones and IAC security conduits. Zone impact assessments only apply to IAC security zones and not external zones. Although an IAC external conduit connects to an external zone, the impact from this conduit type is still in scope because the conduit is also connected to an IAC intermediate zone, which is part of the IAC cyber environment.

Even though both IAC security zones and IAC security conduits are assessed for impact to the business objectives, the security profile selection process is slightly different between the two. This is detailed below.

5.4.2.1 IAC Security Zone Impact Assessment Rules

Zone impact assessments only apply to IAC security zones and not external zones. Based on the shared security requirements of any given IAC security zone, it should be assumed that a threat source may theoretically obtain a sufficient level of lateral movement within the IAC security zone to exploit a shared vulnerability intentionally or accidentally throughout the zone.

All IAC cyber assets within the boundaries of the IAC security zone are included in the collective impact severity calculation of the entire zone. The impact assessment process determines the impact severity of the IAC security zone using the impact severity rating for all business objectives.

- 1) An impact assessment shall be performed on each IAC cyber asset within the IAC security zone.
- 2) An impact assessment shall be performed on the entire IAC security zone, considering the collective and potentially additive impacts of the IAC cyber assets it contains.

- 3) An IAC security zone's impact rating shall not be less than the highest impact rating of any IAC cyber asset it contains.
- 4) The IAC security zone's impact rating is selected based on the zone's collective impact.

EXAMPLE If, for a given IAC security zone, the business objectives of reputation, operations, environment, and health/safety are all at an impact severity of 1, but the property business objective is at an impact severity rating of 2, the entire zone is considered to have an impact severity of 2. The zone would then be classified as an enhanced profile IAC security zone and the P2 security requirements will apply to all IAC cyber assets within the zone.

It is possible, and likely, that an IAC security zone can have a higher impact rating than the highest impact rating of any IAC cyber asset it contains.

5.4.2.2 IAC Security Conduit Impact Assessment Rules

Since an IAC security conduit provides a connection between two security zones, the conduit is assessed on the impact to business objectives from the conduit itself and the impact of the IAC security zones to which it connects.

Organizations shall designate IAC security conduits as having impact ratings. IAC zone impact rating designations shall follow these rules:

- 1) An impact assessment shall be performed on each IAC cyber asset within the IAC security conduit.
- 2) An impact assessment shall be performed on the entire IAC security conduit, considering the collective and potentially additive impacts of the IAC cyber assets it contains.
- 3) An IAC security conduit's impact rating shall not be less than the highest impact rating of any IAC cyber asset it contains
- 4) The IAC security conduit's impact rating is selected based on the conduit's collective impact.

EXAMPLE If, for a given IAC security conduit, the business objective's impact severity is a 1 but one of the two IAC security conduits' business objective impact severity rating is a 2, the IAC security conduit is considered to have an impact severity of 2. The conduit would then be classified as an enhanced profile IAC security conduit and the P2 security requirements will apply to all IAC cyber assets within the conduit.

IAC security conduits can have a higher impact rating than either of the two IAC security zones to which it connects.

5.4.3 Security Zone and Conduit Profile Selection Process

It is not feasible to apply the most stringent and rigorous best practices to all IAC cyber assets and environments without regard to the risk they impose on the organization.

API 1164 focuses on assessing and classifying the potential impact to the organizational objectives by the compromise of an IAC security zone or IAC security conduit. These impact ratings have been aligned to API 1164 IAC profiles. API 1164 profiles were developed using threat protection objectives with increasing threat sophistication and motivation (see 4.3). The result is a scaled approach whereby the higher the impact to business objectives, the higher the protection level required to defend against more advanced threats. This classification process categorizes an IAC security zone to apply an appropriate level of security to achieve a desired level of assurance based on the potential impact.

5.4.3.1 IAC Security Impact Assessment Process Overview

The purpose of the initial IAC cybersecurity impact assessment is to gain a high-level understanding of the worst-case risk the IAC segregated environment presents to the organization should it be compromised. This assessment may assist with the prioritization of detailed risk assessments and may influence which IAC assets belong to which zones or conduits within the IAC cyber environment.

The organization should perform an initial IAC cybersecurity business objective impact assessment of the IAC segregated environment or confirm that a previous impact assessment is still applicable to identify the worst-case unmitigated impact that could result from the interference with, disruption of, or disablement of mission-critical IAC operations.

The organization should develop credible scenarios to define potential cybersecurity threats, considering threat intelligence from various relevant sources. Once the scenario has been defined to determine how an act can be induced, it should describe how a threat could reasonably execute the act. The general sequence of the act should be documented in sufficient detail to allow others reviewing the results to understand the assumptions of the scenario and conclusions. The organization should also deliberate on the level of estimated consequence that each scenario under consideration would reasonably yield.

For potentially hazardous processes, the results from any applicable process hazard analysis and functional safety assessments as part of SIS SIL selection or determination should be referenced as part of the high-level IAC cybersecurity impact assessment to identify reasonable worst-case impacts.

Figure 10 can be used to determine which API 1164 profile is required for an IAC segregated environment.

API 1164 Profile	Threat Protection	Assessed Impact	Business Objective	Business Objective Impact
P3 Extended	T3 Advanced	I3 High	a) Health/Safety	Possibility of any on-site fatalities with a possibility of off-site fatalities.
			b) Environment	Very large to major impact on-site and/or large off-site, between X and =>Y years to recover up to poor chance of recovery.
			c) Property	Over \$Y loss in property damage.
			d) Operations	Long to very long-term (X to =>Y years) business interruption/expense; large-scale disruption to the national economy, public/private operations; loss of critical data.
			e) Compliance	High to very high impact on internal or external assessments with significant remediation or penalties/fines (>\$Y); prosecution by regulator;
			f) Reputation	High to very high loss of reputation or business viability; extensive national coverage up to international coverage.
P2 Enhanced	T2 Heightened	I2 Medium	a) Health/Safety	Possibility of widespread on-site serious injuries; no fatalities or injuries anticipated off site.
			b) Environment	Moderate impact on-site and/or minor off-site impact, >X year(s) to recover.
			c) Property	Over \$X to \$Y loss in property damage.
			d) Operations	Medium-term (Y to Z months) business interruption/expense.
			e) Compliance	Medium impact on internal or external assessments with moderate remediation or penalties/fines (\$X<x<\$Y); attention of regulatory agencies;
			f) Reputation	Medium loss of reputation or business viability; national press coverage.
P1 Baseline	T1 Basic	I1 Low	a) Health/Safety	Possibly minor on-site injuries that are not widespread but only in the vicinity of the incident location; no fatalities or injuries anticipated off site.
			b) Environment	No or minor impacts to immediate incident site area only, less than X year(s) to recover.
			c) Property	Low to \$X loss in property damage.
			d) Operations	Short-term (up to X weeks) to (=>X weeks to Y months) business interruption/expense.
			e) Compliance	Little to no impact on internal or external assessments with minor remediation or penalties/fines (< \$X); query by regulatory agency
			f) Reputation	No impact to low loss of reputation or business viability; up to significant local press coverage.

Figure 10—API 1164 IAC Business Objective Impact Classification Matrix

* The reasonably expected worst-case impact resulting from a cyber-related event within the IAC zone or conduit that causes a disruption to the availability of IAC essential functions, an unauthorized modification of the IAC cyber environment, or unauthorized IAC information disclosure.

5.4.3.2 IAC Security Zone Impact Assessments

Use the following steps to perform the 1164 IAC security zone impact assessments:

- 1) Use the values appropriate for your organization to update the table's variables.

NOTE These values are often obtained from organization authoritative sources familiar with risk and business financial thresholds.

- 2) Perform a detailed cybersecurity impact assessment for each IAC cyber asset within the IAC security zone to determine consequences and impacts.
- 3) Perform a cybersecurity impact assessment for the IAC security zone, considering the collective and potentially additive impacts of the IAC cyber assets it contains to determine consequences and impacts.
- 4) Starting at the top of the matrix, select the profile with the worst case (i.e., highest applicable) IAC security zone impact using the consequence(s) and impact(s) determined during the zone impact assessment.
- 5) The resulting 1164 profile is selected for all IAC cyber assets in the IAC security zone being classified.
- 6) Repeat steps 2–4 until all IAC security zones are categorized.

5.4.3.3 IAC Security Conduit Impact Assessments

Use the following steps to perform the 1164 IAC security conduit impact assessments:

- 1) Using the values derived from IAC security zone impact assessments in Step 1 above, perform a detailed cybersecurity impact assessment for each IAC cyber asset within the IAC security conduit to determine consequences and impacts.
- 2) Perform a cybersecurity impact assessment for the IAC security conduit, considering the collective and potentially additive impacts of the IAC cyber assets it contains to determine consequences and impacts.
- 3) Starting at the top of the matrix, select the profile with the worst-case (i.e., highest applicable) IAC security conduit impact using the consequence(s) and impact(s) determined during the impact assessment.
- 4) If the resulting 1164 profile selected is less than any 1164 profile selected for all IAC security zones to which the IAC security conduit connects, the highest shall be selected for the IAC security conduit.
- 5) The resulting 1164 profile is selected for all IAC cyber assets in the IAC security conduit being classified.
- 6) Repeat steps 1–4 until all IAC security conduits are categorized.

5.5 IAC Cybersecurity Plan—Customizing Selected Profile Requirements

The selection of API 1164 profile requirements is based on the assessed impact to business objectives from IAC security zones and IAC security conduits. Given a virtually limitless number of company-specific considerations, architectures, and scenarios, this standard permits the customization of the profile's requirements prior to their final inclusion in the IAC cybersecurity plan and implementation in the IAC cybersecurity program.

This customization process uses the organization's risk management process and allows the organization to make risk-based decisions regarding the applicability of API 1164 profile requirements. Customization is a prerequisite to profile requirement implementation. The result of the customization process is a risk-appropriate list of IAC cybersecurity requirements for each IAC security zone or conduit that aligns to the organization's operating environment, business needs, and risk tolerance.

The tailoring of selected requirements before their inclusion into an IAC cybersecurity plan can be based on any company-specific unique risk factors, including, but not limited to, an organization's risk tolerance, its business or operating models, or the identification and consideration of additional existing mitigating controls or mitigating circumstances unique to the implementer's environment, architecture, or other unique risk-limiting scenarios.

The customization process has the following characteristics:

- 1) Does not change the assessed impact level nor the selected profile.
- 2) Is applied to each requirement within the selected profile for a given IAC segregated environment.

- 3) Previous customization process artifacts and decisions are considered for historical context of the assumptions, constraints, and rationale used for those risk-based decisions.
- 4) Customization of individual requirements may result in one of the following:
 - d) implementation of a corresponding requirement from a lesser profile;
 - e) modification of the requirement to fit the unique situation; or
 - f) elimination of the requirement entirely.
- 5) Final disposition of requirements is based on risk and not operational convenience.
- 6) Activities, including risk assessment results and decisions, are documented

If all requirements within an API 1164 section are downgraded through the customization process, the result is the assignment of risk-appropriate lower profile requirements for a higher-impact assessed zone or conduit.

The outcomes of the customization process should result in detailed risk assessments and actionable mitigations that are authorized by accountable personnel within the organization.

The resulting customized set of profile requirements and the supporting risk assessment artifacts are used to tailor the company's unique IAC cybersecurity plan.

The resulting tailored IAC cybersecurity plan documents the company's risk-appropriate IAC cybersecurity program ready to be implemented and matured. Governance activities, including testing, assurance, and auditing, should be centered to the company's customized program and not the originally selected API 1164 profile requirements.

6 ONG IAC Cybersecurity Profile Requirements—Identify (ID)

The Identify function develops the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enable an organization to focus and prioritize its efforts consistent with its risk management strategy and business needs. The target profiles outcome categories and subcategories within this function are detailed below.

6.1 Governance (ID.GV)

The objective is to employ an organization-wide formal IAC cybersecurity management program to address the cybersecurity aspects of its IAC cyber environments. The implementation of the IAC program requires the establishment of formal IAC security program documentation in the form of policies, procedures, processes, and operational and procedural controls. These documents detail the organization's cybersecurity regulatory, legal, risk, and operational requirements; how the requirements are satisfied; and how they are managed and monitored in the form of specific people, processes, and technology.

A governance model can then be used to measure the performance of the actual execution of the program against the requirements, deliverables, and outcomes set forth in its formal documentation.

It is critical that the IAC cybersecurity program documents are collaboratively developed, officially approved, and conspicuously published. Policies are approved by senior leadership, which authorizes the resulting program implementation. It is imperative the IAC security program documents are understood through formal training and awareness processes. Roles and responsibilities for the management and operation of the program are appropriately assigned and communicated via formal training, and the operation of the program and the governance of it informs management of its IAC cybersecurity risk.

P1: (1); (2); (3); (4); (5)	P2: (1); (2); (3); (4); (5); (6)	P3: (1); (2); (3); (4); (5); (6)
-----------------------------	----------------------------------	----------------------------------

6.1.1 Baseline Profile Requirements

- 1) A formal IAC cybersecurity policy exists that specifies the requirements for and authorizes the implementation of a risk-based IAC cybersecurity program as specified in a documented IAC cybersecurity plan.
- 2) The IAC cybersecurity policy requires that the IAC cybersecurity program be developed, implemented, and operated as specified in a documented IAC cybersecurity plan.
- 3) The requirements of IAC cybersecurity policy are communicated to and agreed by relevant IAC stakeholders prior to both physical or logical access to an IAC cyber environment.
- 4) The IAC cybersecurity policy is approved by senior leadership accountable for the IAC cybersecurity program.
- 5) The IAC cybersecurity policy is reviewed at organizationally defined frequency and updated as appropriate not to exceed every 36 months or when there is a significant change.

6.1.2 Enhanced Profile Requirements

- 6) The IAC cybersecurity policy is reviewed and updated as appropriate not to exceed every 12 months or when there is a significant change by any organization that has one or more IAC segregated environments with a business objective impact classification higher than I1-Low (baseline profile).

6.1.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.1.4 ID.GV-1—IAC Cybersecurity Plan

The IAC cybersecurity plan is one or more documents that specify all the requirements and outcomes of an IAC cybersecurity program. It specifies all foundational building elements, including the procedures, processes, roles, and responsibilities of stakeholders, and procedural and technical controls required to operationalize a risk-appropriate IAC cybersecurity program. It is scoped for IAC cyber environments, and addresses specific IAC cybersecurity and IAC operational requirements, constraints, and considerations when defining an IAC cybersecurity program.

P1: (1); (2); (3); (4); (5)	P2: (1); (2); (3); (4); (5); (6)	P3: (1); (2); (3); (4); (5); (6)
------------------------------------	---	---

6.1.4.1 Baseline Profile Requirements

- 1) The IAC cybersecurity plan requires that governance processes exist that inform management of the organization's regulatory, legal, environmental, and operational risk.
- 2) The IAC cybersecurity plan requires that the IAC cybersecurity program be measured for performance.
- 3) The IAC cybersecurity plan requires that any IAC cybersecurity program performance deficiencies be addressed.
- 4) The IAC cybersecurity plan requires that the IAC cybersecurity policy and IAC cybersecurity plan be updated to reflect any IAC cybersecurity program performance corrections.
- 5) The IAC cybersecurity plan is reviewed at an organizationally defined frequency and updated as appropriate not to exceed every 36 months, or when there is a significant change.

6.1.4.2 Enhanced Profile Requirements

- 6) The IAC cybersecurity plan is reviewed and updated as appropriate not to exceed every 12 months or when there is a significant change by any organization that has one or more IAC segregated environments with a business objective impact classification higher than I1-Low (baseline profile).

6.1.4.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.1.4.4 Supplemental Guidance

- a) The IAC cybersecurity policy can specify consequences for violation of policy, including, but not limited to, potential disciplinary actions in accordance with company-defined policy compliance requirements.
- b) The IAC cybersecurity plan can be reviewed and assessed in alignment with overall management system requirements of the organization (e.g., relevant requirements in API RP 1173). This would include management review, establishing performance indicators, and tracking performance of the program to inform updates to the IAC cybersecurity program.

6.1.4.5 IIoT Cautions and Supplemental Guidance

- c) If IIoT deployment becomes pervasive, identifying relevant IIoT stakeholders may impose communication/training challenges.

6.1.5 ID.GV-2—IAC Cybersecurity Roles and Responsibilities Coordination

The organization aligns IAC cybersecurity roles and responsibilities with internal and external partners. Identification of individual contributors and stakeholders, their responsibilities, and commitment requirements are critical to an effective cybersecurity program. In the event of a cybersecurity incident, a defined and well-understood responsibility matrix is the key to a well-organized response.

P1: (1); (2); (3); (4); (5); (6)	P2: (1); (2); (3); (4); (5); (6)	P3: (1); (2); (3); (4); (5); (6)
---	---	---

6.1.5.1 Baseline Profile Requirements

- 1) The IAC cybersecurity plan requires the identification of IAC cybersecurity stakeholder roles, including internal and external partners.
- 2) The IAC cybersecurity plan requires that IAC cybersecurity be coordinated between stakeholders.
- 3) The IAC cybersecurity plan requires that the roles and responsibilities of the IAC cybersecurity program be coordinated between any existing company functions and with IAC operations.

NOTE See associated requirements in 6.6.4.

- 4) The IAC cybersecurity plan requires the documentation of where the responsibility and accountability for the design, implementation, management, administration, or operation of IAC cybersecurity transitions between intraorganizational or interorganizational boundaries.
- 5) The IAC cybersecurity plan requires that any IAC cybersecurity responsibility and accountability reassignment be formally agreed to by all involved stakeholders and documented.
- 6) The IAC cybersecurity plan requires that management-of-change processes consult and inform all associated stakeholders on any modifications impacting an IAC cybersecurity responsibility and

accountability transition point (e.g., changes to firewall rules are communicated to the stakeholders of the IAC security conduits and the IAC security zones connected to or associated with the firewall).

6.1.5.2 Enhanced Profile Requirements

See P2 in the table above for enhanced profile requirements.

6.1.5.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.1.5.4 Supplemental Guidance

- a) When addressing IAC cybersecurity roles-and-responsibilities coordination in the IAC cybersecurity plan, organizations should consider referencing Figure 4 for a list of potential stakeholders that may require some level of coordination.

6.1.5.5 Natural Gas Transmission Pipeline Supplemental Guidance

- b) Special consideration should be given to IAC cybersecurity roles-and-responsibilities coordination regarding FERC's Standards of Conduct (SOC) requirements for transmission function employees' and marketing function employees' compliance with the disclosure of non-public transmission function information.

6.1.6 ID.GV-3—IAC Cybersecurity Legal and Regulatory Requirements

The organization understands its legal, regulatory, and contractual requirements. These requirements can impact an organization's business objectives. Compliance with these requirements helps organizations avoid breaches of legal, regulatory, or contractual obligations related to IAC cybersecurity.

P1: (1); (2); (3)	P2: (1); (2); (3)	P3: (1); (2); (3)
--------------------------	--------------------------	--------------------------

6.1.6.1 Baseline Profile Requirements

- 1) The IAC cybersecurity plan requires that sources of legal and regulatory requirements applicable to or impacting the IAC cybersecurity environment are cataloged.
- 2) The IAC cybersecurity plan requires that legal and regulatory requirements be included in risk management decisions.
- 3) The IAC cybersecurity plan requires that legal and regulatory cybersecurity requirements be clearly communicated to stakeholders.

6.1.6.2 Enhanced Profile Requirements

See P2 in the table above for enhanced profile requirements.

6.1.6.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.1.6.4 Supplemental Guidance

- a) Organizations should consider formal training that is completed at a risk-appropriate frequency on applicable legal and regulatory cybersecurity requirements based on IAC user role.

- b) Organizations should consider implementing formal training as a mechanism to clearly communicate to stakeholders any legal or regulatory cybersecurity requirements.

6.1.7 ID.GV-4—IAC Cybersecurity Governance and Risk Management

Governance and risk management strategies identify the risk tolerance for an organization, what methodologies will be used in assessing risk, strategies to mitigate risk, and a means to periodically evaluate risk in accordance with the organization's risk tolerance.

A well-formed governance and risk management strategy will aid an organization in facilitating a consistent, organization-wide approach in mitigation or acceptance of risk.

Risk management is a fundamental principle of cybersecurity. Managing cybersecurity risk allows an organization to adhere to accepted risk levels for its business objectives.

P1: (1); (2)	P2: (1); (2)	P3: (1); (2)
---------------------	---------------------	---------------------

6.1.7.1 Baseline Profile Requirements

- 1) The IAC cybersecurity plan requires the governance and management of IAC cybersecurity risks.
- 2) The IAC cybersecurity plan requires that IAC cybersecurity governance and risk management consider enterprise cybersecurity governance and risk management.

6.1.7.2 Enhanced Profile Requirements

See P2 in the table above for enhanced profile requirements.

6.1.7.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.2 Risk Management Strategy (ID.RM)

The risk management program is the fundamental cybersecurity program capability. It is a collection of people, processes, and optional technology to systematically address risk, including cybersecurity risk, to organizational objectives, organizational assets, individuals, and other organizations (see 5.2).

The foundation of a risk management program is the risk strategy. It is a structured framing that addresses how organizations intend to assess, respond to, and monitor risk. The risk management strategy is a formal declaration of the organization's priorities (e.g., importance of missions/business functions and trade-offs between varying types of risk); constraints on the risk assessment, response, and monitoring alternatives; risk tolerances (e.g., levels and types of risk, and degrees of risk uncertainty that are acceptable); and assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time. The risk management strategy is explicit, transparent, and used to support operational risk decisions.

P1: (1); (2); (3)	P2: (1); (2); (3)	P3: (1); (2); (3)
--------------------------	--------------------------	--------------------------

6.2.1 Baseline Profile Requirements

- 1) The IAC cybersecurity policy or plan requires that an IAC risk management program exists as part of the IAC cybersecurity program to manage risk to availability, integrity, and information security of the organization's IAC cyber environment(s).

- 2) The IAC cybersecurity policy or plan requires that a formal IAC risk management strategy exists as part of the overall IAC risk management program, which specifies the organization's IAC cyber risk priorities, constraints, tolerances, and assumptions to support operational risk decisions.
- 3) The IAC cybersecurity plan requires that identified IAC cybersecurity risk is only communicated to risk appropriate stakeholders.

6.2.2 Enhanced Profile Requirements

See P2 in the table above for enhanced profile requirements.

6.2.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.2.4 Supplemental Guidance

- a) All factors used in a risk calculation, including the likelihood factors of vulnerabilities and threats along with the impact factors and the resulting risk determination, should be protected and only communicated to those with a legitimate business need to know. Those with a need to know would be considered risk appropriate to receive such information.

6.2.5 ID.RM-1—Risk Management Program

Managing cybersecurity risk is a complex activity that requires the involvement of the entire organization, including senior leaders/executives, mid-level leaders, and individuals operating the control systems supporting the organization's missions/business functions. A risk management process is comprehensive and requires the organization to 1) frame risk (see 6.5); 2) assess risk (see 6.5); 3) respond to risk once determined (see 6.5.9); and 4) monitor risk on an ongoing basis (see 8.2). Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level. It ensures that risk-based decisions are integrated into every aspect of the organization. A sound risk management program has processes that are actively managed and agreed to by organizational stakeholders.

P1: (1); (2)	P2: (1); (2)	P3: (1); (2)
---------------------	---------------------	---------------------

6.2.5.1 Baseline Profile Requirements

- 1) The IAC cybersecurity plan requires that the enterprise risk management strategy be considered when defining IAC cybersecurity risk management strategy.
- 2) The IAC cybersecurity plan requires that the operations risk management strategy be considered when defining IAC cybersecurity risk management strategy.

6.2.5.2 Enhanced Profile Requirements

See P2 in the table above for enhanced profile requirements.

6.2.5.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.2.6 ID.RM-2—Risk Tolerance

A risk management strategy is an explicit declaration of the organization's risk priorities, constraints on the risk assessment, response and monitoring alternatives, risk tolerances (e.g., levels and types of risk, and degrees of risk uncertainty that are acceptable), and assumptions about the threats, vulnerabilities, consequences/impact,

and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time. An organization's risk tolerance is determined and expressed within the risk strategy.

P1: (1); (2); (3)	P2: (1); (2); (4)	P3: (1); (2); (5)
--------------------------	--------------------------	--------------------------

6.2.6.1 Baseline Profile Requirements

- 1) The IAC cybersecurity plan requires that the IAC risk management strategy considers enterprise risk tolerance when documenting IAC risk tolerance.
- 2) The IAC cybersecurity plan requires that the IAC risk tolerance be approved by organizationally defined stakeholders.
- 3) The IAC cybersecurity plan requires that the IAC risk management strategy specifies risk tolerance for baseline profile IAC segregated environments.

6.2.6.2 Enhanced Profile Requirements

- 4) The IAC cybersecurity plan requires that the IAC risk management strategy specify risk tolerance for enhanced profile IAC segregated environments.

6.2.6.3 Extended Profile Requirements

- 5) The IAC cybersecurity plan requires that the IAC risk management strategy specify risk tolerance for extended profile IAC segregated environments.

6.2.7 ID.RM-3—Critical Infrastructure Risk Tolerance

The organization's place in critical infrastructure should be identified and clearly communicated. The objective of the critical infrastructure risk tolerance activities is to ensure the organizational roles in these contexts are considered during risk analysis in the organization's determination of its risk tolerance and resulting risk responses.

P1: None	P2: (1); (2); (3); (4); (5)	P3: (1); (2); (3); (4); (5)
-----------------	------------------------------------	------------------------------------

6.2.7.1 Baseline Profile Requirements

There are no baseline profile-specific requirements.

6.2.7.2 Enhanced Profile Requirements

- 1) The IAC cybersecurity plan requires that risk management processes document the organization's role in the critical infrastructure risk in the IAC risk management strategy document.
- 2) The IAC cybersecurity plan requires that the organization's role in the critical infrastructure risk is incorporated into the organization's risk tolerance posture.
- 3) The IAC cybersecurity plan requires that the organization's role in the critical infrastructure risk is considered in risk management decisions, including, but not limited to, risk assessment (e.g., likelihood and impact calculations), rating risk (e.g., risk criticality rating), and risk response actions and prioritization.
- 4) The IAC cybersecurity plan requires that the organization's role in the critical infrastructure risk is considered in decisions regarding the definition of roles and assignment of responsibilities.

- 5) The IAC cybersecurity plan requires that IAC cybersecurity awareness training clearly communicates and educates on the organization's role in the critical infrastructure risk.

6.2.7.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.2.7.4 Supplemental Guidance

- a) The role in critical infrastructure should be considered when assessing or managing the risk of IAC cyber environments.

6.3 Business Environment (ID.BE)

Cybersecurity roles, responsibilities, and risk management decisions depend on the business environment that an organization operates in. The objective of understanding the business environment as it relates to cybersecurity is to prioritize and communicate the protection strategy, accounting for the organization's mission, objectives, critical services, and relation to the critical infrastructure of the sector in which the organization operates.

P1: None	P2: (1)	P3: (1)
-----------------	----------------	----------------

6.3.1 Baseline Profile Requirements

There are no baseline profile-specific requirements.

6.3.2 Enhanced Profile Requirements

- 1) The IAC cybersecurity policy or Plan requires that the IAC risk management strategy document the organization's role in the critical infrastructure essential products and services supply chain, both upstream critical infrastructure suppliers and downstream critical infrastructure customers.

NOTE See 6.2.

6.3.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.3.4 ID.BE-1—Critical Infrastructure Supply Chain Role

For the organization to understand the entirety of the potential risk associated with its operations, it is necessary that the organization's role in the critical infrastructure supply chain is identified and communicated. The objective of the critical infrastructure supply chain role activities is to ensure the organizational roles within the supply chain are identified and considered during risk analysis and the organization's determination of risk tolerance and risk responses.

P1: None	P2: (1); (2); (3)	P3: (1); (2); (3)
-----------------	--------------------------	--------------------------

6.3.4.1 Baseline Profile Requirements

There are no baseline profile-specific requirements.

6.3.4.2 Enhanced Profile Requirements

- 1) The IAC cybersecurity plan requires that the organization's role in the critical infrastructure supply chain influences the organization's risk tolerance posture.

- 2) The IAC cybersecurity plan requires that the organization's role in the critical infrastructure supply chain is included in risk management decisions, including, but not limited to, risk assessment (e.g., likelihood and impact calculations), rating risk (e.g., risk criticality rating), and risk response actions and prioritization.
- 3) The IAC cybersecurity plan requires that the organization's role in the critical infrastructure supply chain is communicated to stakeholders.

6.3.4.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.3.4.4 Supplemental Guidance

- a) The impact of IAC essential function disruptions and outages should be influenced by their role in the critical infrastructure supply chain.
- b) The organization's role in the critical infrastructure supply chain can influence the assignment of IAC cybersecurity responsibilities.

6.3.5 ID.BE-2—Critical Infrastructure and Industry Sector Roles

The role of an organization in providing for and supporting critical infrastructure and industry sectors should be defined, understood, and communicated. This is important to meet the objective of developing protection strategies based on the prioritization of critical assets and resources.

P1: None	P2: (1); (2); (3)	P3: (1); (2); (3)
-----------------	--------------------------	--------------------------

6.3.5.1 Baseline Profile Requirements

There are no baseline profile-specific requirements.

6.3.5.2 Enhanced Profile Requirements

- 1) The IAC cybersecurity plan requires that the IAC risk management strategy documents the organization's role in the critical infrastructure and other sector-specific risk.
- 2) The IAC cybersecurity plan requires that the organization's role in the critical infrastructure and other sector-specific risk is incorporated into the organization's risk tolerance posture and risk responses.
- 3) The IAC cybersecurity plan requires that the organization's role in the critical infrastructure and other sector-specific risk is included in risk management decisions, including, but not limited to, risk assessment (e.g., likelihood and impact calculations), rating risk (e.g., risk criticality rating), and risk response actions and prioritization.

6.3.5.3 Extended Profile Requirements

See P3 in the table above for extended profile requirements.

6.3.5.4 Supplemental Guidance

- a) An IAC cyber asset's role in critical infrastructure should be considered during its IAC security zone or IAC security conduit impact assessment.