Pipeline Cybersecurity – API-1164v3

A NIST CSF Based Community Solution for Pipeline Cybersecurity Regulations

22 March 2022

Agenda

- Introduction
- What is API 1164
- History of the standard
- Key Objectives for Version 3
- Building Blocks of API 1164
- Applicability and flexibility
- Deploying the standard
- High-level overview
- Q&A

Kimberly Denbow
Managing Director, Security & Operations

David White
Founder & President
Axio

What is API 1164?

- API 1164 is a security standard for pipeline and SCADA systems. Version 1 was developed after the terrorist attacks on September 11th, 2001.
- The standard “provides guidance to the operators of oil and gas liquids pipeline systems for managing SCADA system integrity and security.”
- Primary objectives of the standard:
  - Analyze vulnerabilities that can be further exploited
  - List the processes to identify these system vulnerabilities
  - Provide a list of best practices to harden the core architecture
  - Provide examples of industry best practices

axio

Key Terms in API 1164 V3

- **Industrial Automation and Control Systems (IACS)** – From ISA/IEC 62443, a collection of personnel, hardware, software, and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation. As used in API-1164v3, this includes, but is not limited to, supervisory control and data acquisition (SCADA), local control, and industrial internet of things (IIoT) solutions [aka *ICS or OT*].

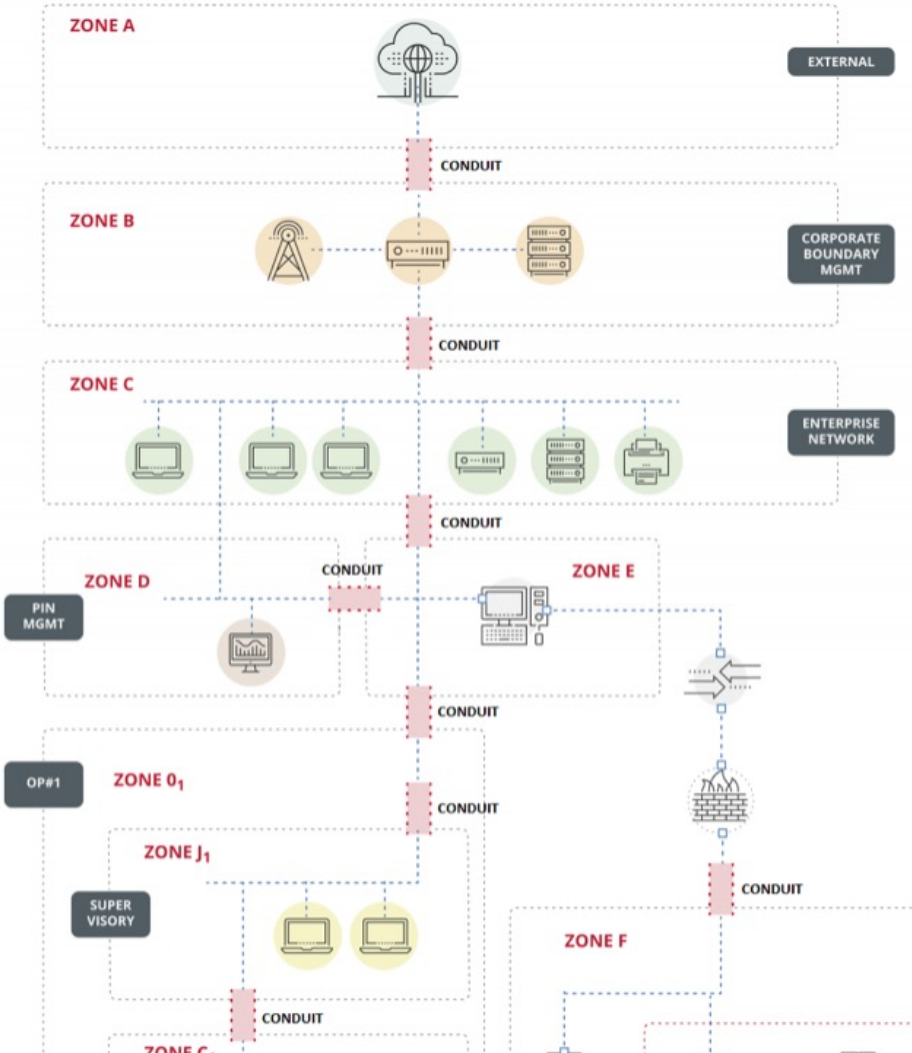
- **IAC Cybersecurity Profile** – From API-1164v3, A collection of defined IAC (industrial automation and control) cyber activities and desired outcomes (functions, categories, subcategories, procedures, practices, and controls) that manages risk to mission/business objectives. API-1164v3 defines three IAC cybersecurity profiles: Baseline, Extended, or Enhanced.

- **Protection Requirements** – Set of protections (for each profile) aligned to the NIST Cyber Security Framework, derived from NIST 800-53 and NIST 800-82 [aka *controls*]

Key Terms in API 1164 V3

- **Security Zones** – Groups of physical or logical assets that share common security requirements, which have clearly defined borders (physical or logical).
- **Security Conduits** – Connections among Security Zones are called conduits and must include security measures in order to control their access, resist denial of service attacks, prevent the spreading of any other type of attack, act as a shield for other systems in the network and protect the integrity and confidentiality of communications.

Diagram from
https://www.incibe-cert.es/en/blog/zones-and-conduits-protecting-our-industrial-network



axio

History of API 1164

An effort to secure SCADA systems

API Standard 1164 v1, September 2004

Initially created to provide guidance to the operators of oil and gas liquid pipeline systems for managing SCADA system integrity and security.

API Standard 1164 v2, June 2009

Updated based on a cross review with

- Other API standards
- DOE's *21 Steps to Improve Cyber Security of SCADA Networks*
- National Institute of Standards and Technology (NIST) 800 Series.

API Standard 1164 v3, August 2021

Rewritten to

- Increase scope to cover all pipeline OT environments (SCADA, local controls and IIoT) for both oil and natural gas
- Harmonize with the NIST Cybersecurity Framework (CSF)
- Cover requirements from the 2018 TSA Pipeline Security Guidelines

Key Objectives for Version 3

Consensus based approach with support from oil and natural gas community and federal partners

API 1164 v3 is built on fundamental security principles that largely extend to other sectors

Progression based which can be customized to any sized entity across industries

Protections in the standard are driven by organizations':

- Business and Mission Objectives
- Significant Threats
- Significant Impacts
- Organization Specific Constraints

Expanded scope to address threat emanating from increasingly converged environments

axio

Collaboration was Key

By the Numbers:

5,000+ hours of work by pipeline owner/operators	Nearly three years of development	75+ industry expert contributors
300 Working Sessions	50+ Companies Participated	25 full-day workshops

Contributors included:

AGA

API American Petroleum Institute

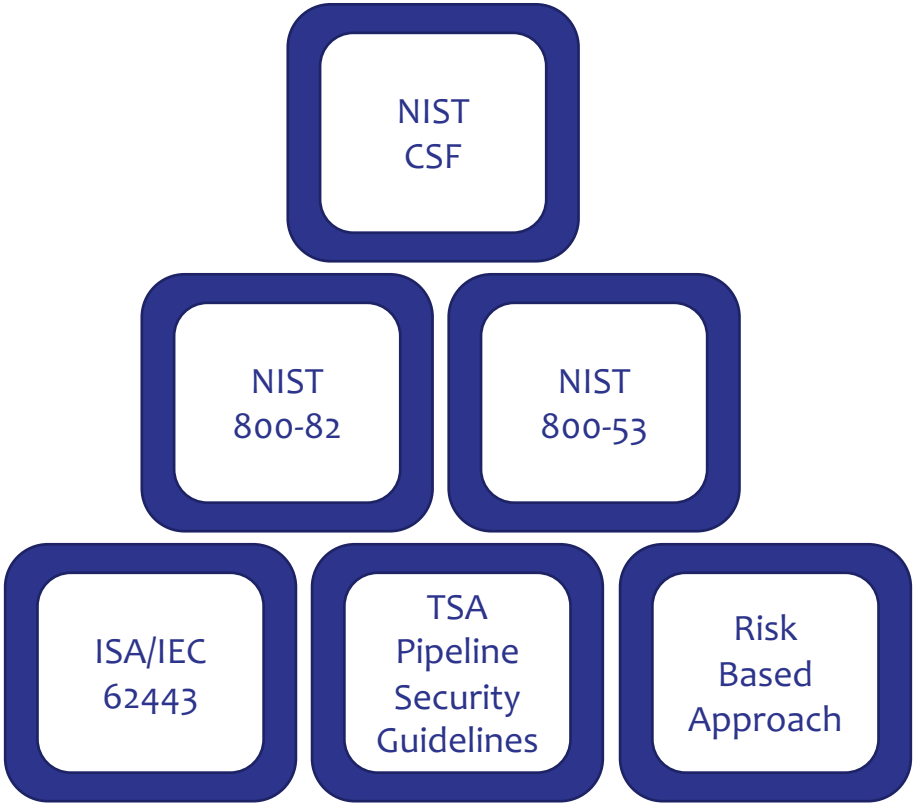
PHMSA

Transportation Security Administration

CISA CYBER+INFRASTRUCTURE

INGAA Interstate Natural Gas Association of America

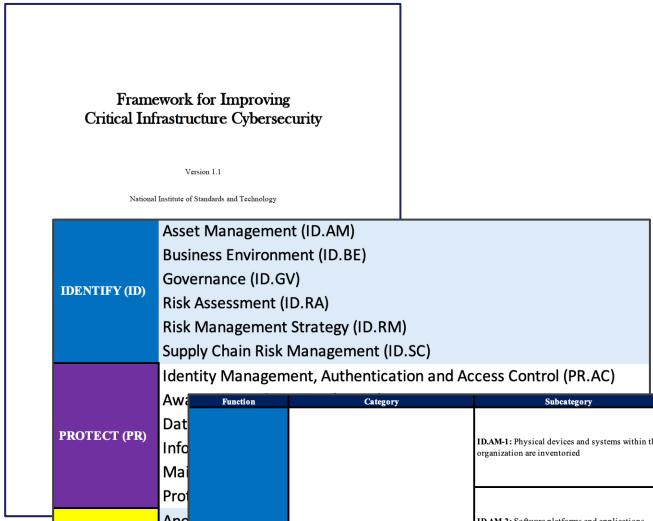
Building Blocks of API 1164



API 1164v3 Implements NIST CSF for pipelines

NIST CSF

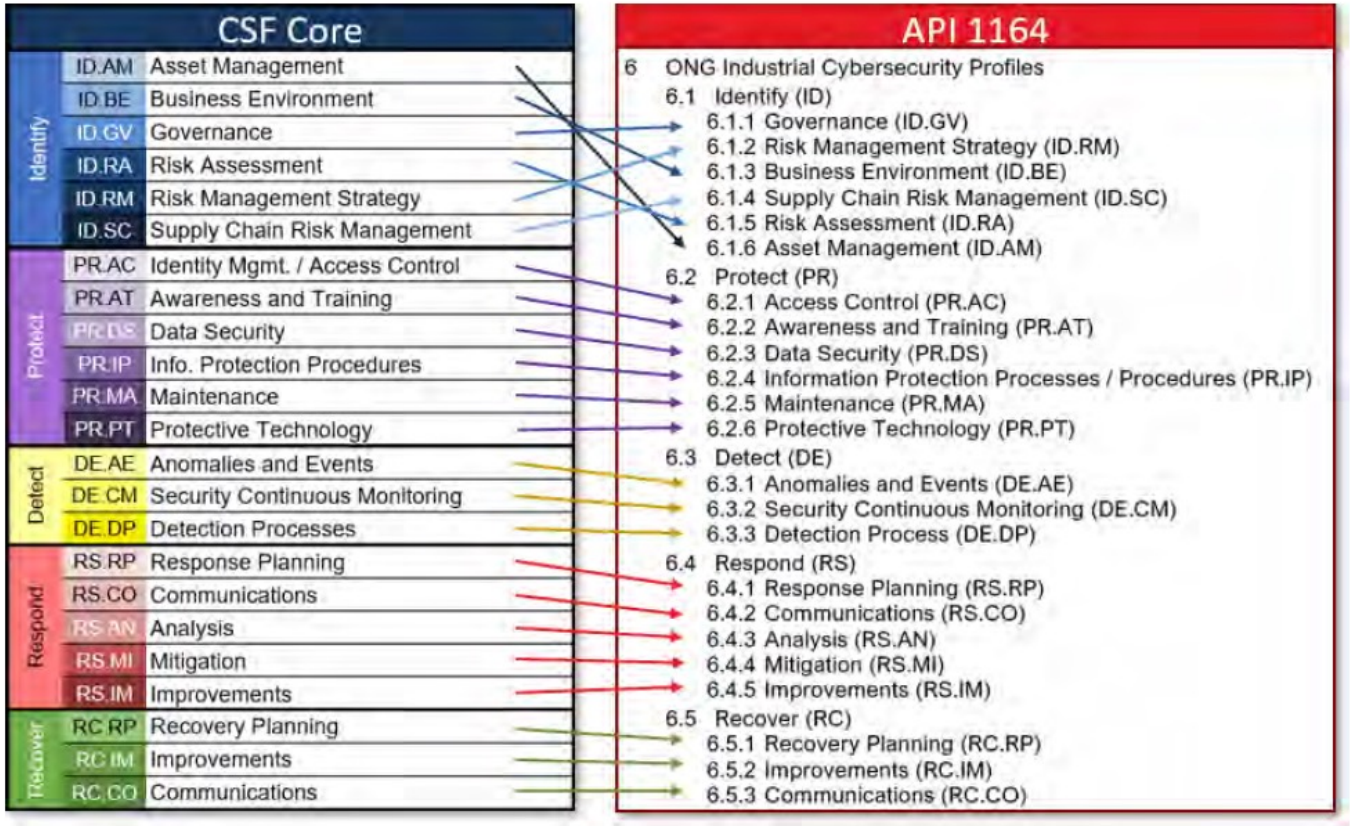
- NIST Cyber Security Framework provides the **organizational construct**
  - API Adopted the NIST CSF Framework Core to organize protection requirements
  - Structure enables clear mapping from NIST CSF to API 1164v3
- **Protection Requirements** are derived from NIST CSF Informative References NIST 800-53 and NIST 800-82
- Methodology for defining Security Zones to apply Protection Requirements based on ISA/IEC 62443



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	- **CIS CSC** 1 - **COBIT 5** BAI09.01, BAI09.02 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISA 62443-3-3:2013** SR 7.8 - **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 - **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	- **CIS CSC** 2 - **COBIT 5** BAI09.01, BAI09.02, BAI09.05 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISA 62443-3-3:2013** SR 7.8 - **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 - **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	- **CIS CSC** 12 - **COBIT 5** DSS05.02 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 - **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	- **CIS CSC** 12 - **COBIT 5** APO02.02, APO10.04, DSS01.02 - **ISO/IEC 27001:2013** A.11.2.6 - **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	- **CIS CSC** 13, 14 - **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 - **ISA 62443-2-1:2009** 4.2.3.6 - **ISO/IEC 27001:2013** A.8.2.1 - **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	- **CIS CSC** 17, 19 - **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 - **ISA 62443-2-1:2009** 4.3.2.3.3 - **ISO/IEC 27001:2013** A.6.1.1 - **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Organization of API 1164 v3 rooted in NIST CSF

NIST CSF



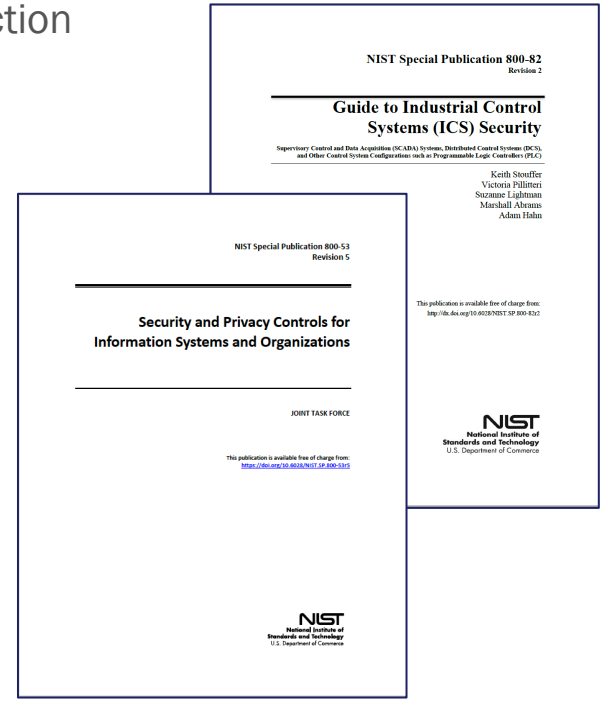
API 1164 V3 Architecture

NIST CSF Function	Baseline (P1) Profile	Enhanced (P2) Profile	Extended (P3) Profile
Identify	P1 Protection Requirements (controls)	P2 Protection Requirements (controls)	P3 Protection Requirements (controls)
Detect			
Protect			
Respond			
Recover			

Protection Requirements sourced directly from NIST 800-53 and NIST 800-82

NIST 800-82 & 800-53

- NIST Special Publications form the basis for protection requirements in API 1164 V3:
  - *800-53 Security and Privacy Controls for Information Systems and Organizations*
  - 800-82 *Guide to Industrial Systems Security*
- Guidance and Controls from NIST are:
  - Identified in NIST CSF references
  - Mapped and reconciled
  - Analyzed for relevance and applicability
  - Refined into actionable protection requirements
  - Further detailed with supplemental guidance



axio

ISA/IEC 62443 Cybersecurity Standards

Security of Industrial Automation and Control Systems (IACS)

ISA/IEC 62443

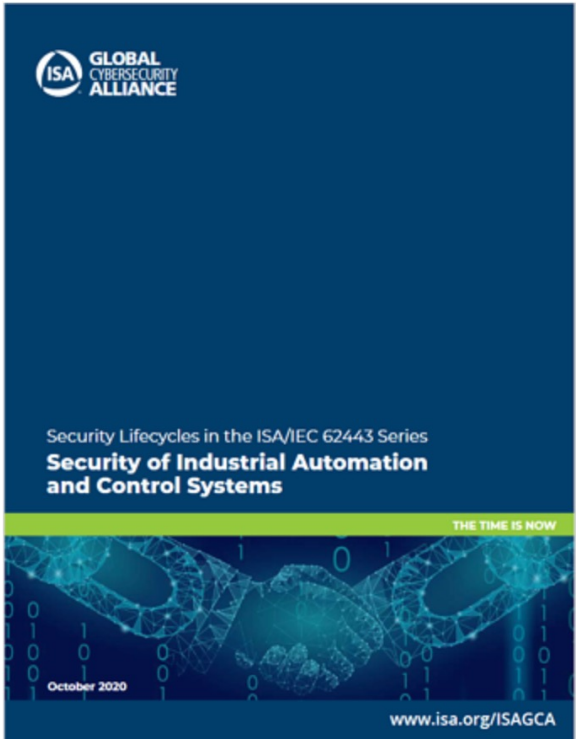
- Joint effort of The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) to improve IACS cybersecurity
- Engineered approach for IACS cybersecurity
- Initially developed for the industrial process sector but since expanded to apply to other sectors
- Brought together industrial cyber security experts from across the globe to develop standards on industrial automation and control systems security that are applicable to all industry sectors and critical infrastructure

Incorporating ISA/IEC 62443 into the Standard

API 1164 v3 used ISA/IEC 62443 methodologies to tie together disparate Security Concepts

ISA/IEC 62443

- API 1164 v3 mapped and refined content from ISA/IEC 62443
- The standard went beyond even what is listed in NIST CSF informative references to pull and incorporate content from the entire family of 62443 standards (2 Standards in CSF vs. 6 in API1164 v3)
- The result is a standard that represents the best in breed of security standards focused on pipeline environments



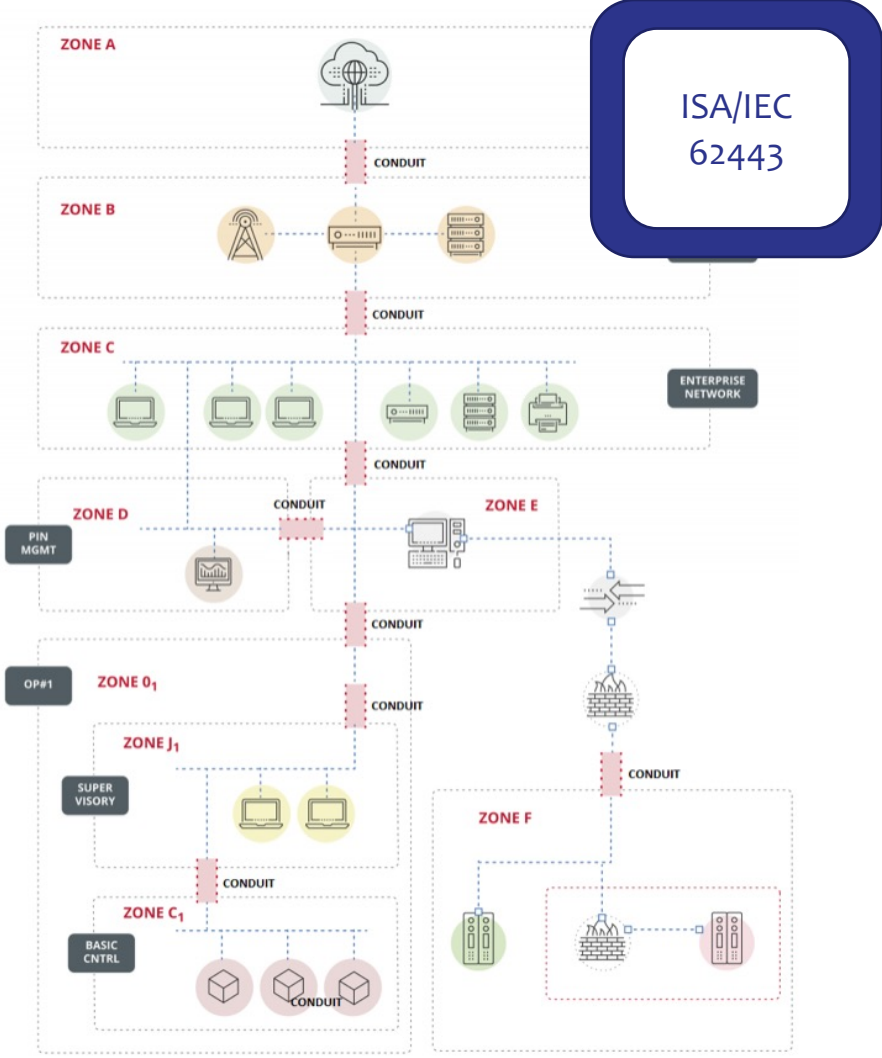
Incorporating ISA/IEC 62443

Security zones and conduits

API 1164 v3 draws on ISA/IEC 62443 to bring clarity to protection boundaries

- **Security Zones** – Groups of physical or logical assets that share common security requirements, which have clearly defined borders (physical or logical).
- **Security Conduits** – Connections among Security Zones are called conduits and must include security measures in order to control their access, resist denial of service attacks, prevent the spreading of any other type of attack, act as a shield for other systems in the network and protect the integrity and confidentiality of communications.

Diagram from
https://www.incibe-cert.es/en/blog/zones-and-conduits-protecting-our-industrial-network

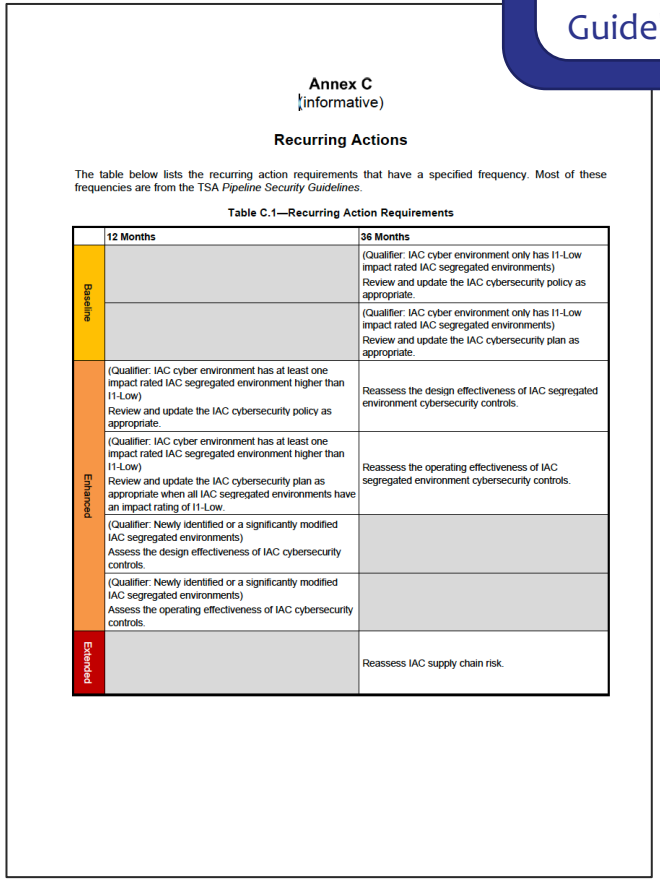


axio

Incorporating TSA Pipeline Security Guidelines

TSA Pipeline Security Guidelines

- Security Guidelines have been incorporated into the Standard in version 3
  - API 1164 v3 addresses all security measures in the Guidelines
  - Content from the guidelines included directly in the body of API 1164V3 protection requirements
  - *Baseline* and *Enhanced* security measures from the guidelines have been further broken down adding an *Extended* grouping for more granularity.
  - The Standard now includes timelines for Recurring Actions Requirements to bring it into alignment with the Guidelines



Annex C
(informative)

Recurring Actions

The table below lists the recurring action requirements that have a specified frequency. Most of these frequencies are from the TSA *Pipeline Security Guidelines*.

Table C.1—Recurring Action Requirements

	12 Months	36 Months
Baseline		(Qualifier: IAC cyber environment only has I1-Low impact rated IAC segregated environments) Review and update the IAC cybersecurity policy as appropriate.
Baseline		(Qualifier: IAC cyber environment only has I1-Low impact rated IAC segregated environments) Review and update the IAC cybersecurity plan as appropriate.
Enhanced	(Qualifier: IAC cyber environment has at least one impact rated IAC segregated environment higher than I1-Low) Review and update the IAC cybersecurity policy as appropriate.	Reassess the design effectiveness of IAC segregated environment cybersecurity controls.
Enhanced	(Qualifier: IAC cyber environment has at least one impact rated IAC segregated environment higher than I1-Low) Review and update the IAC cybersecurity plan as appropriate when all IAC segregated environments have an impact rating of I1-Low.	Reassess the operating effectiveness of IAC segregated environment cybersecurity controls.
Enhanced	(Qualifier: Newly identified or a significantly modified IAC segregated environments) Assess the design effectiveness of IAC cybersecurity controls.	
Enhanced	(Qualifier: Newly identified or a significantly modified IAC segregated environments) Assess the operating effectiveness of IAC cybersecurity controls.	
Extended		Reassess IAC supply chain risk.

Line of sight from API 1164 to TSA Pipeline Security Guidelines

- API 1164v3 and the TSA Pipeline Security Guidelines leverage NIST CSF as an organizing construct creating an inherent mapping
  - Common denominator allows for simple referencing
  - Adopting the Standard meets or exceeds the security measures laid out in the guidelines

TSA Pipeline Security Guidelines

Annex A
(informative)

API Standard 1164 Construction and Mapping

A.1 U.S. TSA Pipeline Security Guidelines Inclusion

The U.S. Transportation Security Administration (TSA) maintains the *Pipeline Security Guidelines* document. The scope of TSA's guidelines is applicable to operational natural gas and hazardous liquid transmission pipelines, natural gas distribution pipeline systems, and liquified natural gas facility operators. The guidelines are also applicable to operational pipeline systems that transport materials categorized as toxic inhalation hazards. The TSA guidelines provide criteria that operators must use to assess and determine criticality of each of their facilities. The guidelines identify baseline security risk-reduction measures that must be implemented at each facility, as well as enhanced measures that must be implemented at facilities determined to be critical.

In March 2018, TSA issued a revised version to address challenges in the everchanging security landscape. A significant update implemented was to align the TSA cybersecurity principles, aspects, and requirements to the NIST CSF. TSA did this by mapping their baseline and enhanced security measures to the NIST Framework Core.

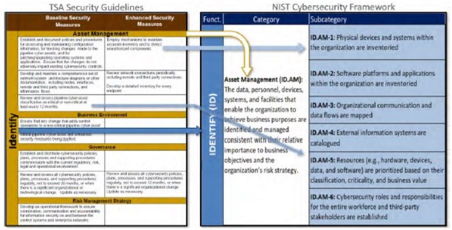


Figure A.1—TSA Cybersecurity Measures to CSF Core Mapping

The baseline measures and enhanced measures specified in *Pipeline Security Guidelines* are used to apply a security control rating of "baseline" or "enhanced". API 1164 has leveraged this and refined it into three levels of security protections.

A.2 NIST Cybersecurity Framework Foundation

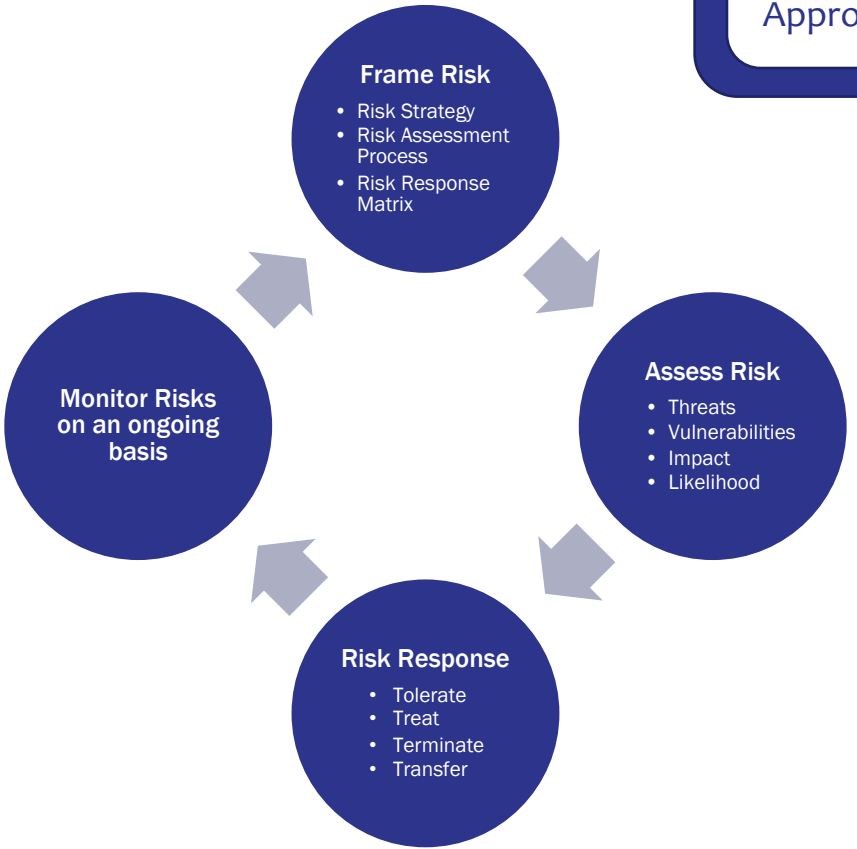
The NIST Cybersecurity Framework allows significant freedom in how it is used or implemented. This is reinforced by clearly stating that the presentation format chosen for the Framework Core is not to be interpreted as prescribing a security program's implementation order or priority. This standard leverages this flexibility to align the Framework Core to one of its guiding tenets: actionable and thereby implementable.

axio

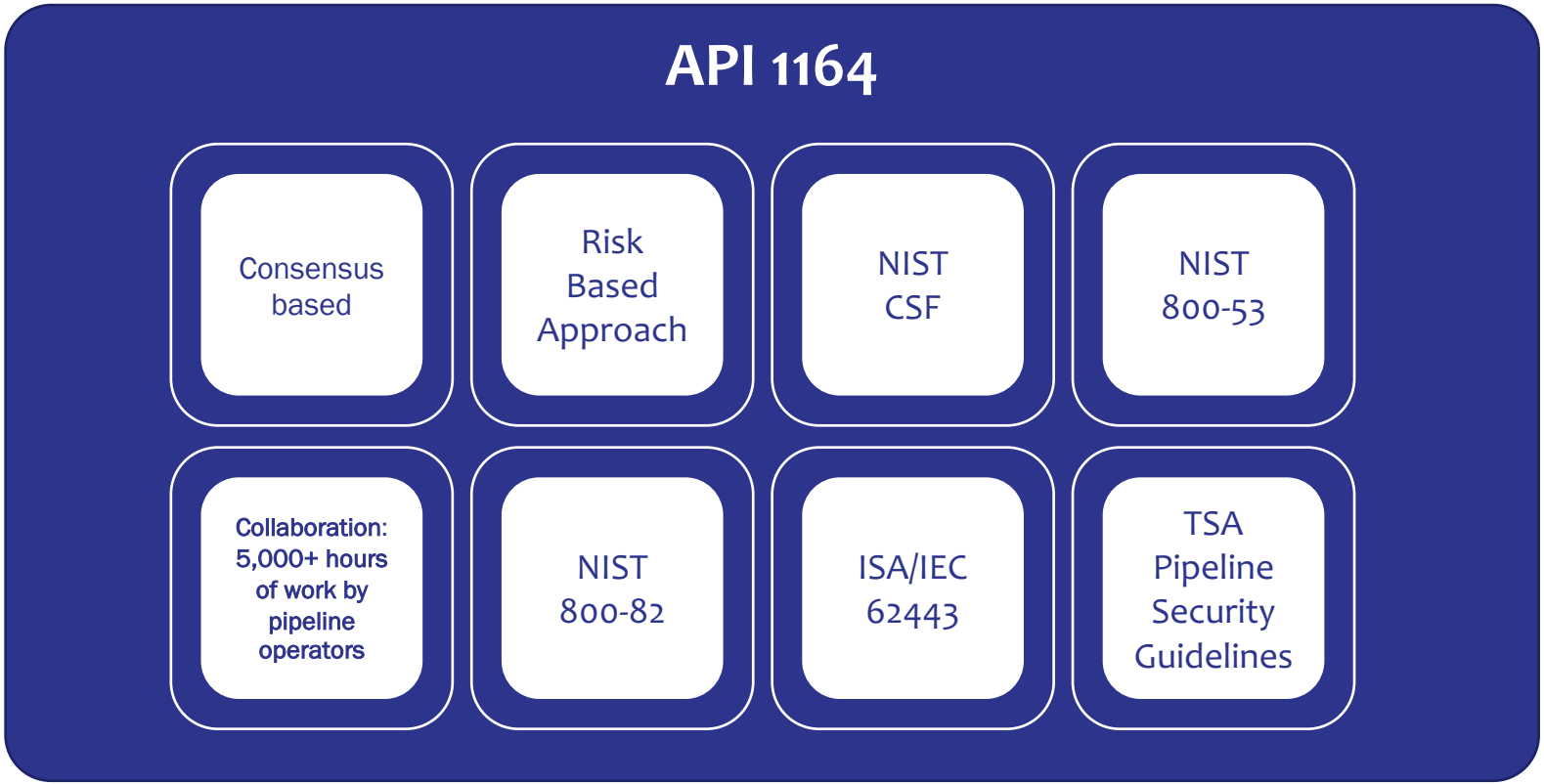
Built on a Foundation of Risk Management

Risk Based Approach

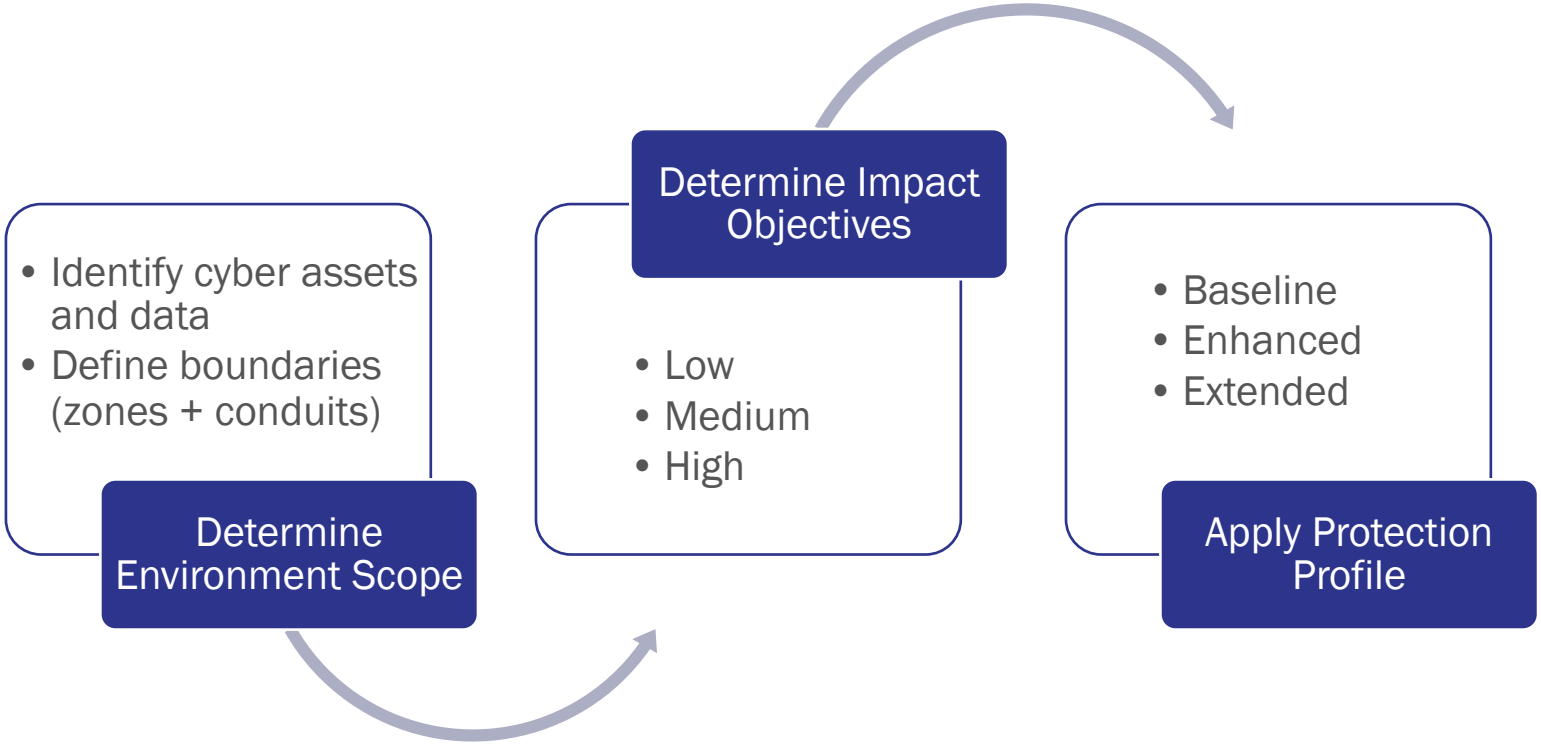
- API 1164 v3 outlines a methodology for:
  - Defining a Risk Management Strategy
  - Consistently Assessing Risks
  - Defining Risk Tolerances
  - Formally Responding to Risks
  - Monitoring Risks
- Outputs of Risk Management processes shape how protections are selected and applied



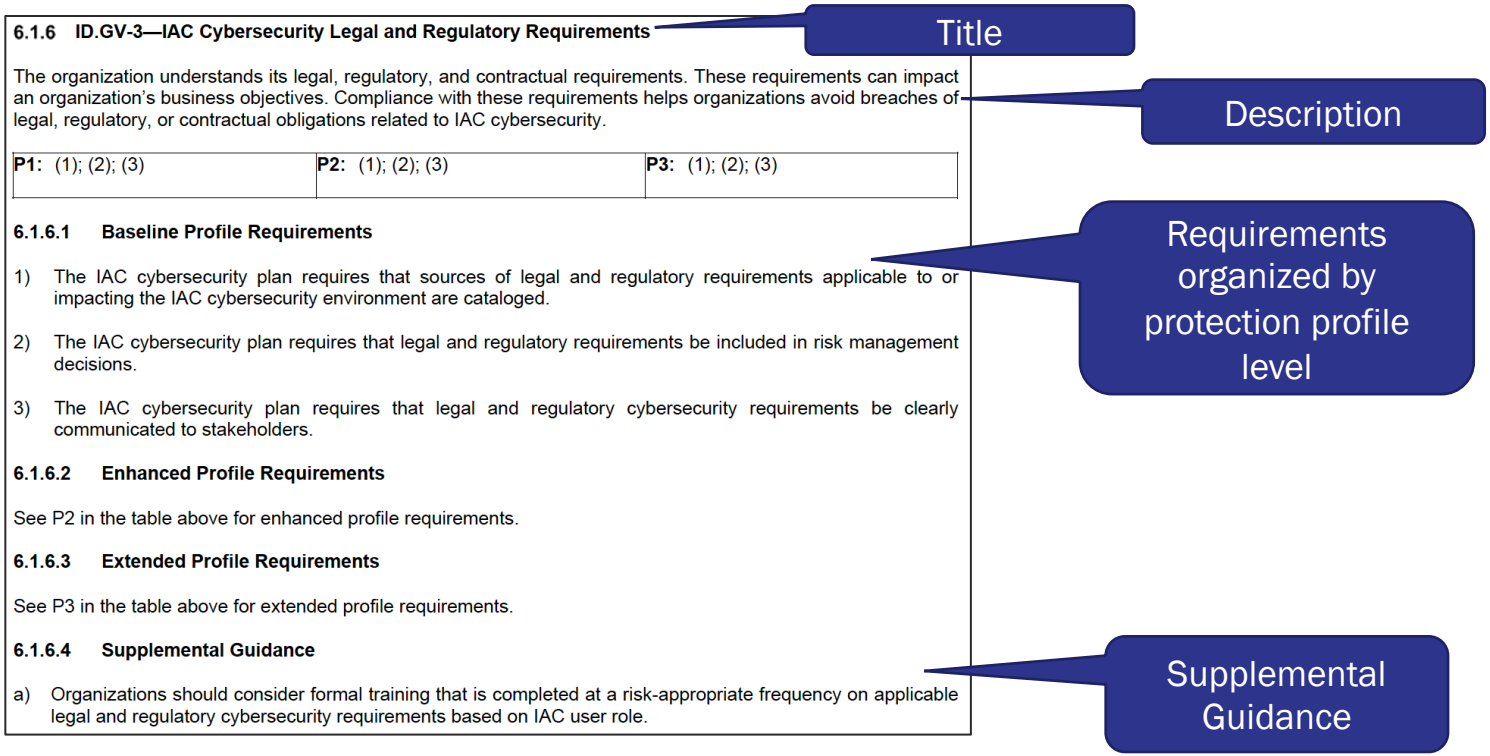
Revisiting the Building Blocks of API 1164 V3



Deploying the Standard



Anatomy of a Protection Requirement in API 1164 v3



Protection Requirements in the context of risk

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.

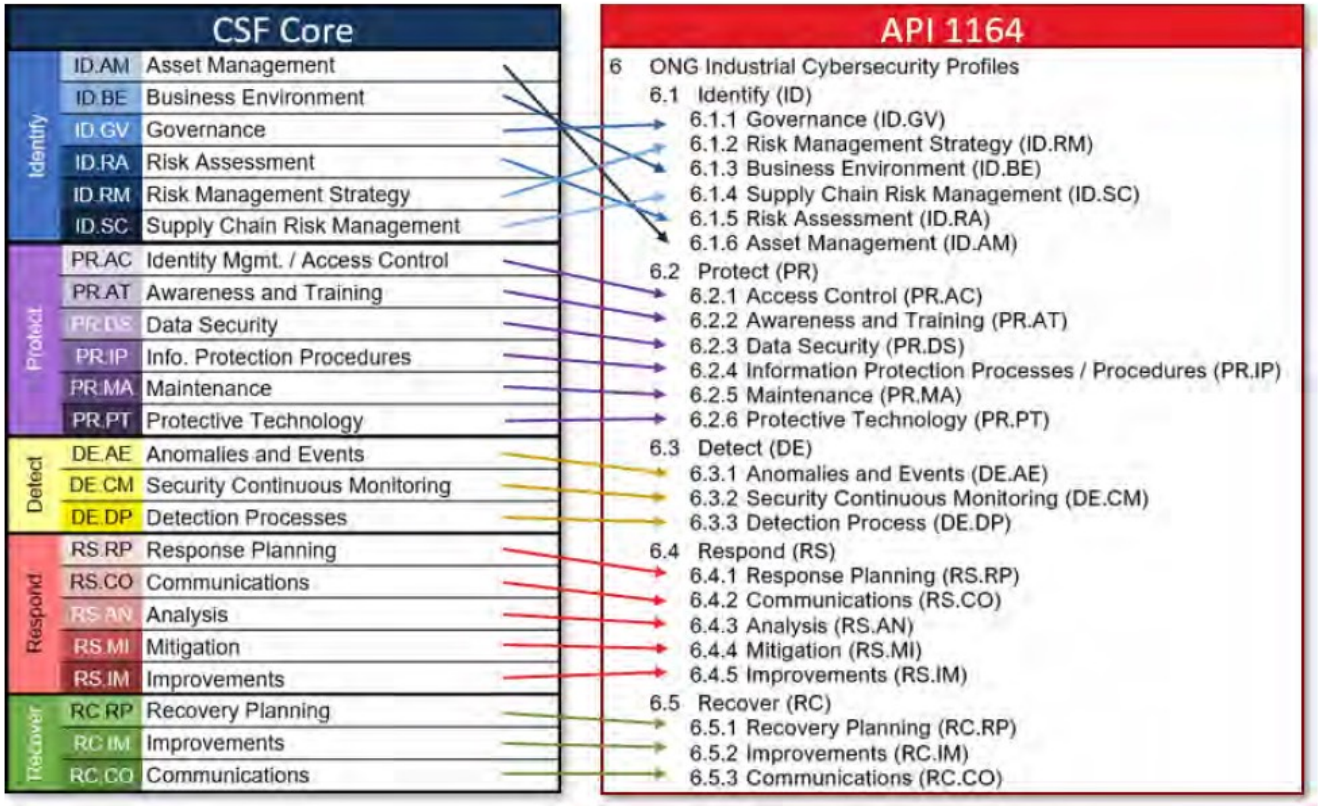
2) The IAC cybersecurity plan requires that the organization's role in the critical infrastructure risk is incorporated into the organization's risk tolerance posture.

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.

Requirements vary based on risk tolerance

Applicability and Flexibility



Who can leverage API 1164 V3?

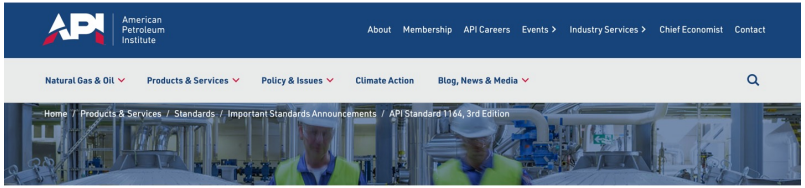
Stakeholders from a variety of functions and backgrounds concerned with Industrial and Automation Control System Security can leverage the standard.

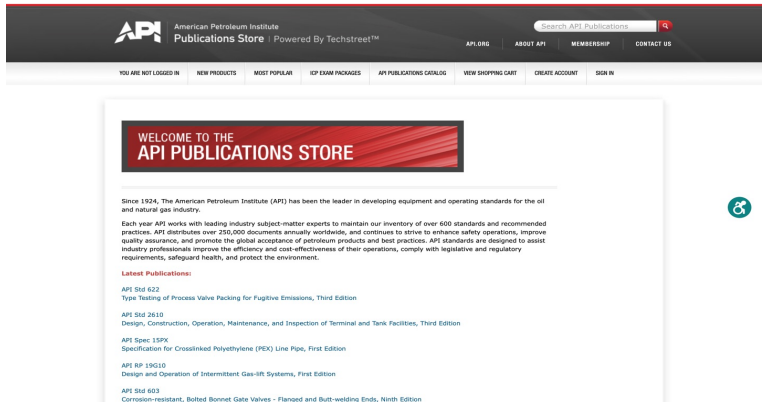
Example Stakeholders include:

- Managers responsible for pipeline systems
- Information Technology (IT) staff (e.g., system administrators, network administrators)
- Operational Technology (OT) staff (e.g., control engineers, integrators, and architects)
- Supply chain stakeholders (e.g., products and services vendors)
- Regulators concerned with pipeline and broader OT cybersecurity
- Government stakeholders concerned with pipeline and broader security needs
- Researchers, academic institutions, and analysts

Accessing API 1164 V3

- The API 1164 V3 Standard is available at through the API website and API Publication store
- Electronic PDF and Print versions are available at www.techstreet.com





Q & A