The Framework for Improving Critical Infrastructure Cybersecurity

December 2017

cyberframework@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

National Institute of Standards and Technology

About NIST

- Agency of U.S. Department of Commerce
- NIST's mission is to develop and promote measurement, standards and technology to enhance productivity, facilitate trade, and improve the quality of life.
- Federal, non-regulatory agency around since 1901

NIST Cybersecurity

- Cybersecurity since the 1970s
- Computer Security Resource Center – csrc.nist.gov

NIST Priority Research Areas


Advanced Manufacturing


IT and Cybersecurity


Healthcare


Forensic Science


Disaster Resilience


Cyber-physical Systems


Advanced Communications

Cybersecurity Framework *Initial* Charter

Improving Critical Infrastructure Cybersecurity

February 12, 2013

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

Executive Order 13636

December 18, 2014

Amends the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) to say:

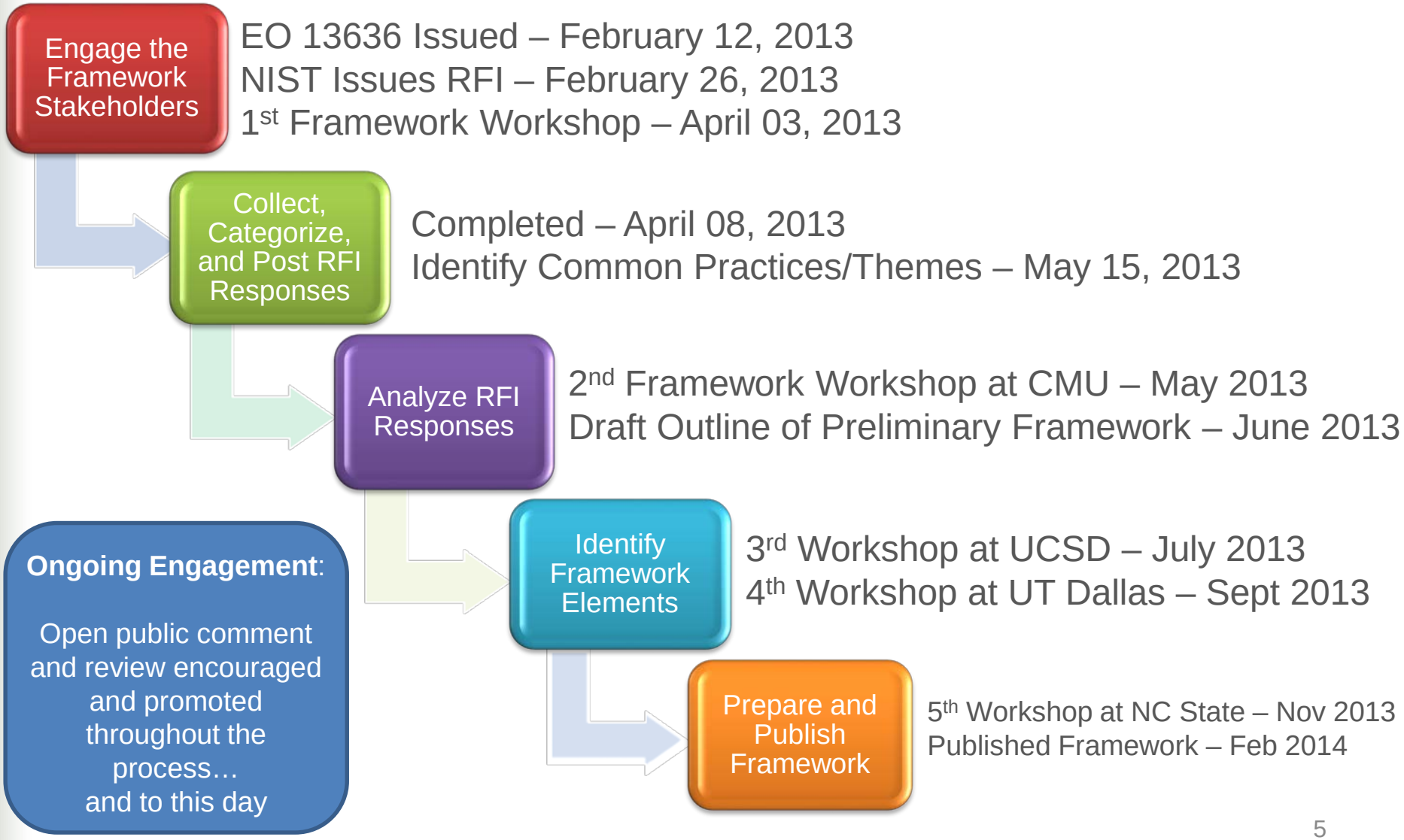
"…on an ongoing basis, facilitate and support the development of a ***voluntary***, ***consensus-based***, ***industry-led*** *set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure*"

Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

Requirements from the Executive Order

- Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Identify areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations
- Be consistent with voluntary international standards

Multistakeholder Development Process



Key Attributes

It's flexible to many sectors

- Meant to be *customized*.

It's a catalog of cybersecurity outcomes

- Provides a *common language* and systematic methodology for managing cyber risk.
- Does not tell an organization *how* much cyber risk is tolerable, nor provide "the one and only" formula for cybersecurity.

It's meant to be paired

- Take advantage of great pre-existing things

It's a living document

- Enable best practices to become *standard practices for everyone*
- Can be updated as *technology and threats* changes.
- Evolves *faster* than regulation and legislation
- Can be updated as stakeholders *learn from implementation*

Cybersecurity Framework *Current* Charter

Improving Critical Infrastructure Cybersecurity

February 12, 2013

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

Executive Order 13636

December 18, 2014

Amends the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) to say:

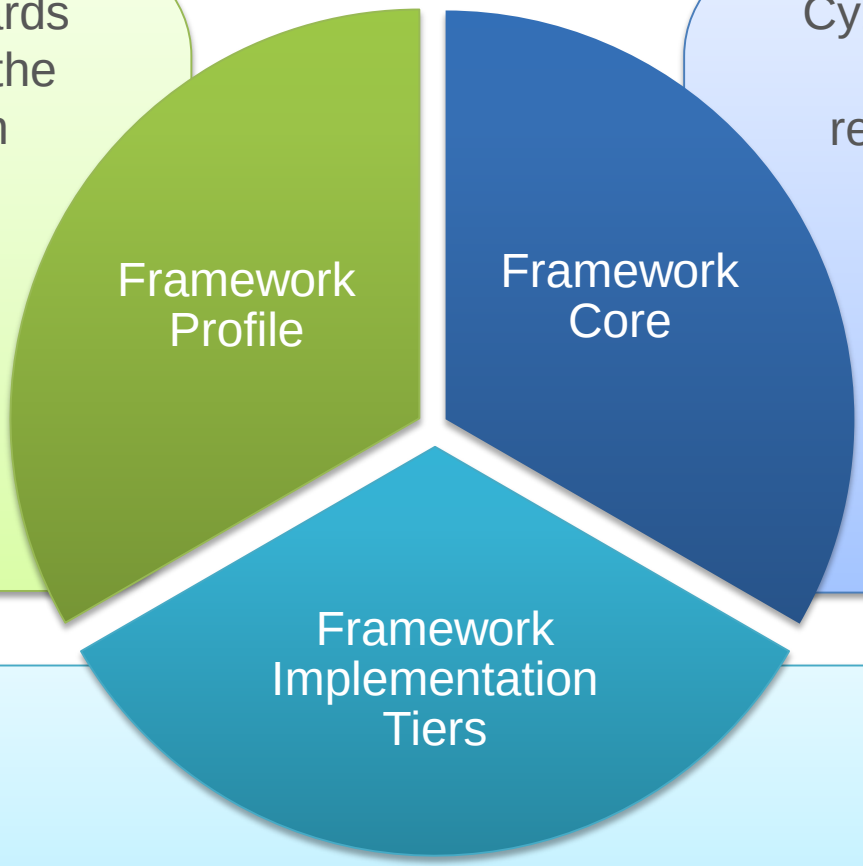
"…on an ongoing basis, facilitate and support the development of a ***voluntary***, ***consensus-based***, ***industry-led*** *set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure*"

Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

Cybersecurity Framework Components

Aligns industry standards and best practices to the Framework Core in an implementation scenario

Supports prioritization and measurement while factoring in business needs

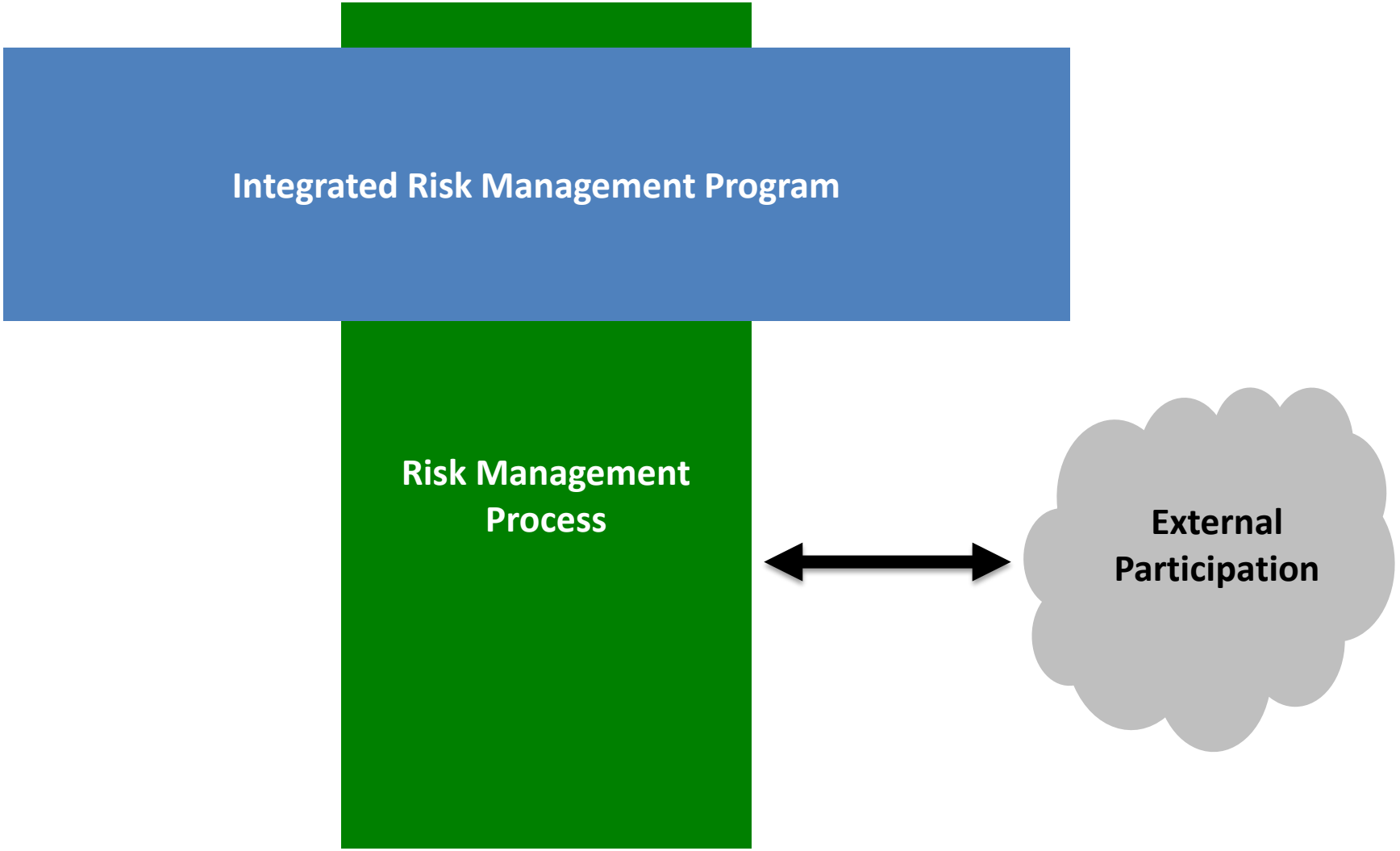


Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Key Properties of Cyber Risk Management



Implementation Tiers

	1	2	3	4
	Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization benefits my sharing or receiving information from outside parties			

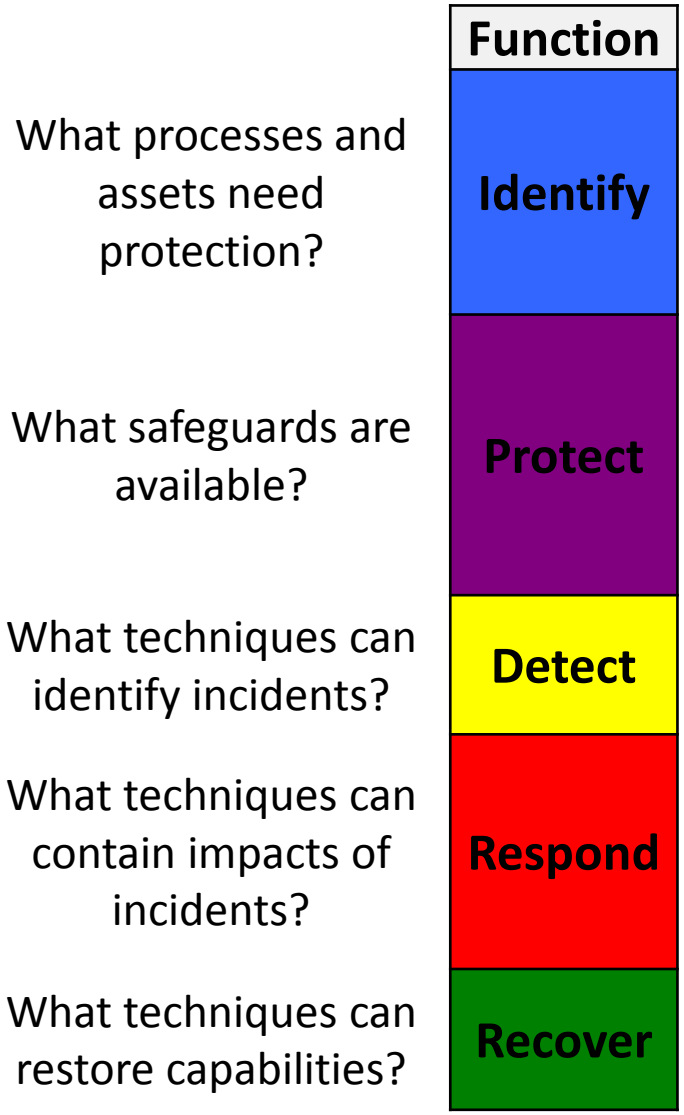
Intel Adaptation of Implementation Tiers

	1 Partial	2 Risk Informed	3 Repeatable	4 Adaptive
People	Whether people have assigned roles, regular training, take initiative by becoming champions, etc.			
Process	*Risk Management Process* + *Integrated Risk Management Program*			
Technology	Whether tools are implemented, maintained, evolved, provide effectiveness metrics, etc.			
Ecosystem	*External Participation* + Whether the organization understands its role in the ecosystem, including external dependencies with partners			

Case Study Available At:
https://www.nist.gov/cybersecurity-framework/cybersecurity-framework-industry-resources

Core

A Catalog of Cybersecurity Outcomes



- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

Core

A Catalog of Cybersecurity Outcomes

	Function	Category
What processes and assets need protection?	**Identify**	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
What safeguards are available?	**Protect**	Access Control
		Awareness and Training
		Data Security
		Information Protection Processes & Procedures
		Maintenance
		Protective Technology
What techniques can identify incidents?	**Detect**	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
What techniques can contain impacts of incidents?	**Respond**	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
What techniques can restore capabilities?	**Recover**	Recovery Planning
		Improvements
		Communications

Core – Example

Cybersecurity Framework Component

Function	Category	Subcategory	Informative Reference
Identify	Business Environment	**ID.BE-3**: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14

14

Core – Example

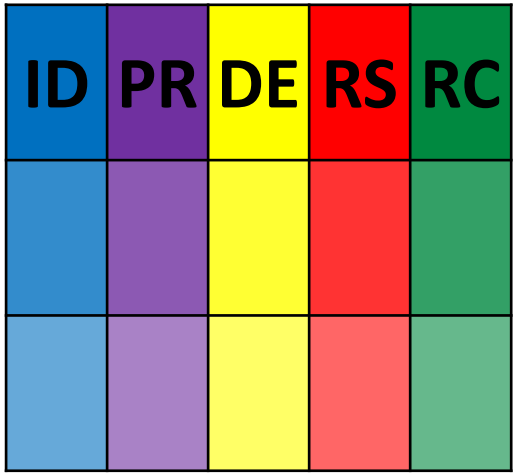
Cybersecurity Framework Component

Function	Category	Subcategory	Informative Reference
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1

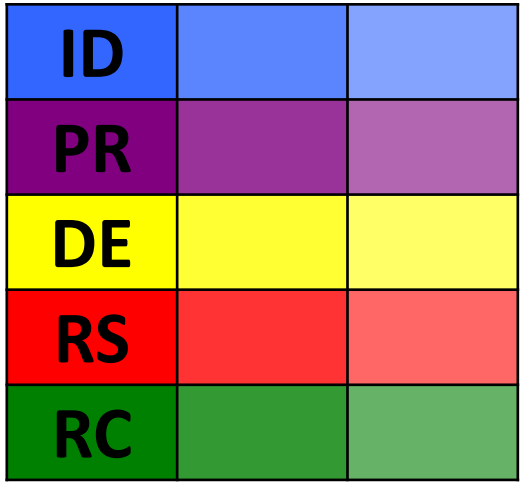
A Common Language

Foundational for Integrated Teams

Senior Executives



IT, OT, Contracts, Marketing, Business Professionals

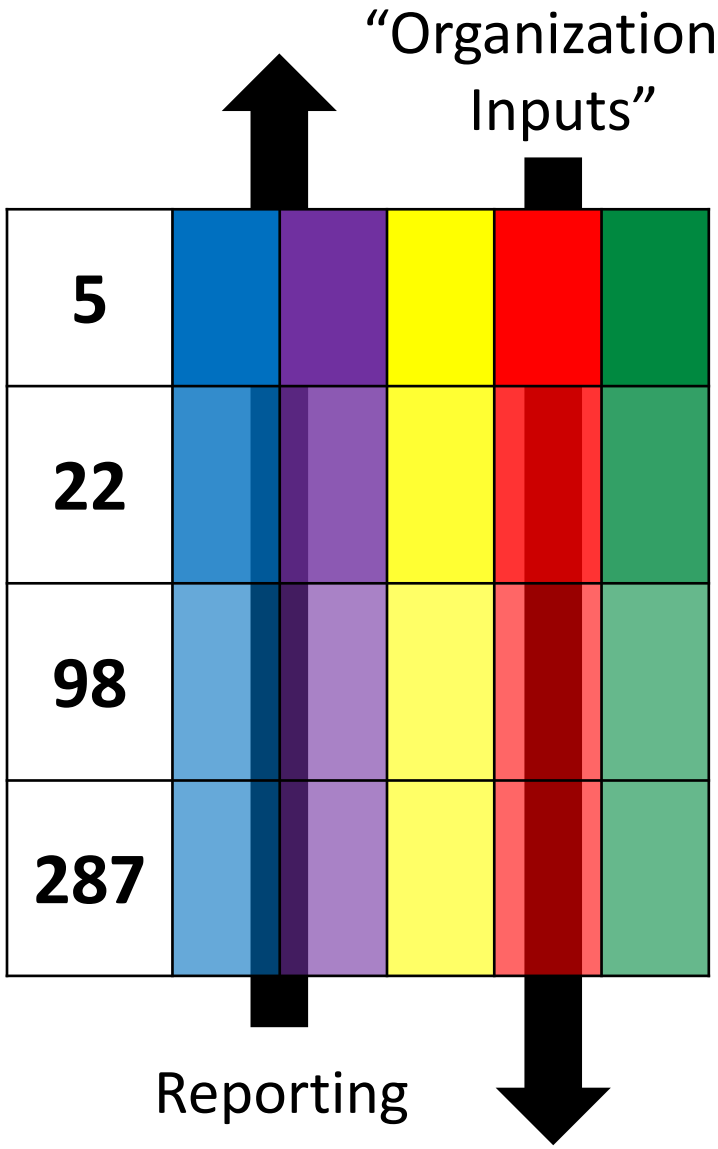


Cybersecurity Professionals

Highly technical and specialized language

Core for Greater Cybersecurity Participation

A Catalog of Cybersecurity Outcomes



Functions

Categories

Subcategories

Informative References

Profile

Customizing Cybersecurity Framework

Ways to think about a Profile:

- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity risk management

Cybersecurity Program Objectives

Three Things All Cybersecurity Programs Must Do

- Support Mission/Business Objectives
- Fulfill Cybersecurity Requirements
- Manage Vulnerability and Threat Associated with the Technical Environment

Cybersecurity Program Objectives

Three Things All Cybersecurity Programs Must Do

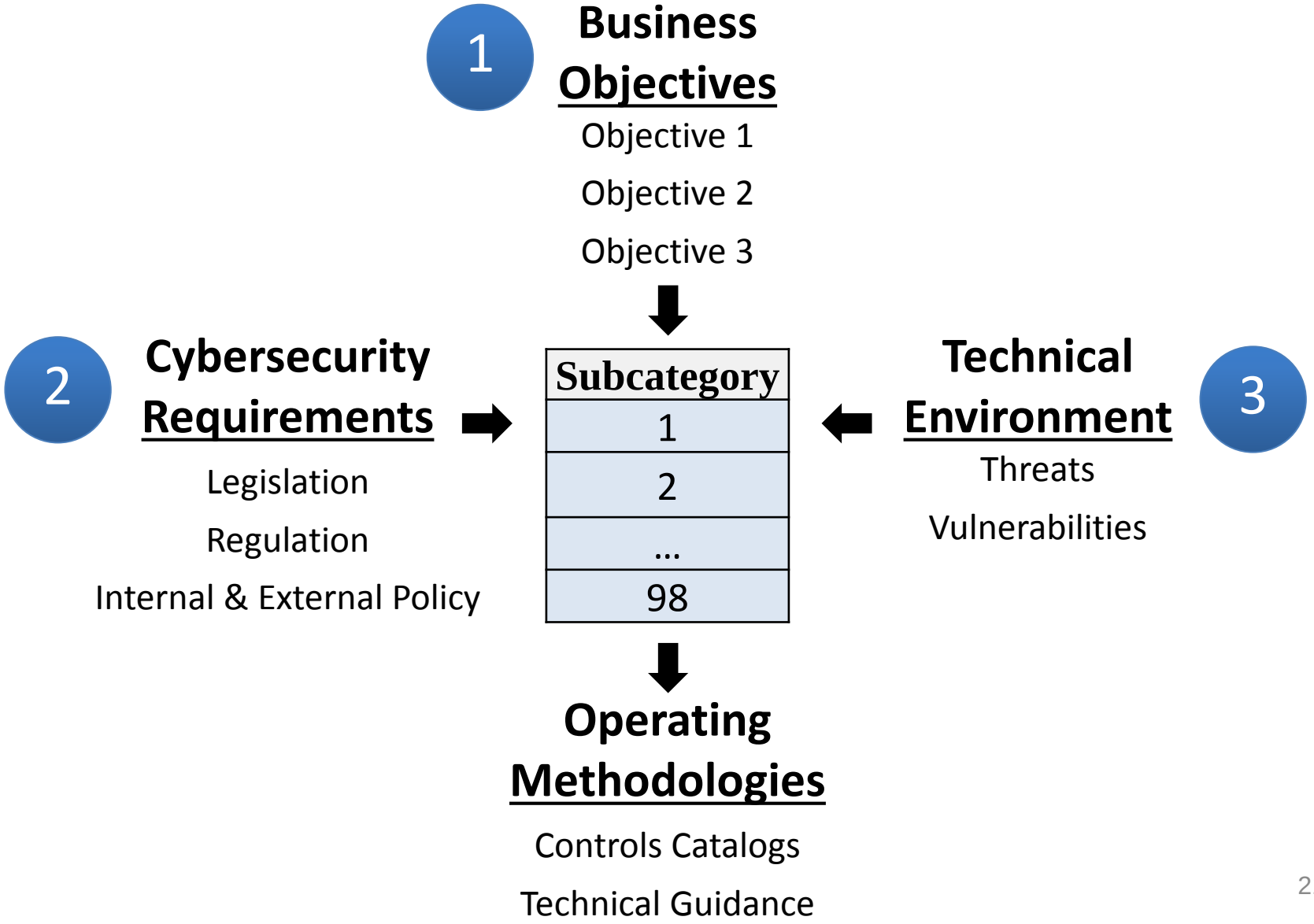
- Support Mission/Business Objectives
- Fulfill Cybersecurity Requirements
- Manage Vulnerability and Threat Associated with the Technical Environment

…accomplished through the processes of:

- Dependency Analysis
- Requirements/Compliance Management
- Threat and Vulnerability Management

Profile Foundational Information

A Profile Can be Created from Three Types of Information



Framework Seven Step Process

Gap Analysis Using Framework Profiles

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a **Target Profile**
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implementation Action Plan

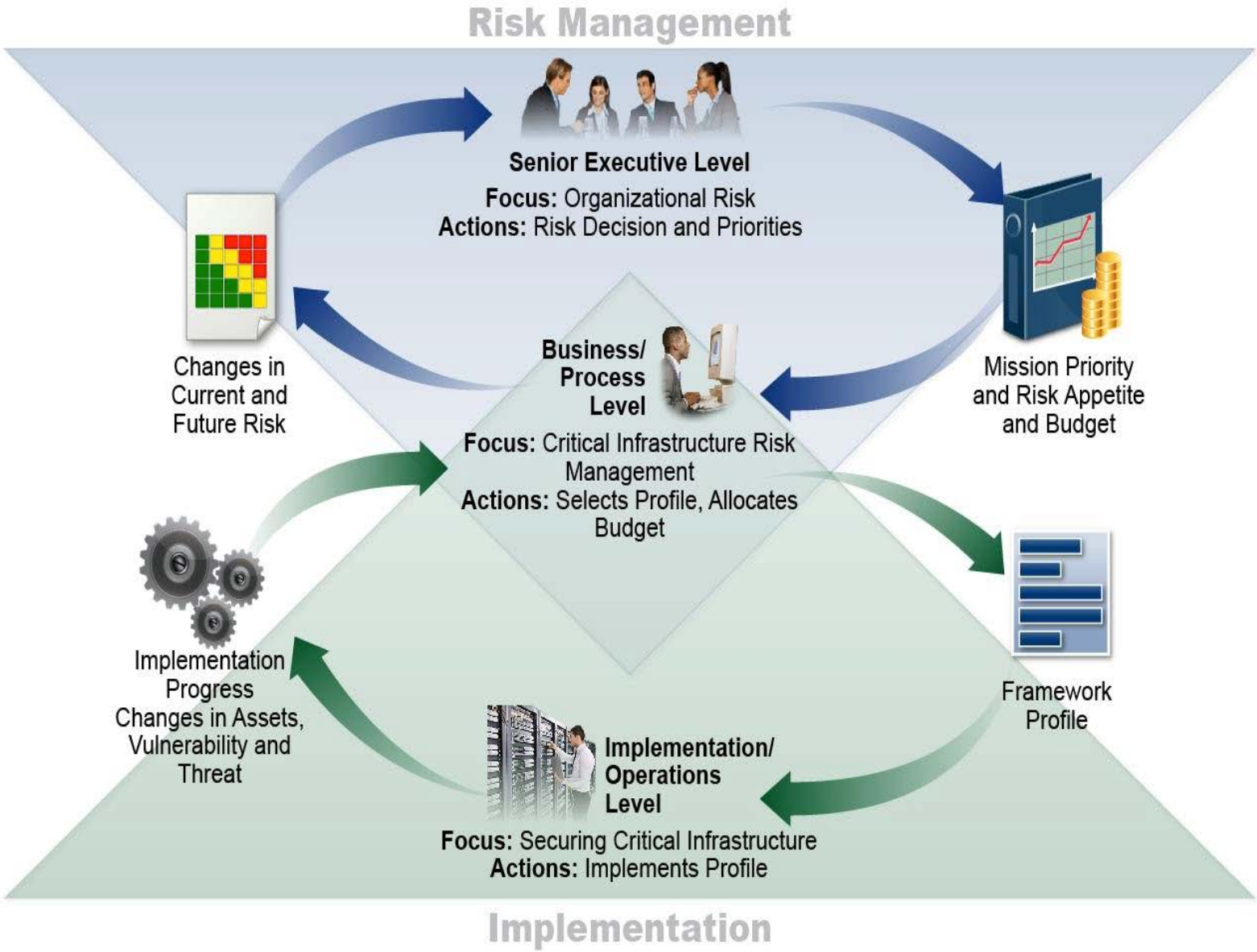
Resource and Budget Decisioning

What Can You Do with a CSF Profile

Sub-category	Priority	Gaps	Budget	Year 1 Activities	Year 2 Activities
1	moderate	small	$$$		X
2	high	large	$$	X	
3	moderate	medium	$	X	
…	…	…	…		
98	moderate	none	$$		reassess

Framework supports operating decisions and improvement

Supporting Risk Management with Framework



Operate

Use Cybersecurity Framework Profiles to distribute and organize labor

Subcats	Reqs	Priorities	Who	What	When	Where	How
1	A, B	High					
2	C, D, E, F	High					
3	G, H, I, J	Low					
…	…	…					
98	XX, YY, ZZ	Mod					
	Reqs	Priorities					

Common Patterns of Use

- Integrate the **Functions** into Your Leadership Vocabulary and Management Tool Sets
- Determine Optimal and Measure Current Risk Management Using **Implementation Tiers**
- Reflect on Business Environment, Governance, and Risk Management Strategy **Categories**
- Develop a Profile of Cybersecurity Priorities, Leveraging (Sub)Sector **Profiles** When Available

Small Business Use

If your organization has a cybersecurity risk executive:

- Integrate the **Functions** into Your Leadership Vocabulary and Management Tool Sets
- Determine Optimal and Measure Current Risk Management Using **Implementation Tiers**
- Reflect on Business Environment, Governance, and Risk Management Strategy **Categories**
- Develop a Profile of Cybersecurity Priorities, Leveraging (Sub)Sector **Profiles** When Available

If your organization does not have a cybersecurity risk executive, but does have technologist(s):

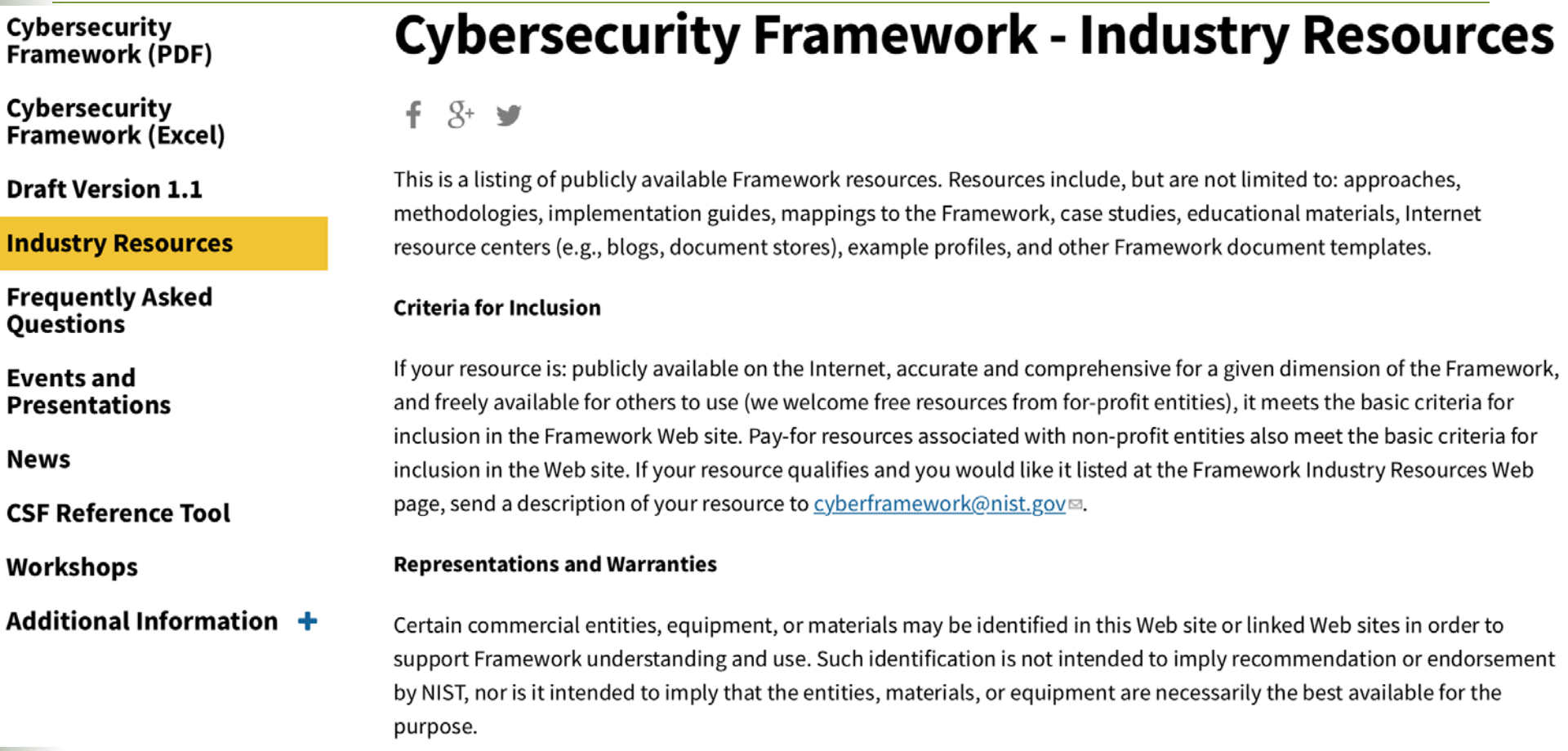
- Consider the recommendations in ***Small Business Information Security: The Fundamentals*** (NIST Interagency Report 7621 revision 1)

If your organization does not have those people:

- Use the ***National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*** (NIST Special Publication 800-181) to determine relevant knowledge, skills, and abilities for a consultant or employee

Industry Resources

www.nist.gov/cyberframework/industry-resources



Cybersecurity Framework (PDF)

Cybersecurity Framework (Excel)

Draft Version 1.1

Industry Resources

Frequently Asked Questions

Events and Presentations

News

CSF Reference Tool

Workshops

Additional Information +

Cybersecurity Framework - Industry Resources

This is a listing of publicly available Framework resources. Resources include, but are not limited to: approaches, methodologies, implementation guides, mappings to the Framework, case studies, educational materials, Internet resource centers (e.g., blogs, document stores), example profiles, and other Framework document templates.

Criteria for Inclusion

If your resource is: publicly available on the Internet, accurate and comprehensive for a given dimension of the Framework, and freely available for others to use (we welcome free resources from for-profit entities), it meets the basic criteria for inclusion in the Framework Web site. Pay-for resources associated with non-profit entities also meet the basic criteria for inclusion in the Web site. If your resource qualifies and you would like it listed at the Framework Industry Resources Web page, send a description of your resource to cyberframework@nist.gov.

Representations and Warranties

Certain commercial entities, equipment, or materials may be identified in this Web site or linked Web sites in order to support Framework understanding and use. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Over 70 Unique Resources for Your Understanding and Use!

Examples of Framework Industry Resources

www.nist.gov/cyberframework/industry-resources

Italy's National Framework for Cybersecurity

American Water Works Association's *Process Control System Security Guidance for the Water Sector*

The Cybersecurity Framework in Action: An Intel Use Case

Cybersecurity Risk Management and Best Practices Working Group 4: Final Report

Financial Services Sector Specific Cybersecurity "Profile"

Examples of U.S. State & Local Use

www.nist.gov/cyberframework/industry-resources

Texas, Department of Information Resources

- Aligned Agency Security Plans with Framework
- Aligned Product and Service Vendor Requirements with Framework

North Dakota, Information Technology Department

- Allocated Roles & Responsibilities using Framework
- Adopted the Framework into their Security Operation Strategy

Houston, Greater Houston Partnership

- Integrated Framework into their Cybersecurity Guide
- Offer On-Line Framework Self-Assessment

National Association of State CIOs

- 2 out of 3 CIOs from the 2015 NASCIO Awards cited Framework as a part of their award-winning strategy

New Jersey

- Developed a cybersecurity framework that aligns controls and procedures with Framework

Recent NIST Work Products

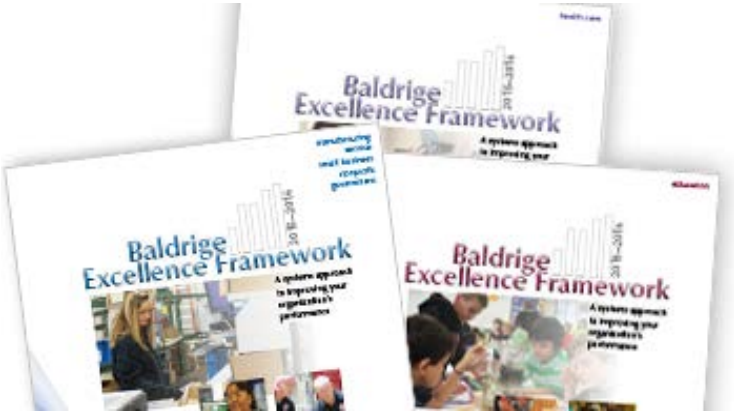
www.nist.gov/cyberframework/industry-resources

Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Self-Assessment Criteria

Baldrige Cybersecurity Excellence Builder



Maritime Profile

U.S. Coast Guard Bulk Liquid Transport Profile

Roadmap Concepts

Roadmap to Improving Critical Infrastructure Cybersecurity

The Roadmap:

- identifies key areas of development, alignment, and collaboration
- provides a description of activities related to the Framework

Roadmap items are generally:

- Topics that are meaningful to critical infrastructure cybersecurity risk management
- Focus areas of both private sector and the federal government
- Related to Framework, but managed as separate efforts

Work in Progress: Framework Roadmap

Authentication

Automated Indicator Sharing

Conformity Assessment

Cybersecurity Workforce

Data Analytics

Federal Agency Cybersecurity Alignment

International Aspects, Impacts, and Alignment

Supply Chain Risk Management

Technical Privacy Standards

Cybersecurity Executive Order 13800

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Risk Management:

(ii) "…agency head **shall use** The Framework" and

"…provide a risk management report within 90 days containing a description of the "…agency's **action plan to implement the Framework**."

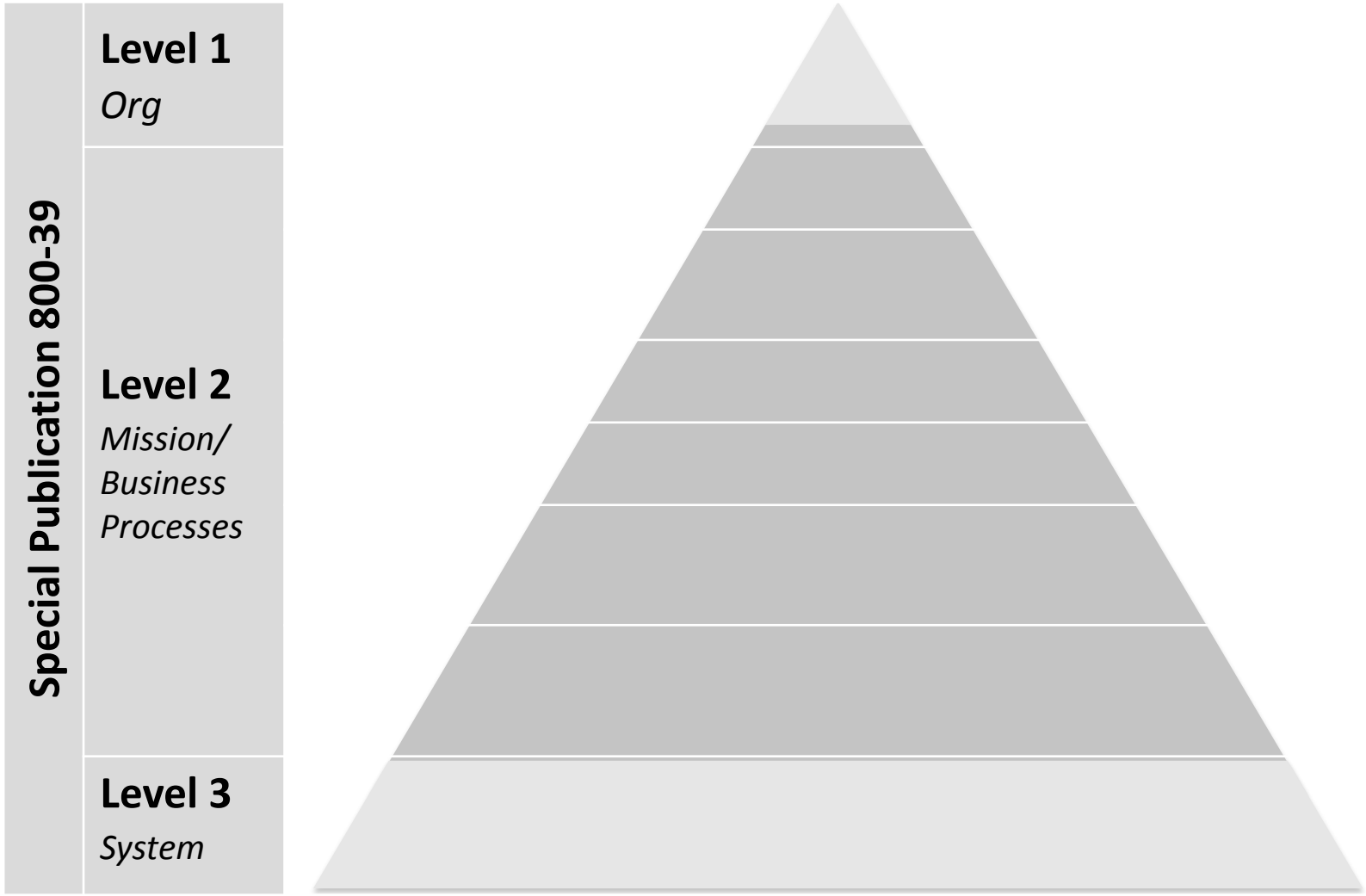
Proposed U.S. Federal Usage

NIST IR 8170 The Cybersecurity Framework: Implementation Guidance for Federal Agencies

1. **Integrate enterprise and cybersecurity risk management**
2. **Manage cybersecurity requirements**
3. **Integrate and align cybersecurity and acquisition processes**
4. **Evaluate organizational cybersecurity**
5. **Manage the cybersecurity program**
6. **Maintain a comprehensive understanding of cybersecurity risk** *(supports RMF Authorize)*
7. **Report cybersecurity risks** *(supports RMF Monitor)*
8. **Inform the tailoring process** *(supports RMF Select)*

Proposed Federal Usage

NIST IR 8170 The Cybersecurity Framework: Implementation Guidance for Federal Agencies



Proposed Federal Usage

[NIST IR 8170 The Cybersecurity Framework: Implementation Guidance for Federal Agencies]

Special Publication 800-39

Level 1
Org

Level 2
Mission/ Business Processes

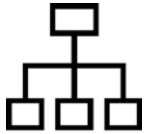
Level 3
System

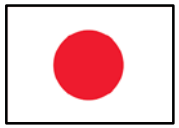
Framework Roadmap Items

- Authentication
- Automated Indicator Sharing
- Conformity Assessment
- Cybersecurity Workforce
- Data Analytics
- Federal Agency Cybersecurity Alignment
- International Aspects, Impacts, and Alignment
- Supply Chain Risk Management
- Technical Privacy Standards

Cybersecurity Framework Use

- Used by over 30% of U.S. organizations, trending to 50% (Gartner, 2015, https://www.gartner.com/webinar/3163821)
- Required within the United States federal government
- Japanese translation by Information-technology Promotion Agency
- Italian translation and adaptation within Italy's National Framework for Cybersecurity
- Hebrew translation and adaptation by Government of Israel
- Bermuda uses it within government and recommends it to industry
- Focus of International Organization for Standardization & International Electrotechnical Commission






Ways to Help

Stakeholder Recommended Actions

Stakeholders should consider activities to:

- Customize Framework for your sector or community
- Publish a sector or community Profile or relevant "crosswalk"
- Advocate for the Framework throughout your sector or community, with related sectors and communities.
- Publish "summaries of use" or case studies of your Framework implementation.
- Submit a paper during the NIST call for abstracts
- Share your Framework resources with NIST at cyberframework@nist.gov.

Resources

Where to Learn More and Stay Current

Framework for Improving Critical Infrastructure Cybersecurity and related news and information:
www.nist.gov/cyberframework

Additional cybersecurity resources:
http://csrc.nist.gov/

Questions, comments, ideas:
cyberframework@nist.gov