The Framework for Improving Critical Infrastructure Cybersecurity

May 2018

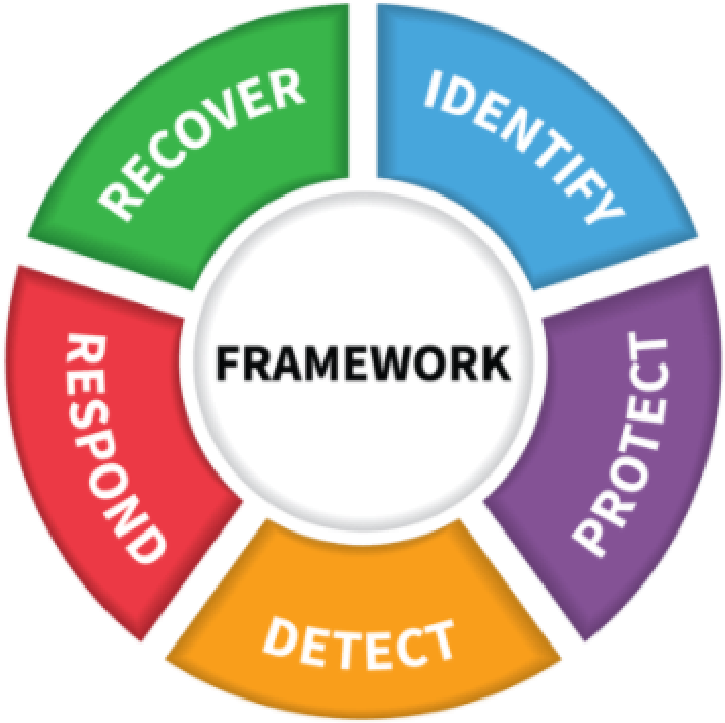
cyberframework@nist.gov

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

Objective and Agenda

Objective: Convey Cybersecurity Framework v1.1, relevant CSF happenings, and status of NISTIR 8170

- Charter
- Attributes & Components
- NISTIR 8170
- Web Site
- Upcoming events
- Informative References



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)

Version 1.0 and 1.1 Are Fully Compatible

Framework for Improving Critical Infrastructure Cybersecurity

- Additions, including new categories and subcategories, do not invalidate existing V1.0 uses or work products

Component	Version 1.0	Version 1.1	Comments
Functions	5	5	
Categories	22	23	• Added a new category in ID.SC – Supply Chain
Subcategories	98	108	• Added 5 subcategories in ID.SC • Added 2 subcategories in PR.AC • Added 1 subcategory each to PR.DS, PR.PT, RS.AN • Clarified language in 7 others
Informative References	5	5	

Key Framework Attributes

Principles of the Current and Future Versions of Framework

Common and accessible language

- Understandable by many professionals

It’s adaptable to many **technologies**$^{1.1}$, **lifecycle phases**$^{1.1}$, sectors and uses

- Meant to be *customized*

It’s risk-based

- A Catalog of cybersecurity outcomes
- Does not provide *how or how much* cybersecurity is appropriate

It’s meant to be paired

- Take advantage of great pre-existing things

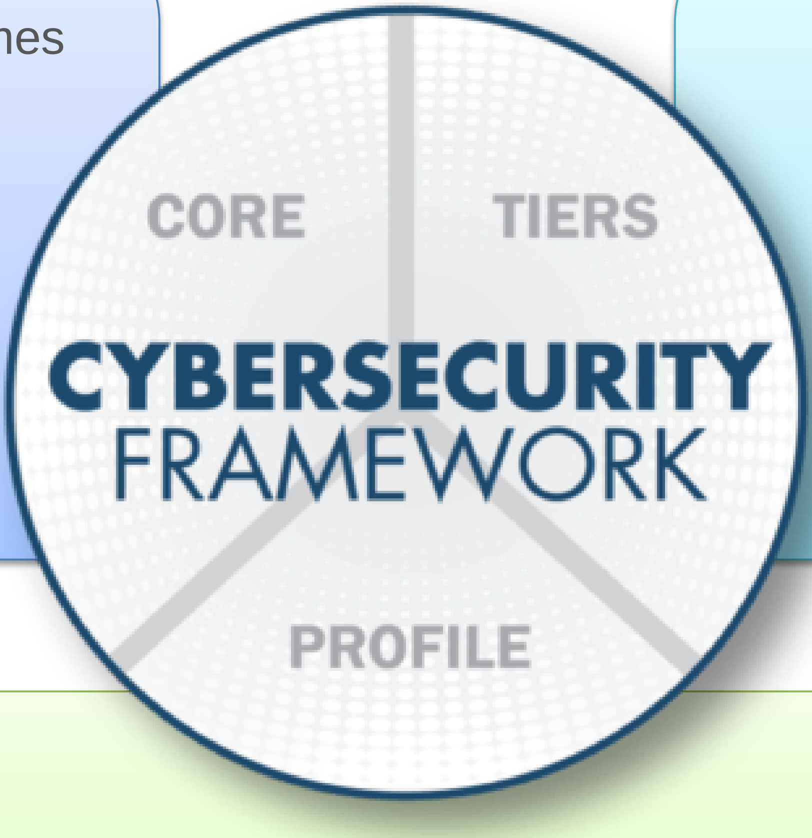
It’s a living document

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

Cybersecurity Framework Components

Cybersecurity outcomes and informative references

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

Aligns industry standards and best practices to the Framework Core in an implementation scenario
Supports prioritization and measurement while factoring in business needs

Implementation Tiers

	1 Partial	2 Risk Informed	3 Repeatable	4 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: • **monitors and manages supply chain risk**[1.1] • benefits my sharing or receiving information from outside parties			

Core

A Catalog of Cybersecurity Outcomes

	Function
What processes and assets need protection?	**Identify**
What safeguards are available?	**Protect**
What techniques can identify incidents?	**Detect**
What techniques can contain impacts of incidents?	**Respond**
What techniques can restore capabilities?	**Recover**

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

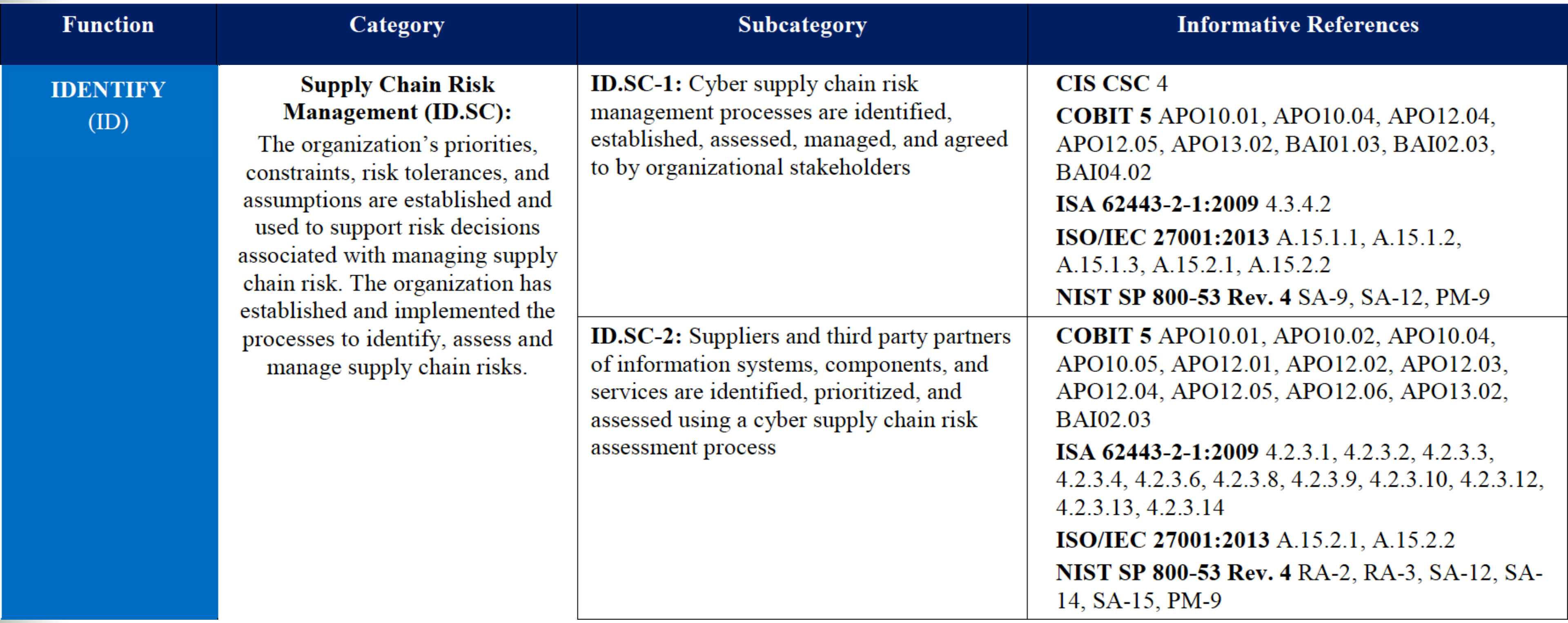
Core

A Catalog of Cybersecurity Outcomes

	Function	Category
What processes and assets need protection?	**Identify**	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management$^{1.1}$
What safeguards are available?	**Protect**	**Identity Management, Authentication and Access Control$^{1.1}$**
		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$^{1.1}$

Cybersecurity Framework Component



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

Profile

Customizing Cybersecurity Framework

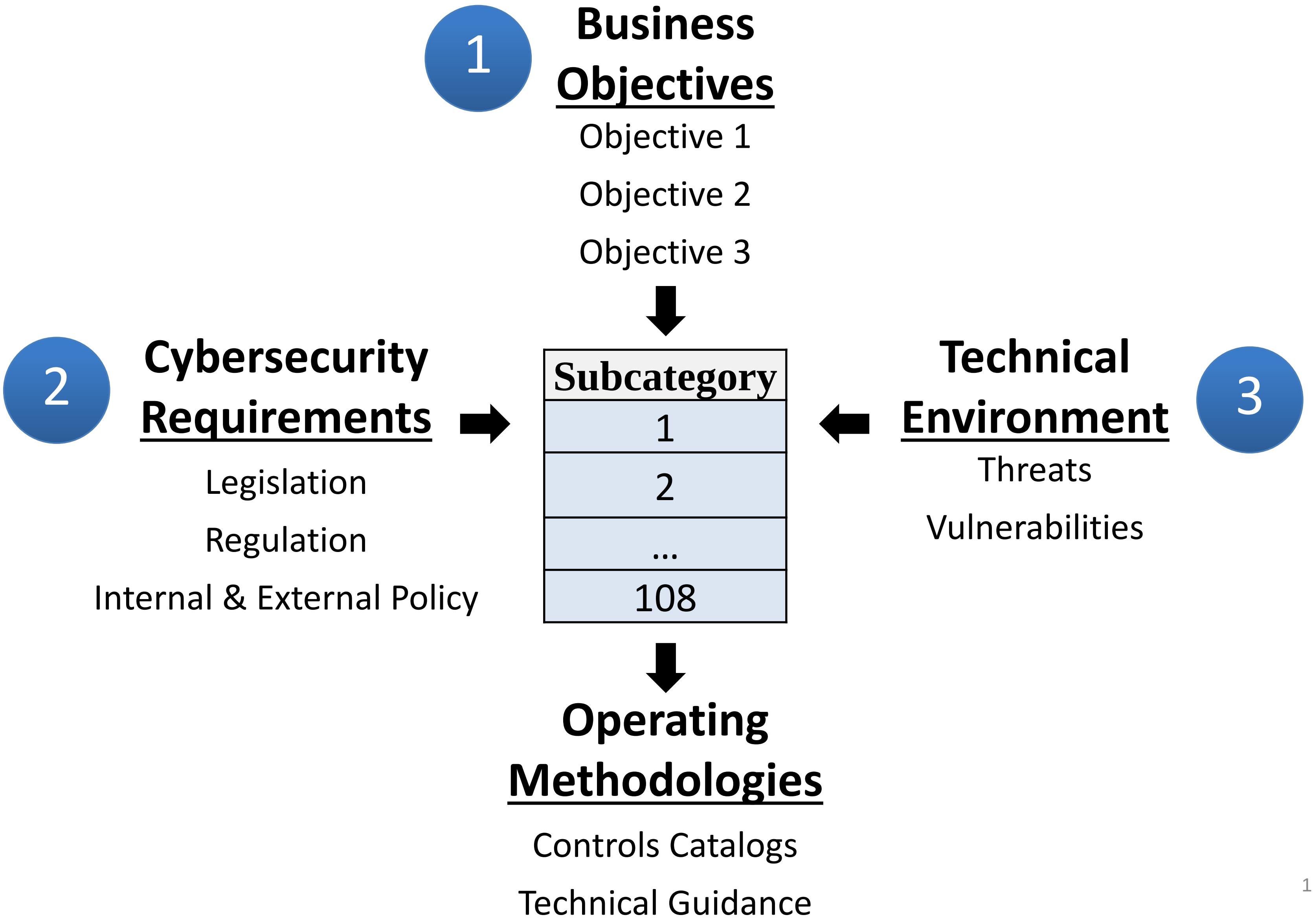
Ways to think about a Profile:

- 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

Identify
Protect
Detect
Respond
Recover

Profile Foundational Information

A Profile Can be Created from Three Types of Information



1 **Business Objectives**

Objective 1

Objective 2

Objective 3

2 **Cybersecurity Requirements**

Legislation

Regulation

Internal & External Policy

Subcategory
1
2
…
108

3 **Technical Environment**

Threats

Vulnerabilities

Operating Methodologies

Controls Catalogs

Technical Guidance

Framework Seven Step Process

Gap Analysis Using Framework Profiles

- **Step 1:** Prioritize and Scope
  - Implementation Tiers may be used to express varying risk tolerances[1.1]
- **Step 2:** Orient
- **Step 3:** Create a Current Profile
- **Step 4:** Conduct a Risk Assessment
- **Step 5:** Create a Target Profile
  - When used in conjunction with an Implementation Tier, characteristics of the Tier level should be reflected in the desired cybersecurity outcomes[1.1]
- **Step 6:** Determine, Analyze, and Prioritize Gaps
- **Step 7:** Implementation Action Plan

Resource and Budget Decisioning

Framework supports operating decisions and improvement

As-Is

Year 1 To-Be

Year 2 To-Be

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

Resource and Budget Decisioning

Framework supports operating decisions and improvement

As-Is

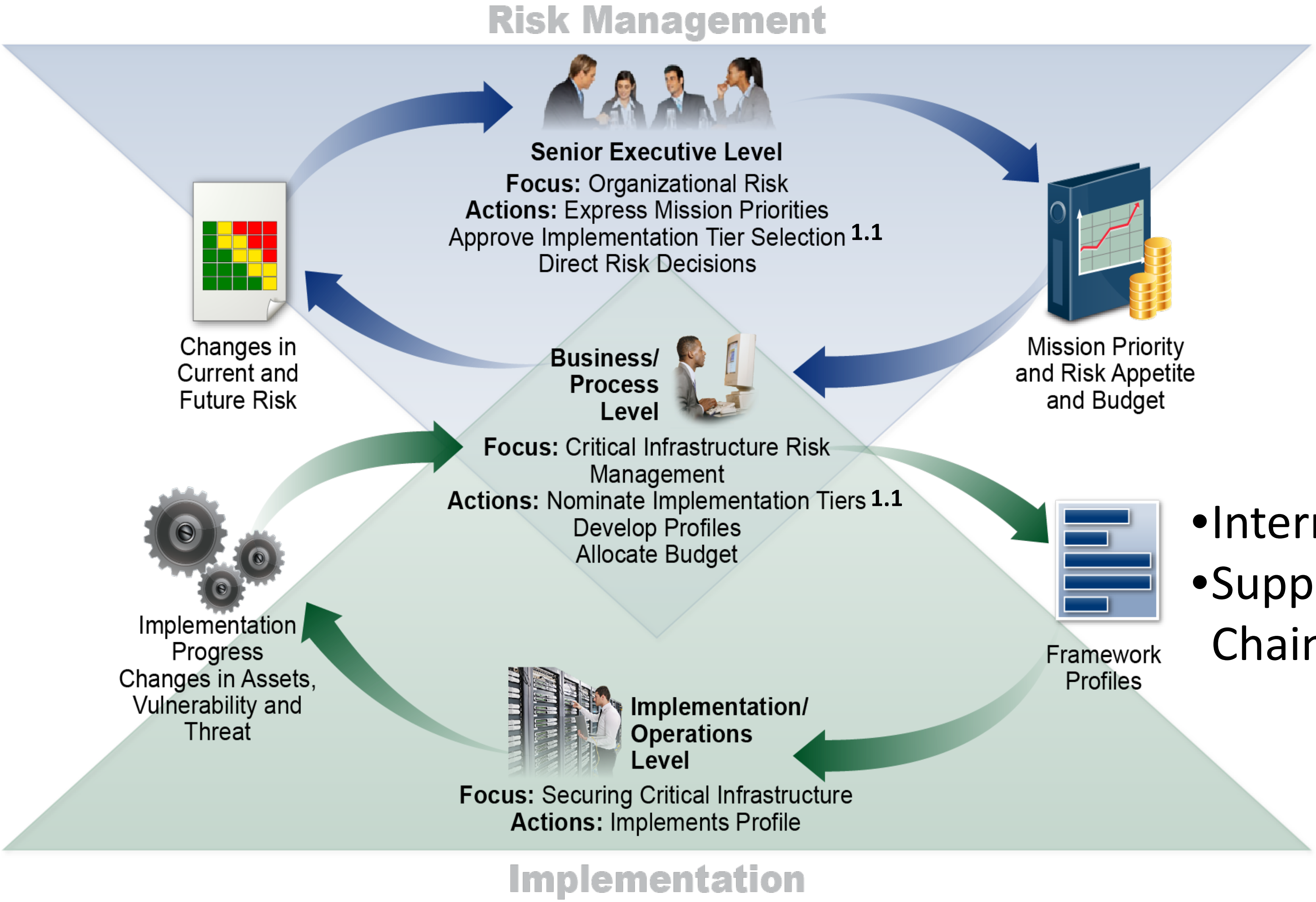
Year 1
To-Be

Year 2
To-Be

Sub-category	Priority	Gaps	Budget	Year 1 Activities	Year 2 Activities
1	moderate	small	$$$		X
2	high	large	$$	X	
3	moderate	medium	$	X	
…	…	…	…		
108	moderate	none	$$		reassess
Step 5 **Target Profile**		**Step 6**		**Step 7**	

Supporting Risk Management with Framework

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1



Senior Executive Level

Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection **1.1**
Direct Risk Decisions

Mission Priority and Risk Appetite and Budget

Changes in Current and Future Risk

Business/ Process Level

Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers **1.1**
Develop Profiles
Allocate Budget

Framework Profiles

Implementation Progress
Changes in Assets, Vulnerability and Threat

Implementation/ Operations Level

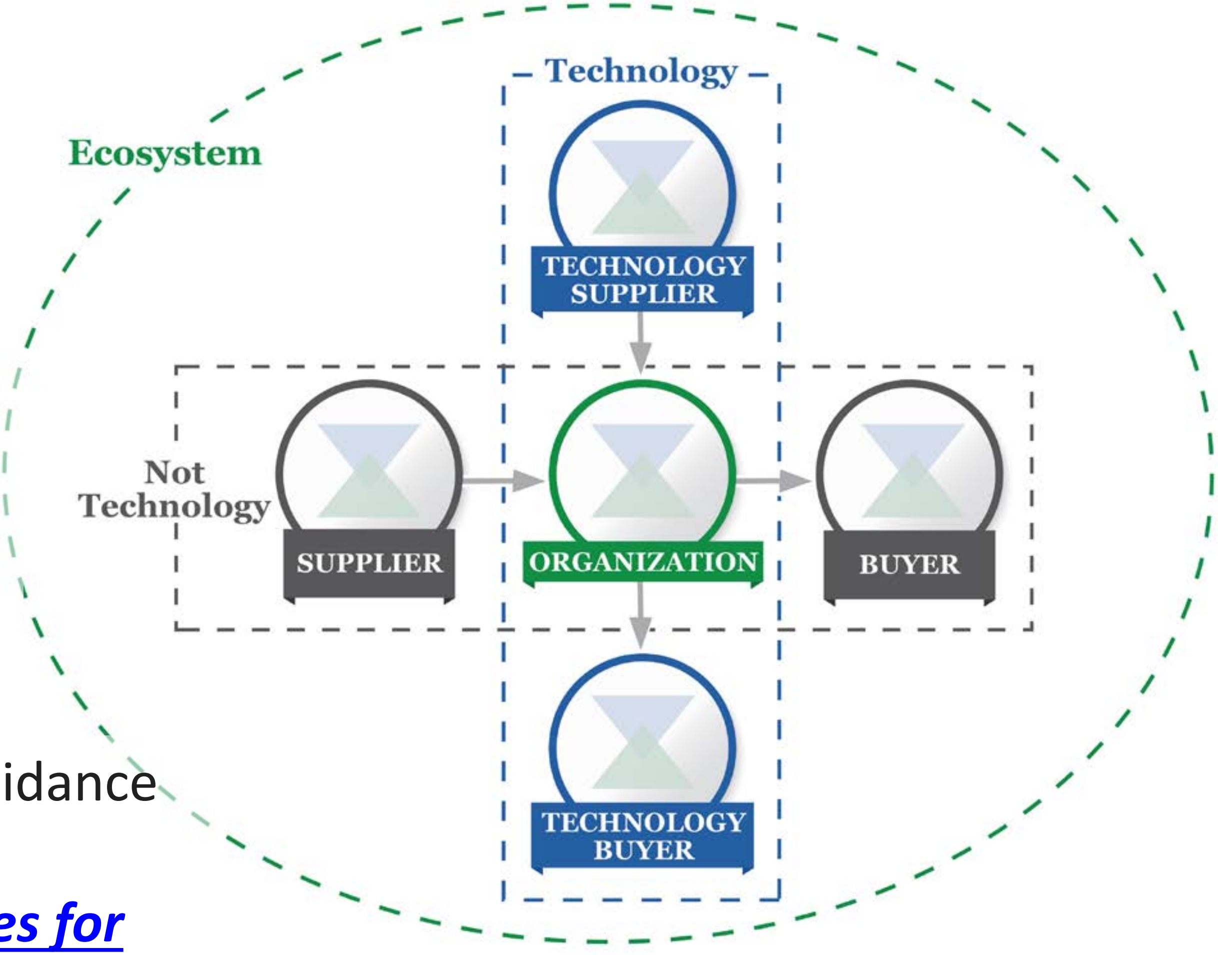
Focus: Securing Critical Infrastructure
Actions: Implements Profile

- Internal
- Supply Chain

Cyber SCRM Taxonomy$^{1.1}$

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

- Simple Supplier-Buyer model
- Technology minimally includes IT, OT, CPS, IoT
- Applicable for public and private sector, including not-for-profits
- Aligns with Federal guidance ***Supply Chain Risk Management Practices for Federal Information Systems and Organizations*** (Special Publication 800-161)



Self-Assessing Cybersecurity Risk$^{1.1}$

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Emphasizes the role of measurements in *self-assessment*

Stresses critical linkage of business results:

- Cost
- Benefit

…to cybersecurity risk management

Continued discussion of this linkage will occur under Roadmap area – Measuring Cybersecurity

Proposed U.S. Federal Usage

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

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
Executive Order 13800

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)*

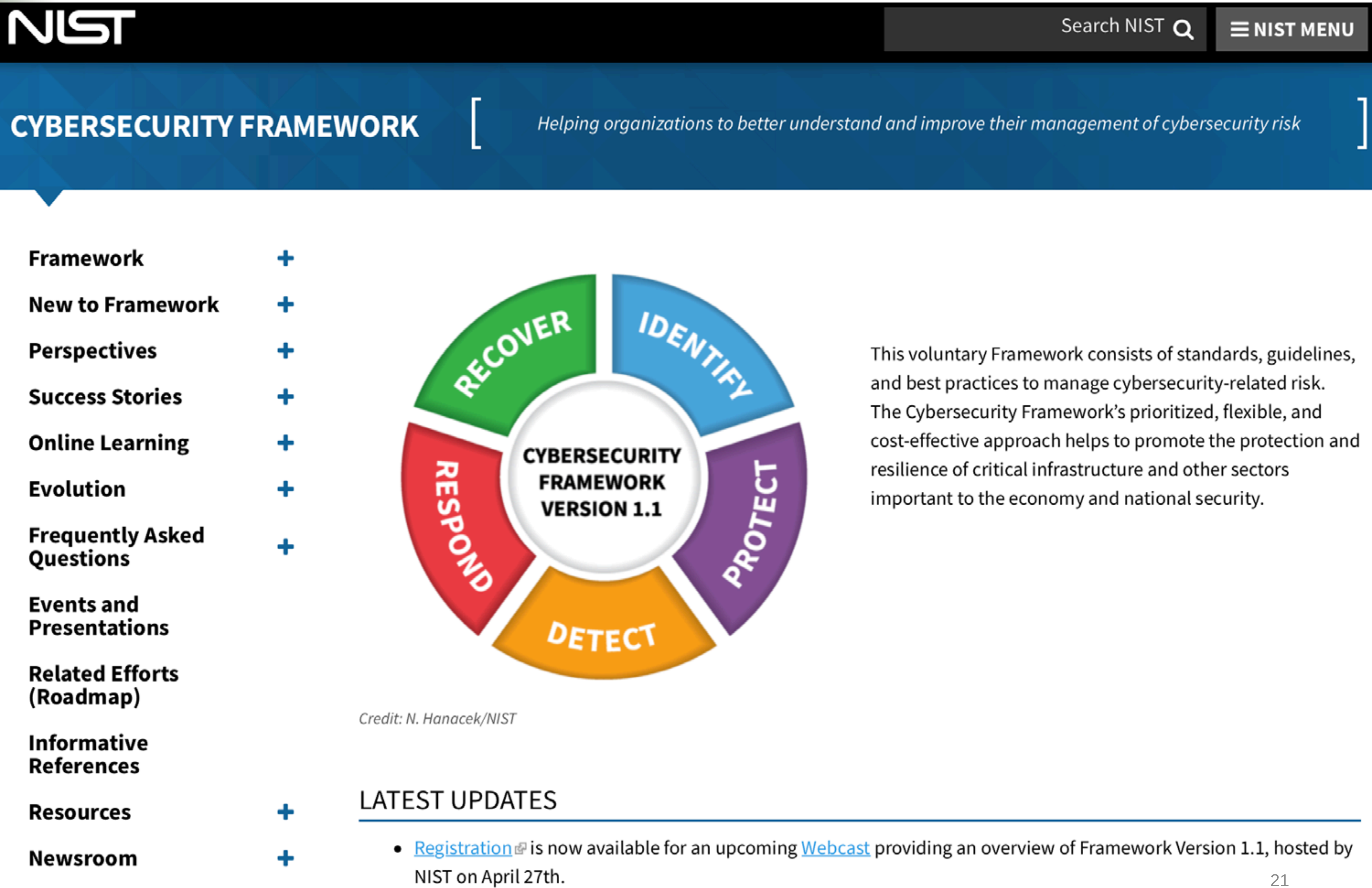
Proposed U.S. Federal Usage

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

Special Publication 800-39	**Level 1** *Org*	**1. Integrate enterprise and cybersecurity risk management**	Core
	Level 2 *Mission/ Business Processes*	**2. Manage cybersecurity requirements**	Profile(s)
		3. Integrate and align cybersecurity and acquisition processes	Profile(s)
		4. Evaluate organizational cybersecurity	Imp. Tiers
		5. Manage the cybersecurity program	Profile(s)
		6. Maintain a comprehensive understanding of cybersecurity risk *supports RMF Authorize*	Core
		7. Report cybersecurity risks *supports RMF Monitor*	Core
	Level 3 *System*	**8. Inform the tailoring process** *supports RMF Select*	Profile(s)

The Framework Web Site

www.nist.gov/cyberframework



CYBERSECURITY FRAMEWORK [*Helping organizations to better understand and improve their management of cybersecurity risk*]

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

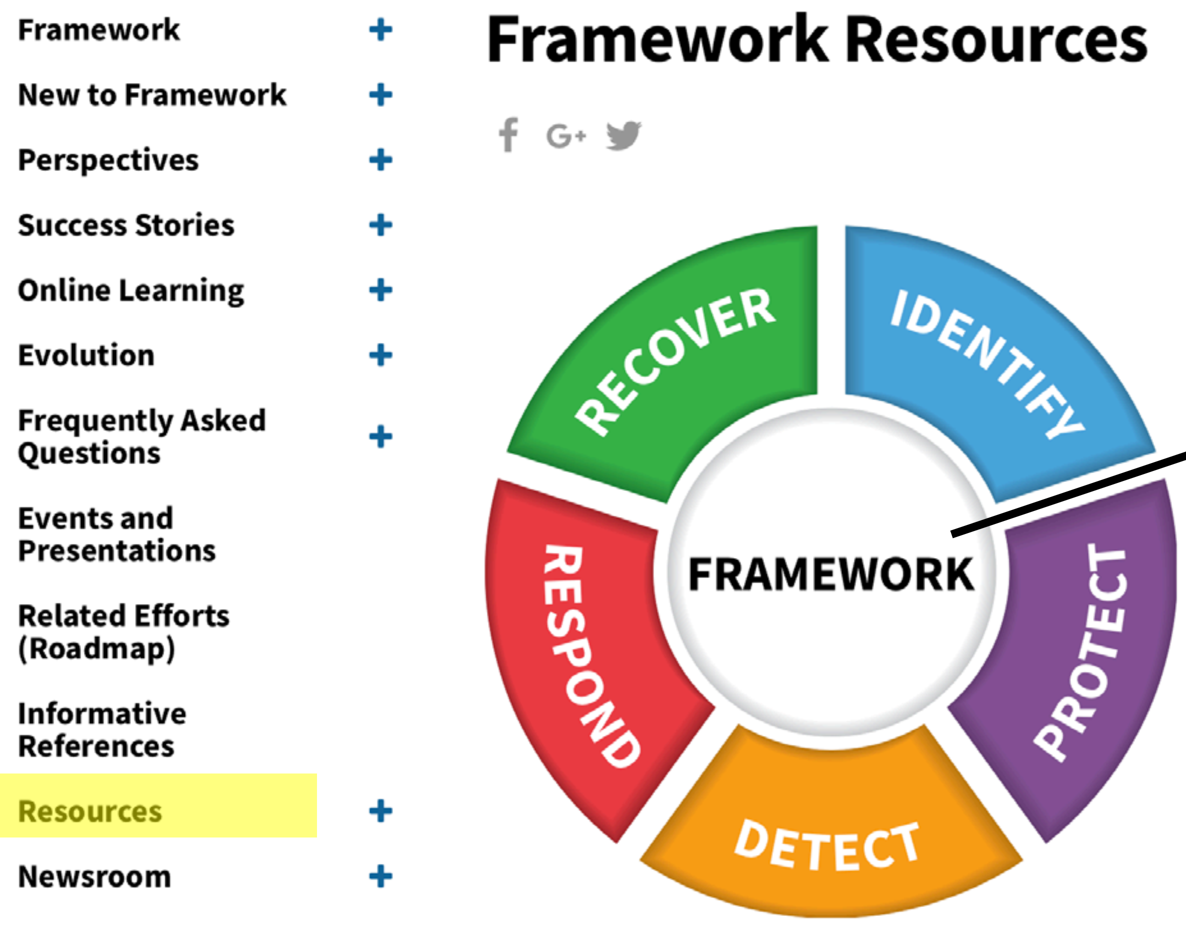
Credit: N. Hanacek/NIST

LATEST UPDATES

- Registration is now available for an upcoming Webcast providing an overview of Framework Version 1.1, hosted by NIST on April 27th.

Resources

https://www.nist.gov/cyberframework/framework-resources-0



Framework Resources

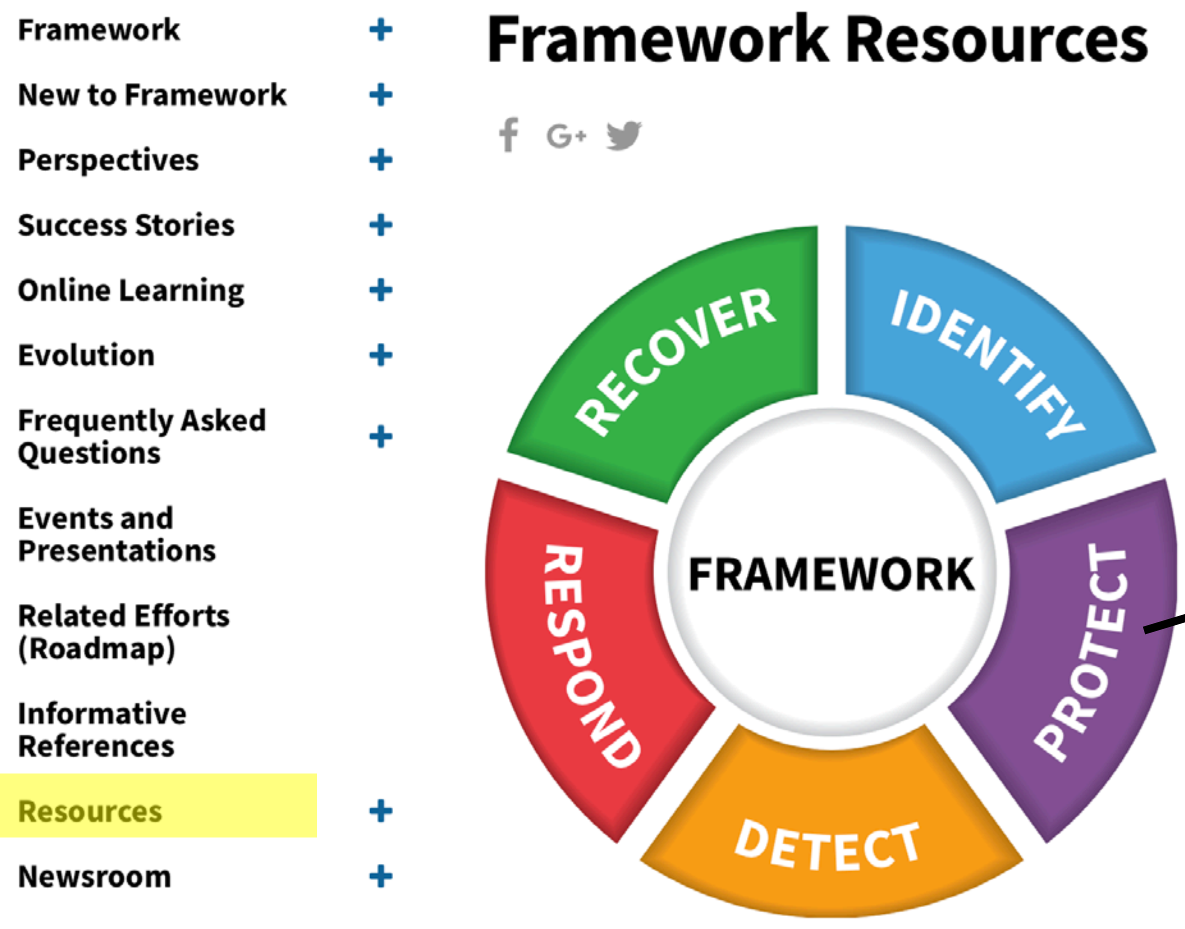
General Resources sorted by User Group:

- Critical Infrastructure
- Small and Medium Business
- International
- Federal
- State Local Tribal Territorial Governments
- Academia
- Assessments & Auditing
- General

Over 150 Unique Resources for Your Understanding and Use!

Resources

https://www.nist.gov/cyberframework/framework-resources-0



Framework Resources

NIST Special Publications

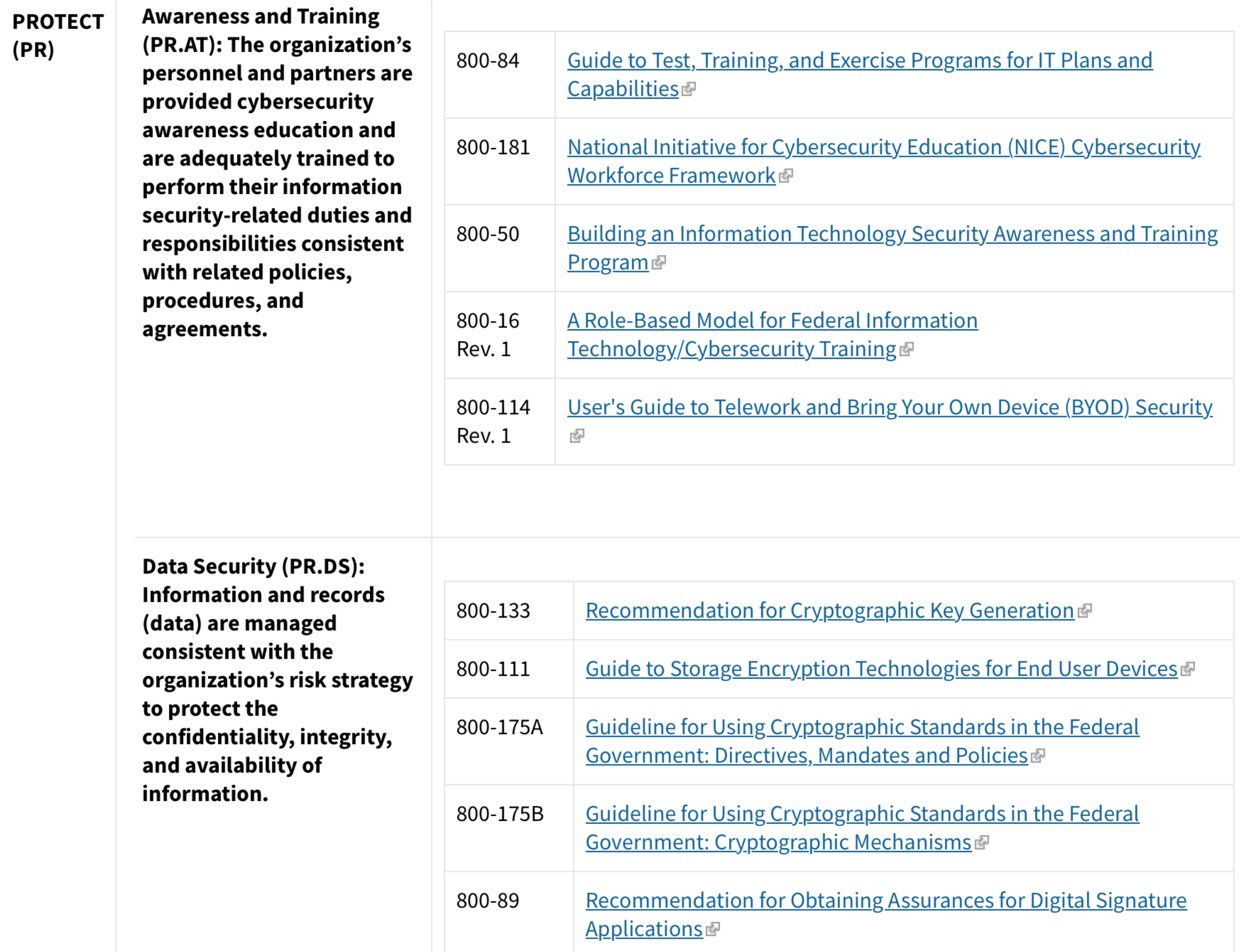
Computer Security
Resource Center
800 Series @ csrc.nist.gov

National Cybersecurity
Center of Excellence
1800 Series @ nccoe.nist.gov

Over 150 Unique Resources for Your Understanding and Use!

NIST Special Publications by Category

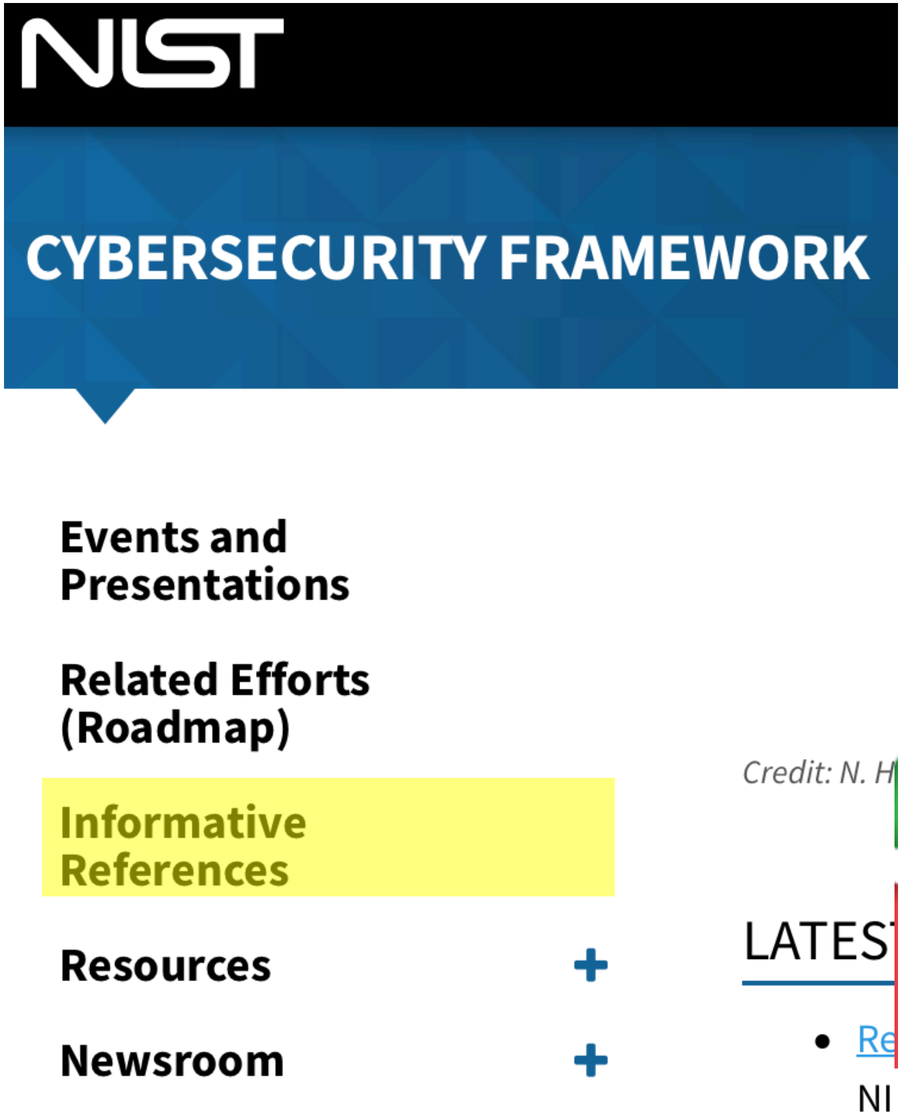
https://www.nist.gov/cyberframework/protect



PROTECT (PR)	**Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.**	800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
		800-181	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
		800-50	Building an Information Technology Security Awareness and Training Program
		800-16 Rev. 1	A Role-Based Model for Federal Information Technology/Cybersecurity Training
		800-114 Rev. 1	User's Guide to Telework and Bring Your Own Device (BYOD) Security
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	800-133	Recommendation for Cryptographic Key Generation
		800-111	Guide to Storage Encryption Technologies for End User Devices
		800-175A	Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies
		800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
		800-89	Recommendation for Obtaining Assurances for Digital Signature Applications

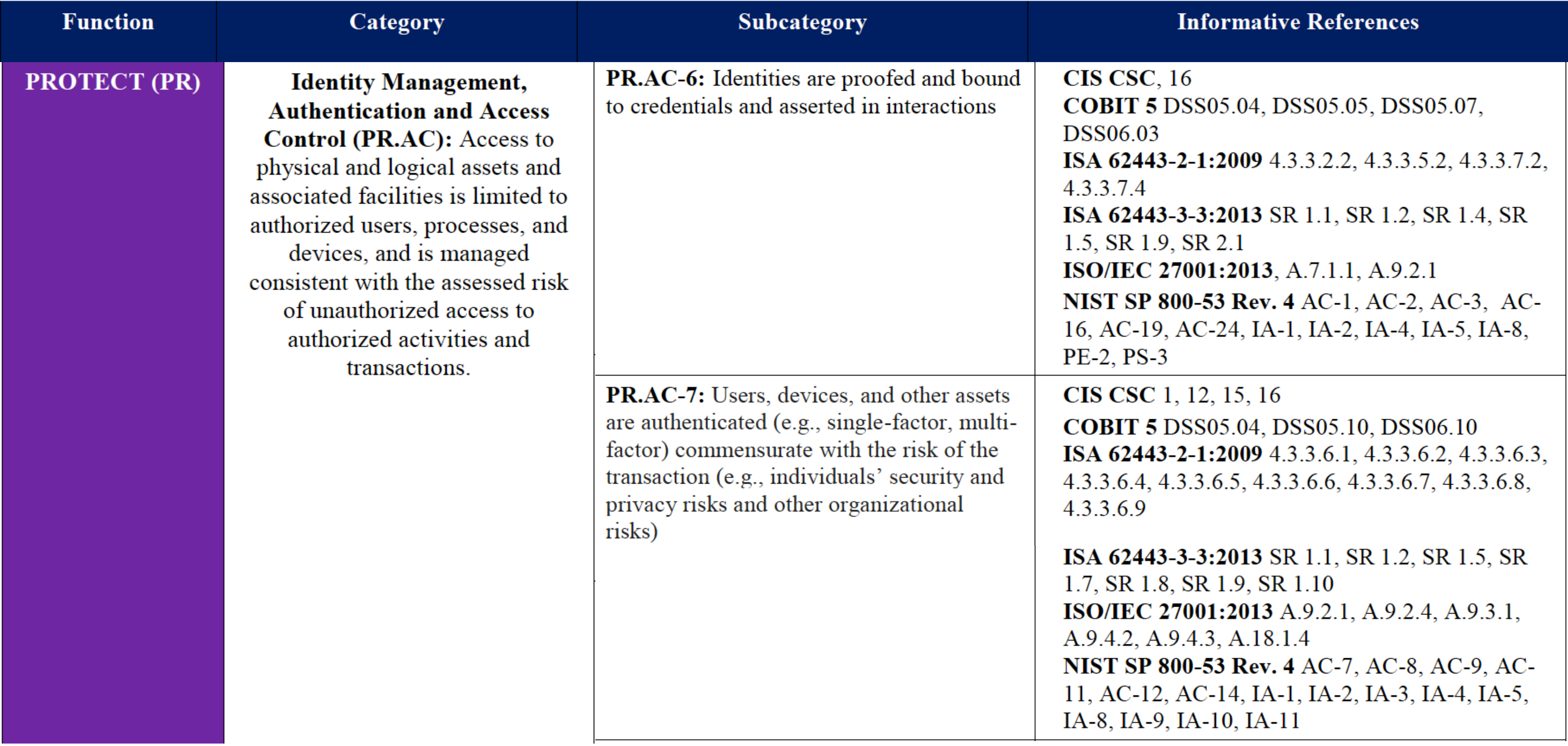
Online Informative References

https://www.nist.gov/cyberframework/informative-references



Core – Example$^{1.1}$

Cybersecurity Framework Component



Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

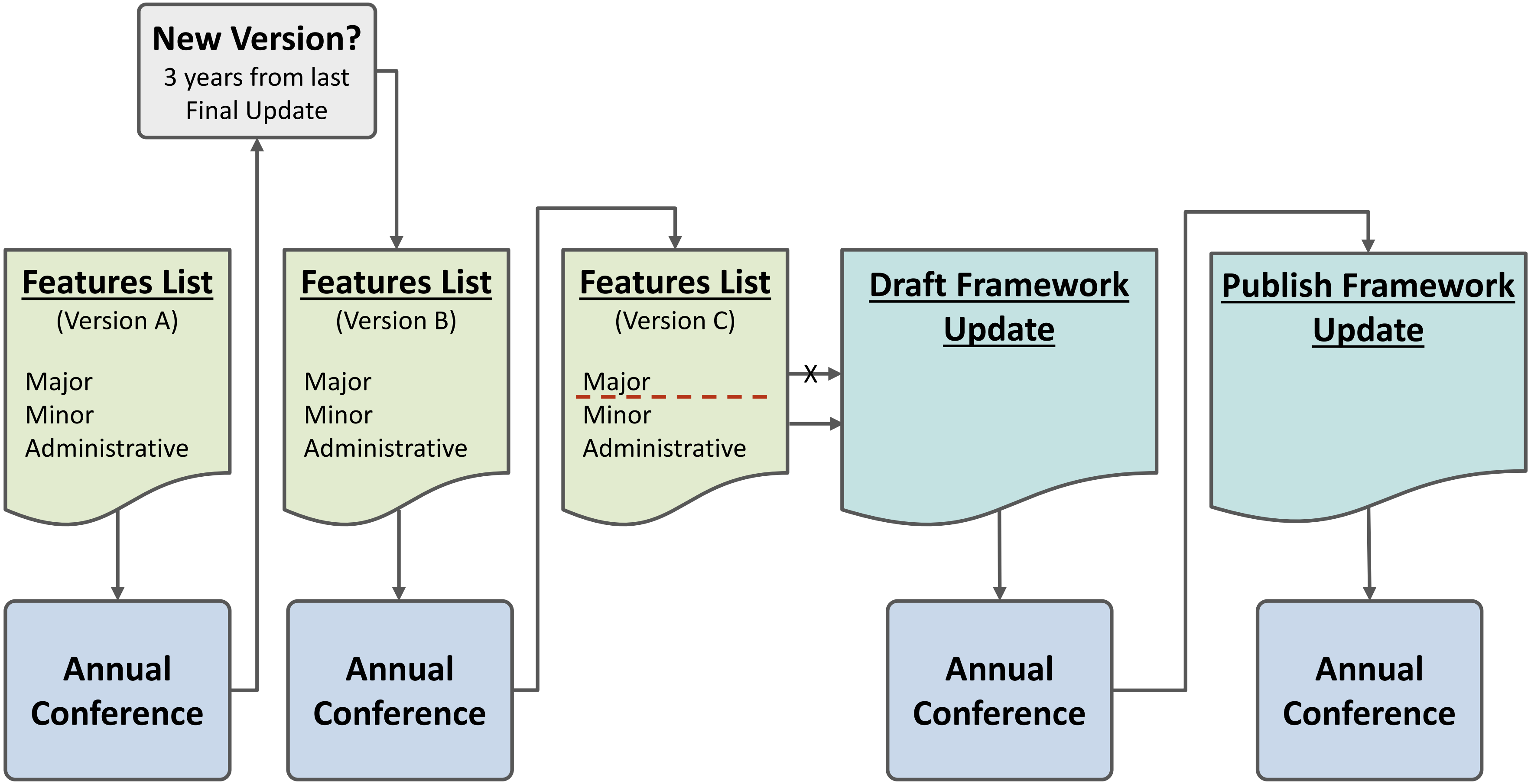
Continued Improvement of Critical Infrastructure Cybersecurity

Update Activities	Engagement
Request for Information – Views on the Framework for Improving Critical Infrastructure Cybersecurity – Dec 2015	105 Responses
7th Workshop – Apr 2016	653 Physical Attendees, 140 Online Attendees
Draft 1 – Framework Version 1.1 – Released Jan 2017	Approx. 42,000+ downloads As of 4/27/18
Request for Comment – Proposed update to the Framework for Improving Critical Infrastructure Cybersecurity – Jan 2017	129 Responses
8th Workshop – May 2017	517 Physical Attendees, 1528 Online Attendees
Draft 2 – Framework Version 1.1 – Released Dec 2017	Approx. 32,000+ downloads As of 4/27/18
Request for Comment – Cybersecurity Framework Version 1.1 – Draft 2 – Dec 2017	89 Responses
Framework Version 1.1 – Release April 2018	Approx. 27,000+ downloads thus far

Milestones

Three Year Minimum Update Cycle

https://www.nist.gov/cyberframework/online-learning/update-process



New Version?

3 years from last Final Update

Features List

(Version A)

Major

Minor

Administrative

Features List

(Version B)

Major

Minor

Administrative

Features List

(Version C)

Major

Minor

Administrative

Draft Framework Update

Publish Framework Update

Annual Conference

Annual Conference

Annual Conference

Annual Conference

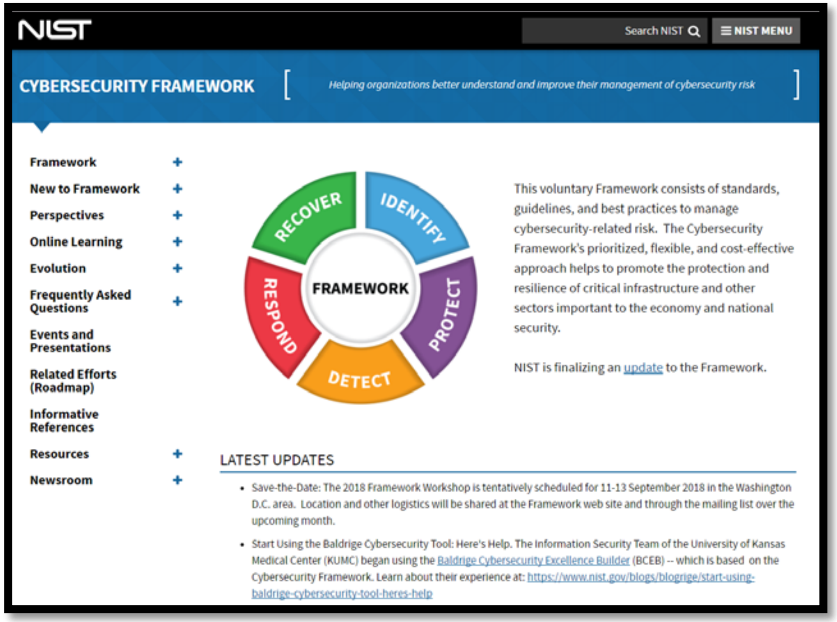
Upcoming

15-16 May 2018	Federal Computer Security Managers Forum https://csrc.nist.gov/Events/2018/Federal-Computer-Security-Managers-Forum-2-day
Spring 2018	Publication of Roadmap for Improving Critical Infrastructure Cybersecurity
Spring 2018	Publication of NIST Interagency Report 8170
Summer 2018	Spanish Language Framework Version 1.1
6-8 November 2018	NIST Cybersecurity Risk Management Conference - Call for Speakers
Winter 2018-19	Small Business Starter Profiles

Resources

- 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



[*Helping organizations better understand and improve their management of cybersecurity risk*]

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

NIST is finalizing an update to the Framework.

LATEST UPDATES

- Save-the-Date: The 2018 Framework Workshop is tentatively scheduled for 11-13 September 2018 in the Washington D.C. area. Location and other logistics will be shared at the Framework web site and through the mailing list over the upcoming month.
- Start Using the Baldrige Cybersecurity Tool: Here's Help. The Information Security Team of the University of Kansas Medical Center (KUMC) began using the Baldrige Cybersecurity Excellence Builder (BCEB) -- which is based on the Cybersecurity Framework. Learn about their experience at: https://www.nist.gov/blogs/blogrige/start-using-baldrige-cybersecurity-tool-heres-help