

Framework for Improving Critical Infrastructure Cybersecurity



Matthew Barrett

NIST Program Manager
Applied Cybersecurity Division
Information Technology Laboratory (ITL)

(presented at NITRD Faster Administration and Technology
Education and Research (FASTER) Community of Practice (CoP)
on March 22, 2018)

cyberframework@nist.gov

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

Agenda

Framework for Improving Critical Infrastructure Cybersecurity

- Charter
- Users
- Component Overview
- Key Attributes
- Proposed Update
- Work Products
- Federal Use
- Online 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”*

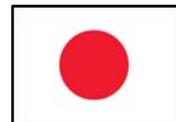
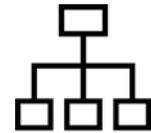


Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

Signs of Use

Framework for Improving Critical Infrastructure Cybersecurity

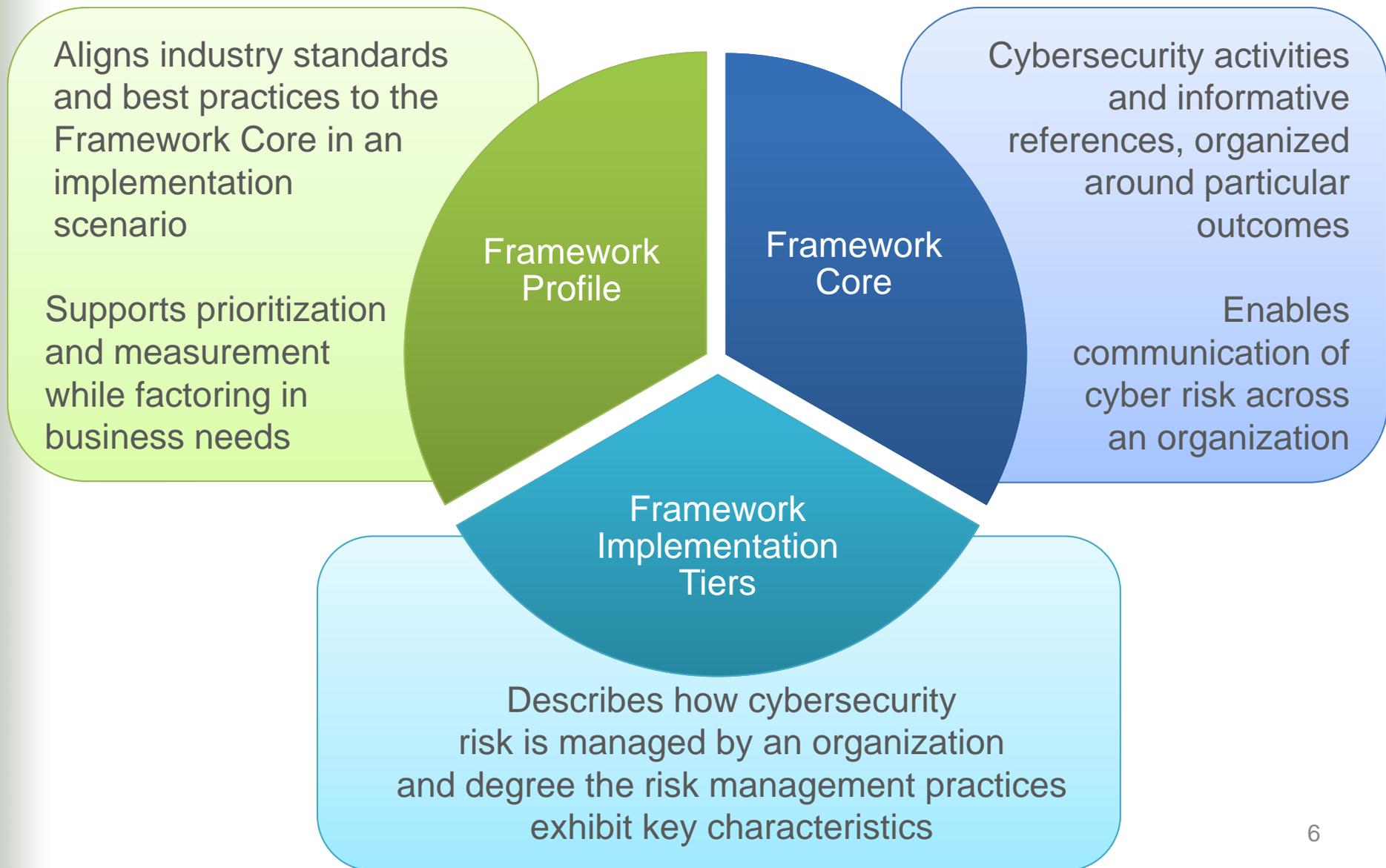
- Used by over 30% of U.S. organizations, trending to 50% (Gartner, 2015, <https://www.gartner.com/webinar/3163821>)
- Required within the United States federal government
- Japanese translation by Information-technology Promotion Agency
- Italian translation and adaptation within Italy's National Framework 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



Cybersecurity Framework Use

- Cisco
- SIEMENS
- Intel
- Motorola
- IBM
- Microsoft
- Dell
- CA Technologies
- State of Indiana
- State of Michigan
- University of Pittsburg
- University of Chicago
- Emblem Health
- Novant Health
- AdvaMed
- Merck
- Kaiser Permanente
- JP Morgan
- Sempra Energy
- Duke Energy
- Boeing
- AT&T
- Nippon Telegraph and Telephone Corporation
- City of Toronto

Cybersecurity Framework Components



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



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

Cybersecurity Framework Component

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
What safeguards are available?	Protect	Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

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

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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

Profile

Cybersecurity Framework Component

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

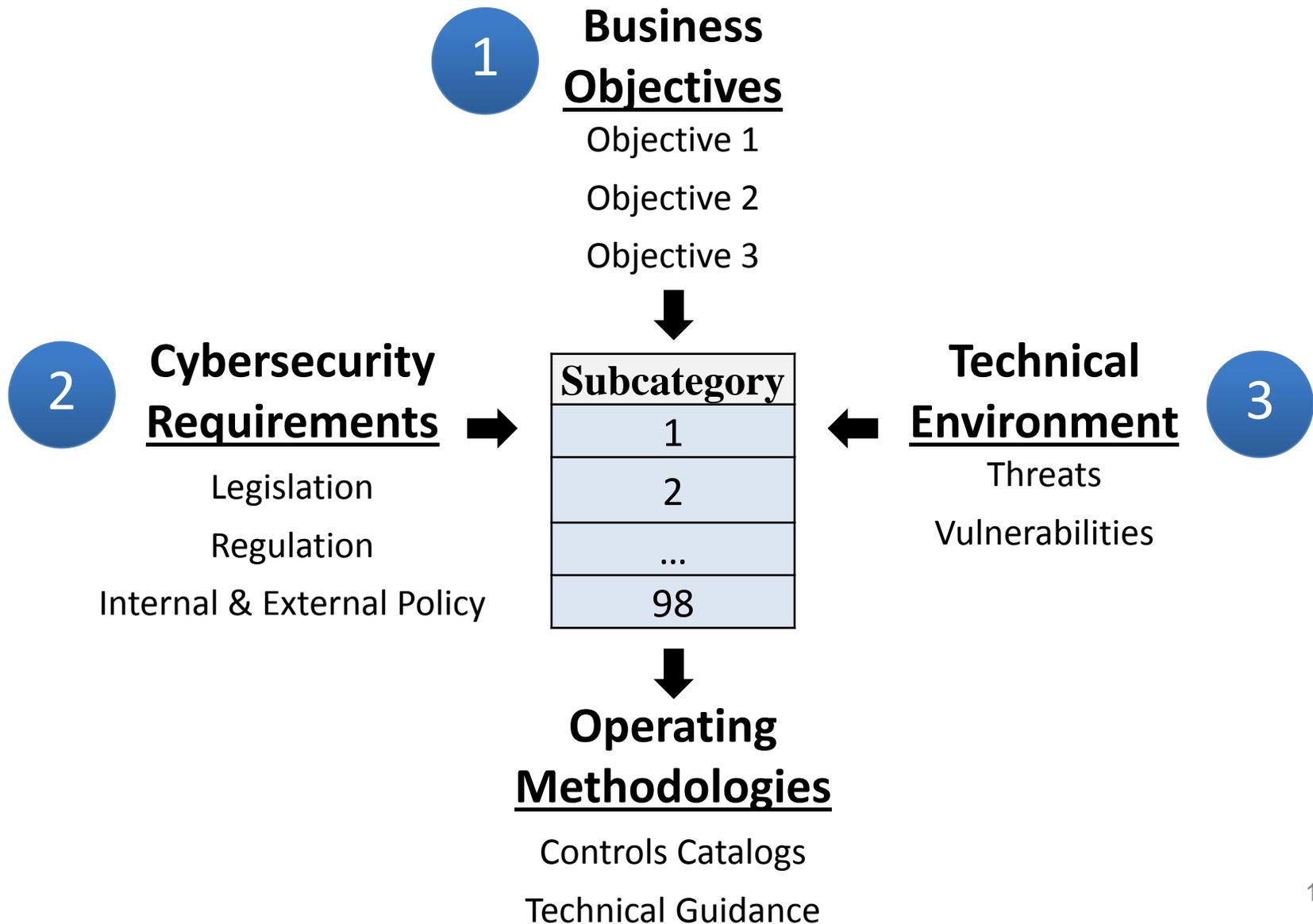
Cybersecurity Program Objectives

Three Things All Cybersecurity Programs Must Do

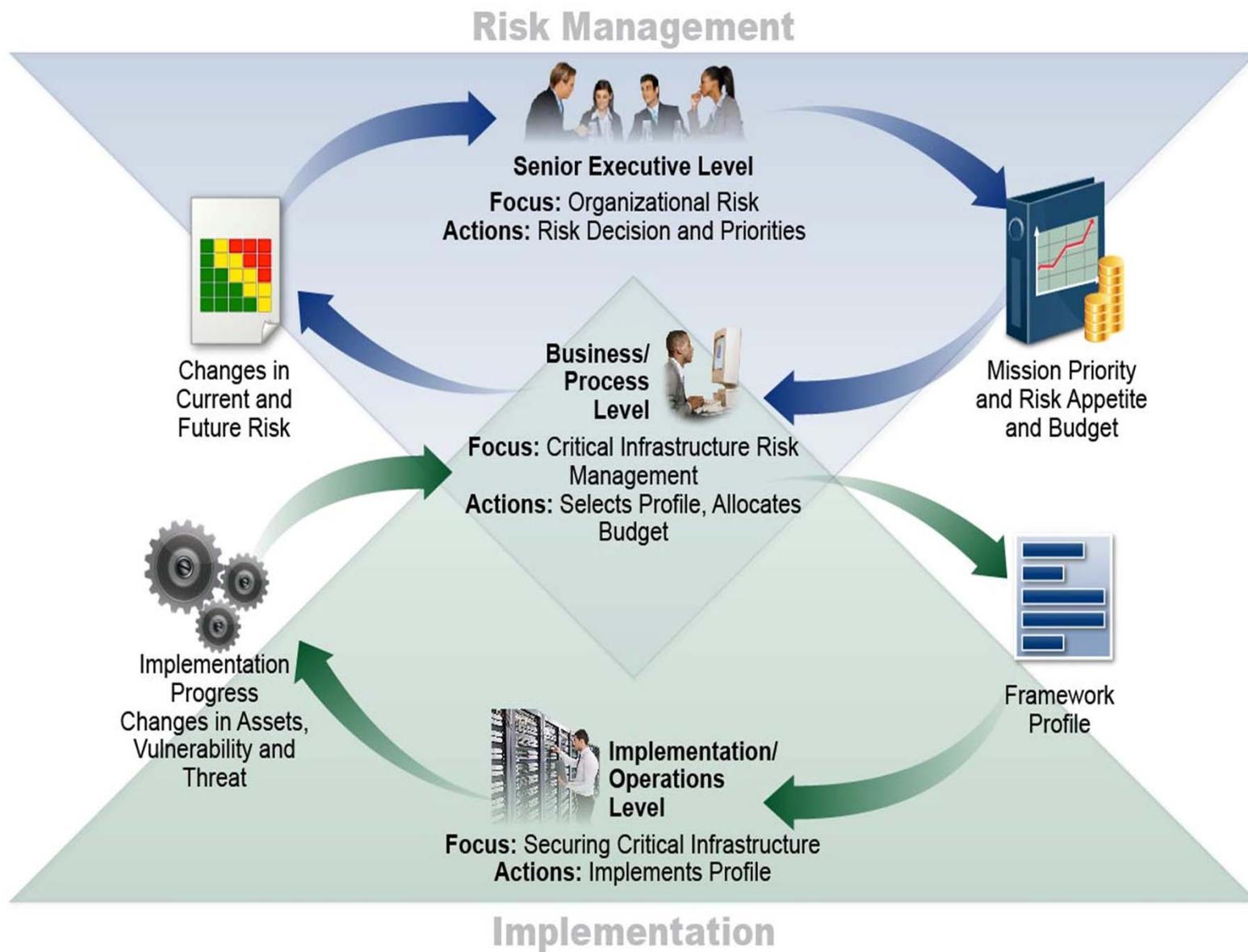
- Support Mission/Business Objectives
- Fulfill Cybersecurity Requirements
- Manage Vulnerability and Threat Associated with the Technical Environment

Profile Foundational Information

A Profile Can be Created from Three Types of Information



Supporting Risk Management with Framework



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

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					

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 sectors and uses

- Meant to be customized

It's risk-based

- A Catalog of cybersecurity outcomes
- Does 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

Framework Proposed Updates

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

- Affirms [Cybersecurity Enhancement Act](#) of 2014 as the current chartering document
- Applicability to "technology" and defines technology
- Applicability for all [system lifecycle phases](#)
- Administratively updates the [Informative References](#)
- New guidance for [self-assessment](#)
- Enhanced guidance for [managing cybersecurity within supply chains and for buying decisions](#)
- Better accounts for [Authorization, Authentication, and Identity Proofing](#)
- Accounts for emerging vulnerability information (a.k.a., [Coordinated Vulnerability Disclosure](#))
- Clarity on Implementation Tiers and their relationship to Profiles

Roadmap Concepts

Draft Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1

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

Proposed Roadmap Topics

Draft Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1

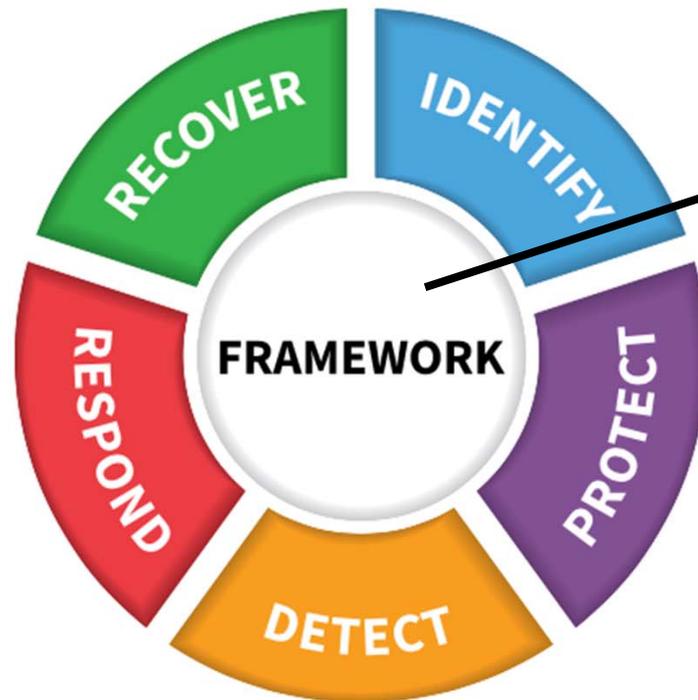
Original Roadmap <i>9 topics</i>	Proposed Roadmap <i>12 topics</i>
Conformity Assessment	<i>Confidence Mechanisms</i>
Automated Indicator Sharing	<i>Cyber-Attack Lifecycle</i>
Data Analytics	Includes Coordinated Vulnerability Disclosure
Cybersecurity Workforce	Cybersecurity Workforce
Supply Chain Risk Management	<i>Cyber Supply Chain Risk Management</i>
Federal Agency Cybersecurity Alignment	Federal Agency Cybersecurity Alignment
	<i>Governance and Enterprise Risk Management</i>
Authentication	Identity Management
International Aspects, Impacts, and Alignment	International Aspects, Impacts, and Alignment
	<i>Measuring Cybersecurity</i>
Technical Privacy Standards	<i>Privacy Engineering</i>
	<i>Referencing Techniques</i>
	<i>Small Business Awareness and Resources</i> ²²

Industry Resources

www.nist.gov/cyberframework/industry-resources

- Framework +
- New to Framework +
- Perspectives +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources** +
- Newsroom +

Framework Resources



General Resources sorted by User Group

Over 150 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



GREATER HOUSTON
PARTNERSHIP

Making Houston Greater.

[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](#)

Industry Resources

www.nist.gov/cyberframework/industry-resources

- Framework +
- New to Framework +
- Perspectives +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources** +
- Newsroom +

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

www.nist.gov/cyberframework/industry-resources

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 

Federal Milestones

Framework for Improving Critical Infrastructure Cybersecurity



[FY 2015-16 Guidance on Federal Information Security and Privacy Management Requirements Cybersecurity Strategy and Implementation Plan](#)
OMB Memorandum M-16-03 & 04

[Managing Information as a Strategic Resource](#)
OMB Circular A-130 Update



[Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure](#)
Executive Order 13800

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.**”

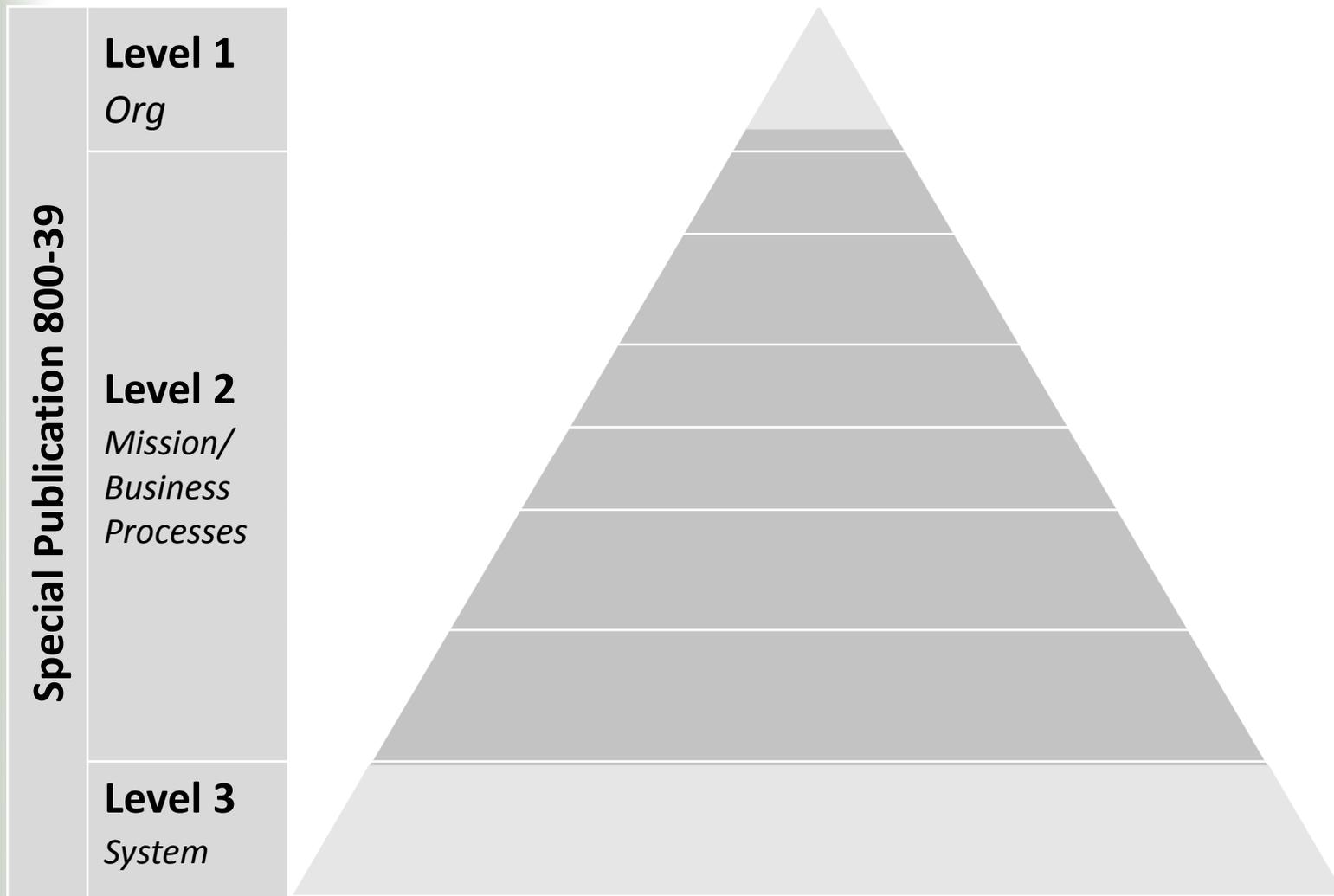
Proposed U.S. Federal Usage

[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)*

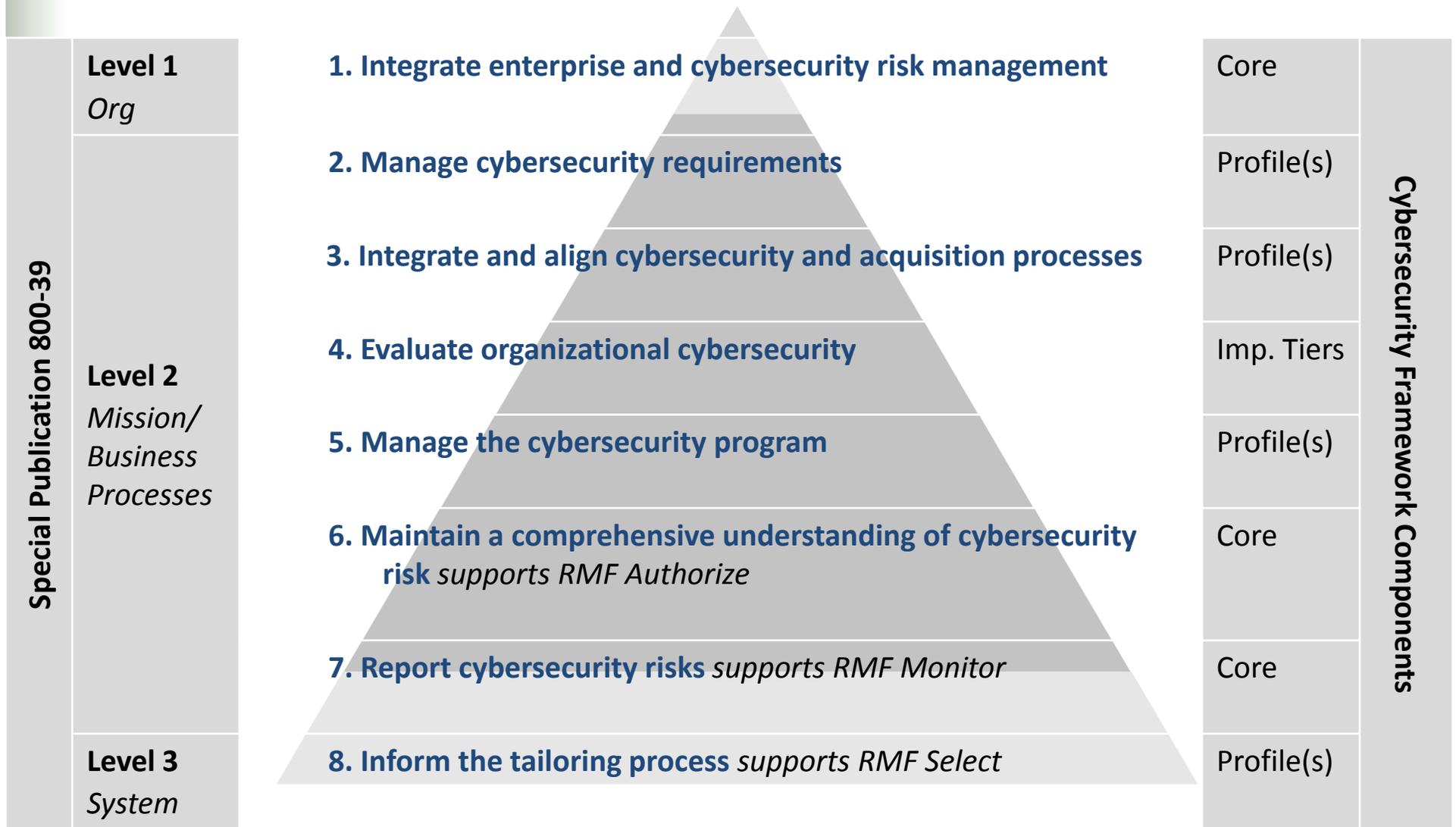
Proposed U.S. Federal Usage

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

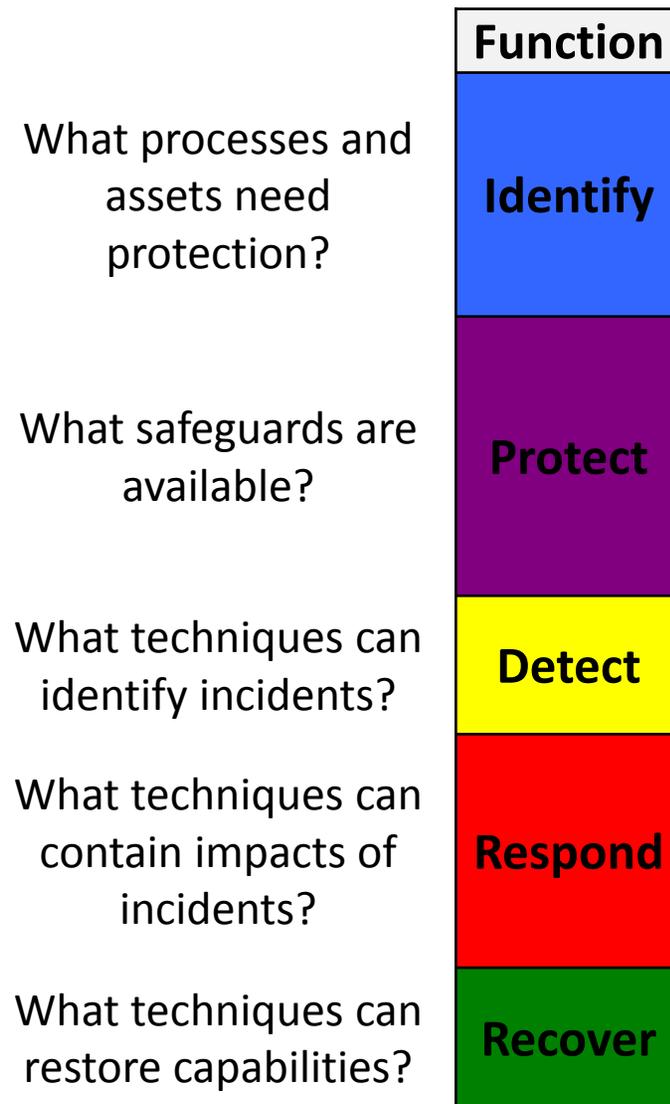


Proposed U.S. Federal Usage

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

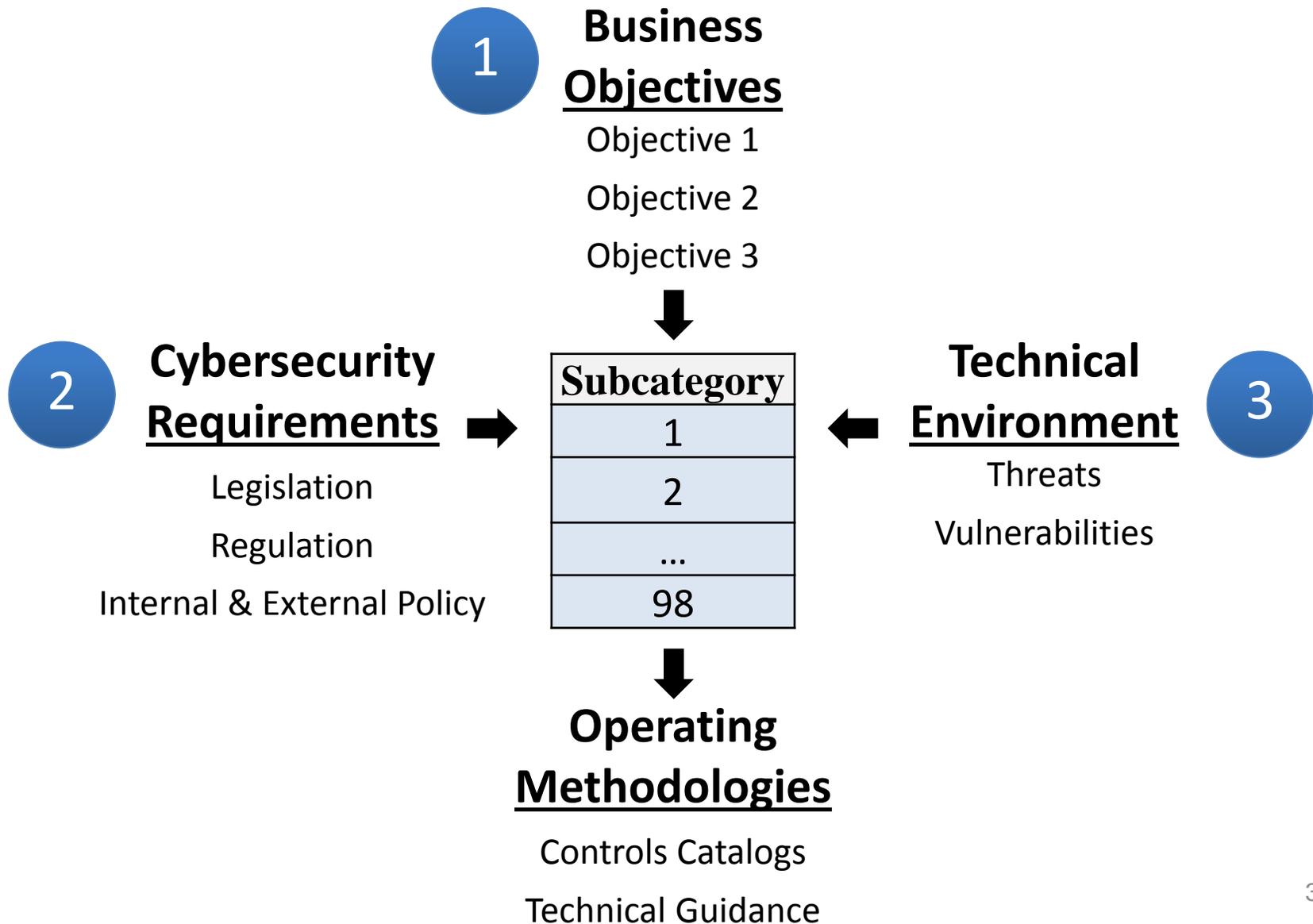


1. Integrate enterprise and cybersecurity risk management



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

2. Manage cybersecurity requirements



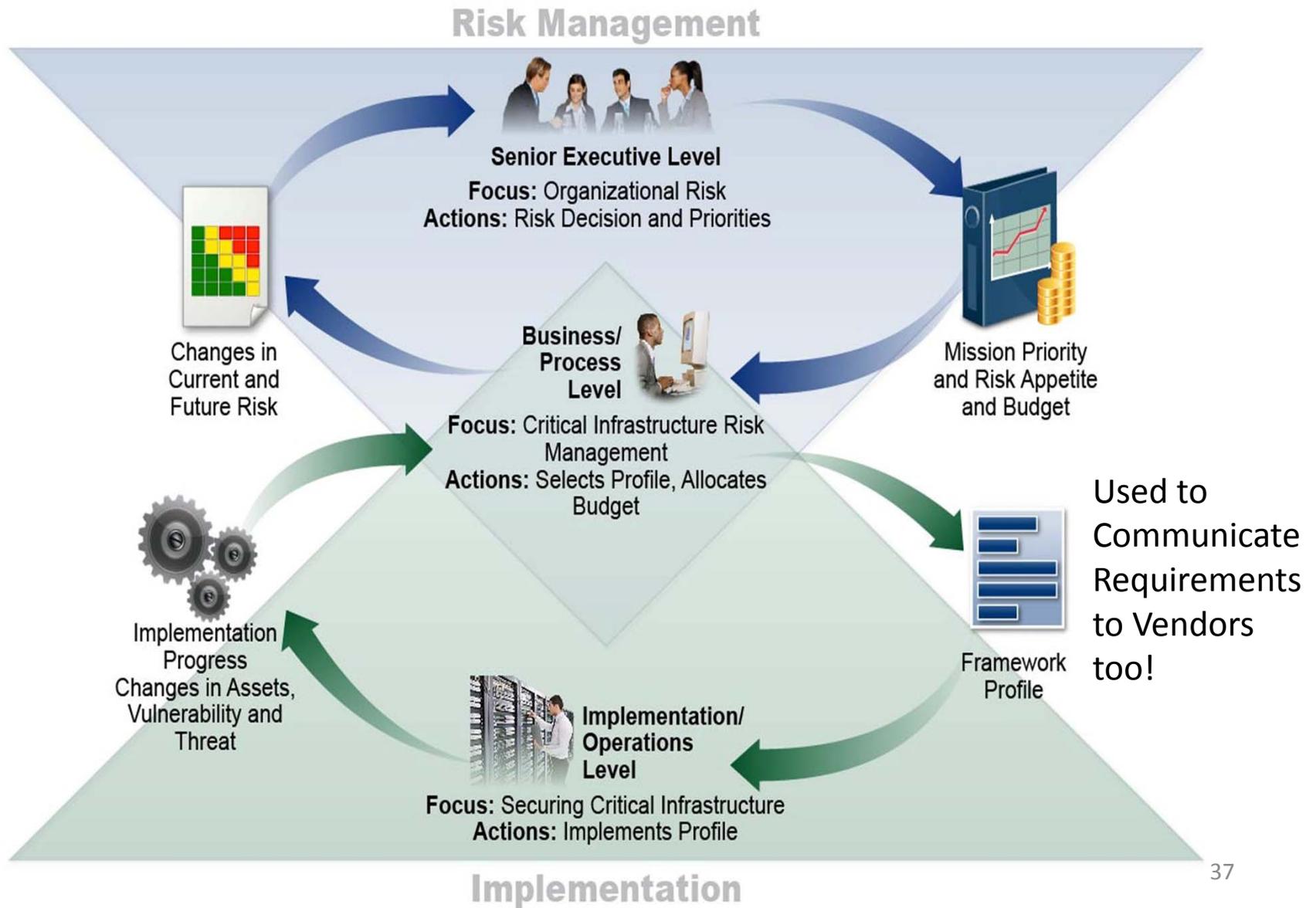
Reconcile

Use Cybersecurity Framework Profiles to Align and Deconflict Requirements

Subcats	Requirements			
1	A		B	
2	C	D	E	F
3	G	H	I	J
...
98	XX		YY	ZZ
	Law	Regulation	Org Policy	Environment

Static ← → *Dynamic*

3. Integrate and align cybersecurity and acquisition processes



4. Evaluate organizational cybersecurity

1	2	3	4
Partial	Risk Informed	Repeatable	Adaptive

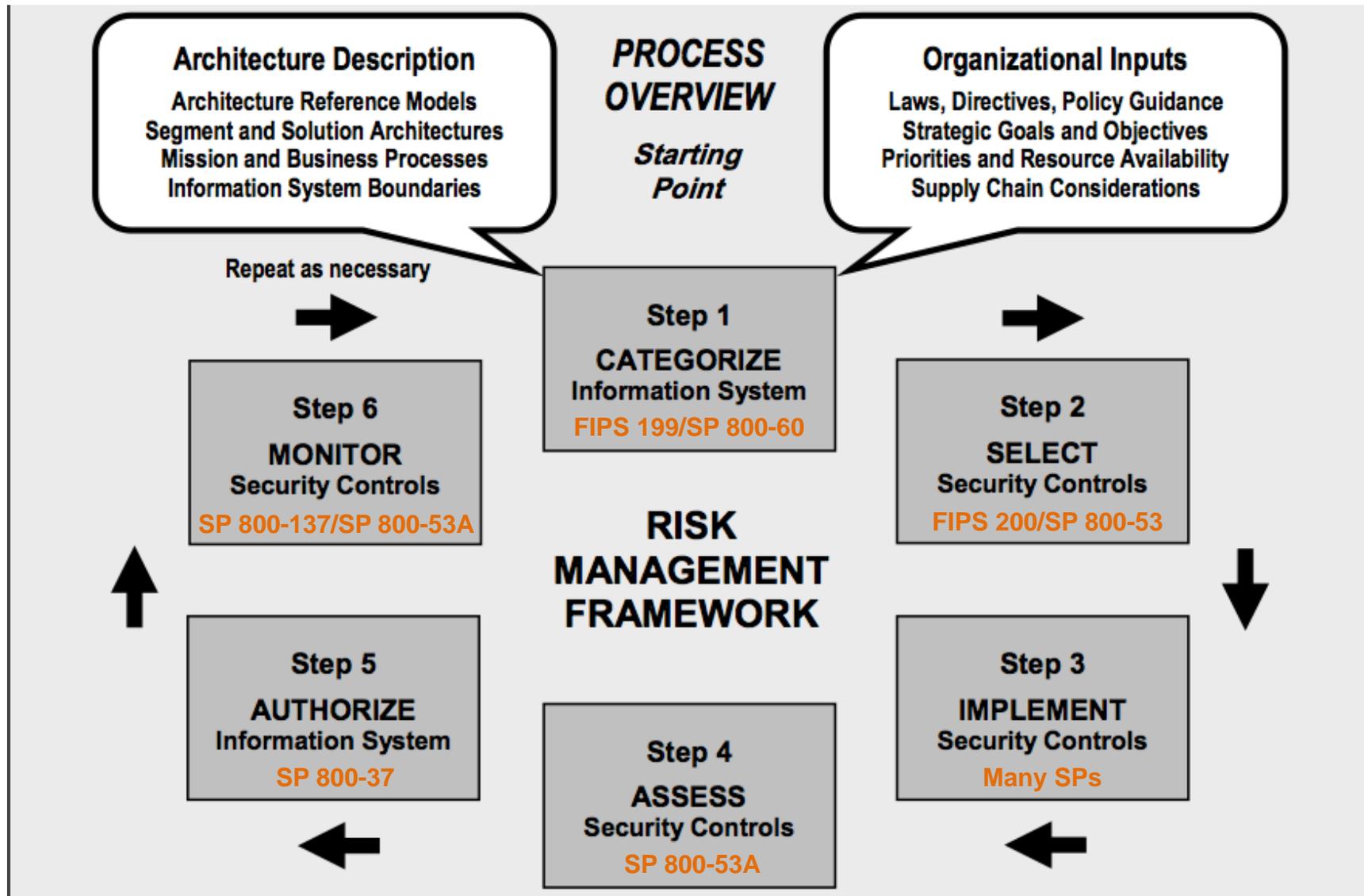
Risk Management Process	The functionality and repeatability of cybersecurity risk management
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions
External Participation	The degree to which the organization benefits my sharing or receiving information from outside parties



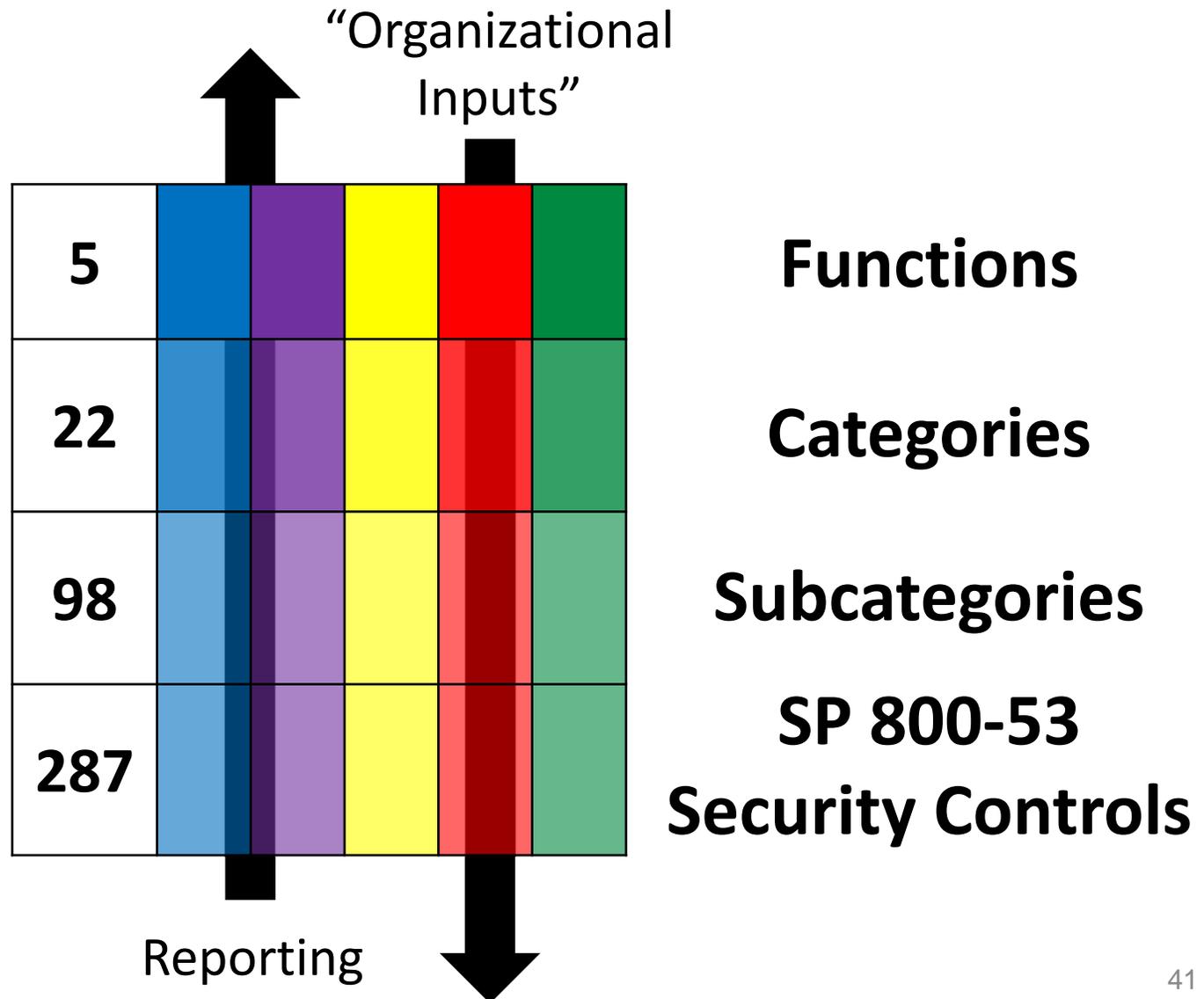
5. Manage the cybersecurity program

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					

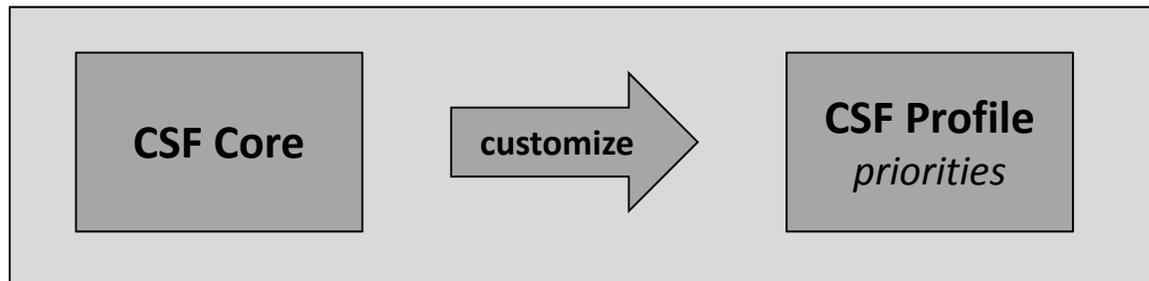
6. Maintain a comprehensive understanding of cybersecurity risk



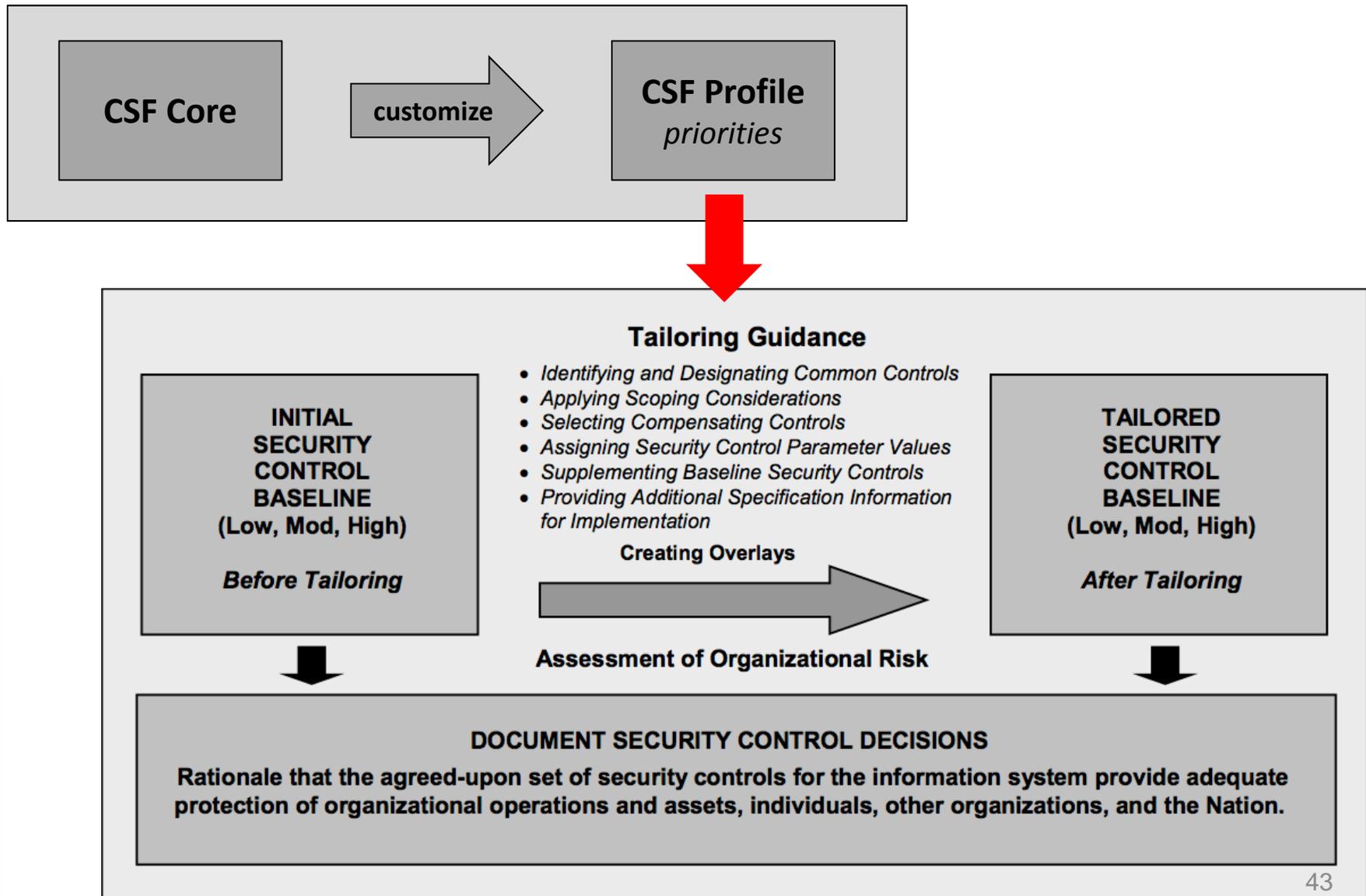
7. Report cybersecurity risks



8. Inform the tailoring process



8. Inform the tailoring process



NIST Federal Framework Publications

Framework for Improving Critical Infrastructure Cybersecurity

[The Cybersecurity Framework:
Implementation Guidance for
Federal Agencies](#)

Draft NIST Interagency Report 8170

The NIST logo is displayed in a large, bold, black, sans-serif font.The NIST logo is displayed in a large, bold, black, sans-serif font.

[SP 800-53rev4 Controls-to-
Cybersecurity Framework](#)

National Institute of Standards and
Technology

[SP 800-171rev1 Requirements-to-
Cybersecurity Framework](#)

National Institute of Standards and
Technology

The NIST logo is displayed in a large, bold, black, sans-serif font.The NIST logo is displayed in a large, bold, black, sans-serif font.

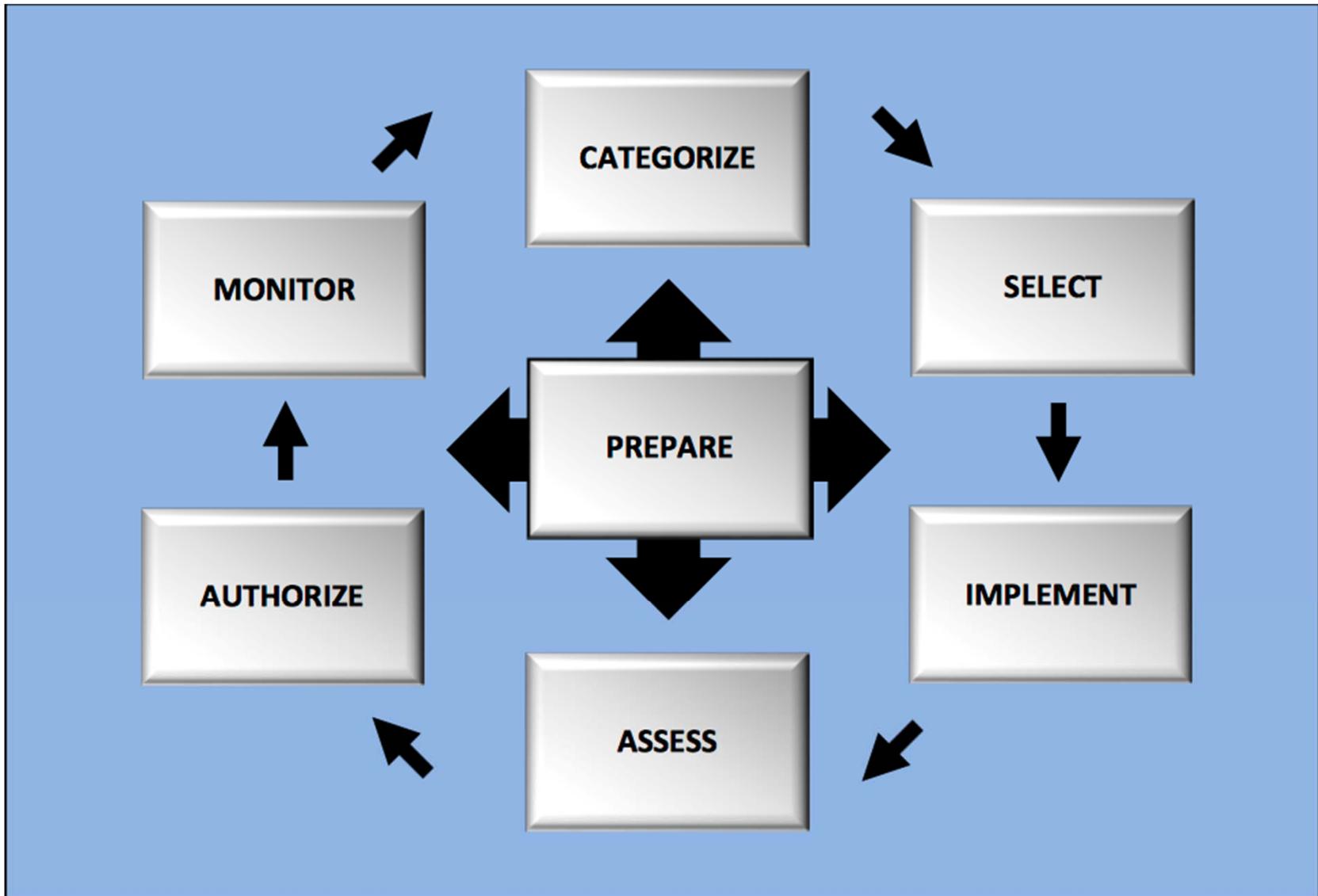
[Risk Management Framework for
Information Systems and Organizations](#)

Discussion Draft NIST

Special Publication 800-37 Revision 2

SP 800-37rev2 Discussion Draft Highlights

[Special Publication 800-37 Revision 2 Discussion Draft](#)



SP 800-37rev2 Discussion Draft Highlights

Special Publication 800-37 Revision 2 Discussion Draft

TABLE B-1: PREPARATION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
<p><u>TASK 1</u></p> <p>Risk Management Roles</p> <p>Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.</p>	<ul style="list-style-type: none"> • <u>Head of Agency</u> or <u>Chief Executive Officer</u> 	<ul style="list-style-type: none"> • <u>Senior Accountable Official for Risk Management</u> • <u>Risk Executive (Function)</u> • <u>Chief Information Officer</u> • <u>Senior Agency Information Security Officer</u> • <u>Senior Agency Official for Privacy</u>
<p><u>TASK 2</u></p> <p>Risk Management Strategy</p> <p>Establish a risk management strategy for the organization that includes a determination of risk tolerance.</p>	<ul style="list-style-type: none"> • <u>Head of Agency</u> or <u>Chief Executive Officer</u> 	<ul style="list-style-type: none"> • <u>Mission/Business Owner</u> • <u>Senior Accountable Official for Risk Management</u> • <u>Risk Executive (Function)</u> • <u>Authorizing Official</u> or <u>Designated Representative</u> • <u>Chief Information Officer</u> • <u>Senior Agency Information Security Officer</u> • <u>Senior Agency Official for Privacy</u>

FISMA Implementation Pub Schedule

As of 8 February 2018, Subject to Change

NIST Special Publication 800-37, Revision 2: *Risk Management Framework for Security and Privacy*

Initial Public Draft: May 2018

Final Public Draft: July 2018

Final Publication: October 2018

NIST Special Publication 800-53, Revision 5: *Security and Privacy Controls*

Final Public Draft: October 2018

Final Publication: December 2018

NIST Special Publication 800-53A, Revision 5: *Assessment Procedures for Security and Privacy Controls*

Initial Public Draft: March 2019

Final Public Draft: June 2019

Final Publication: September 2019

FIPS Publication 200, Revision 1: *Minimum Security Requirements*

Initial Public Draft: October 2018

Final Public Draft: April 2019

Final Publication: July 2019

FIPS Publication 199, Revision 1: *Security Categorization*

Initial Public Draft: December 2018

Final Public Draft: May 2019

Final Publication: August 2019

Updates - <https://csrc.nist.gov/Projects/Risk-Management/Schedule>

Questions or comments - sec-cert@nist.gov 47

What is an Informative Reference?

Online Informative References

- Cybersecurity Framework is outcome-based
- No “How” or “How Much” is specified
- Higher level value when paired
- Potential pairings are called Informative References



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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

February 2018 Web Launch

Online Informative References

NIST

Search NIST 

 NIST MENU

CYBERSECURITY FRAMEWORK

Framework +

New to Framework +

Perspectives +

Online Learning +

Evolution +

Frequently Asked Questions +

Events and Presentations

Related Efforts (Roadmap)

Informative References

Resources +

Newsroom +

Informative References



NIST works with the Framework community to create and maintain a [catalog of Informative References](#) (References). References are citations of detailed cybersecurity documents to any combination of Functions, Categories, and Subcategories within the Framework. References show how to use a given cybersecurity document in coordination with the Framework for the purposes of cybersecurity risk management.

Historically, References have only appeared in the Framework document. To maintain the readability of the document, only a small number of Reference Documents were listed. With release of Version 1.1 of the Framework document, References appear both in the Framework document and in an online format. The online format provides the entire Framework community an opportunity to create a more comprehensive catalog of cybersecurity methodologies, unified through the structure of the Framework.

The online References catalog uses a federated model, where submitting parties develop and host their respective References. NIST analyzes the submitted References for correctness, works with submitters regarding any necessary corrections, and hosts links to the public draft and final versions of the References. The catalog of References includes links to draft content (while it is being evaluated for public comment) and final versions. Draft content is not retained once a document is declared final.

Disclaimer: References are linked to by NIST for information purposes only and do not constitute an endorsement by NIST of the submitted content.

cyberframework-refs@nist.gov

Vocabulary

Online Informative References

Cybersecurity Framework

Element A
Element B
Element C

Reference Document

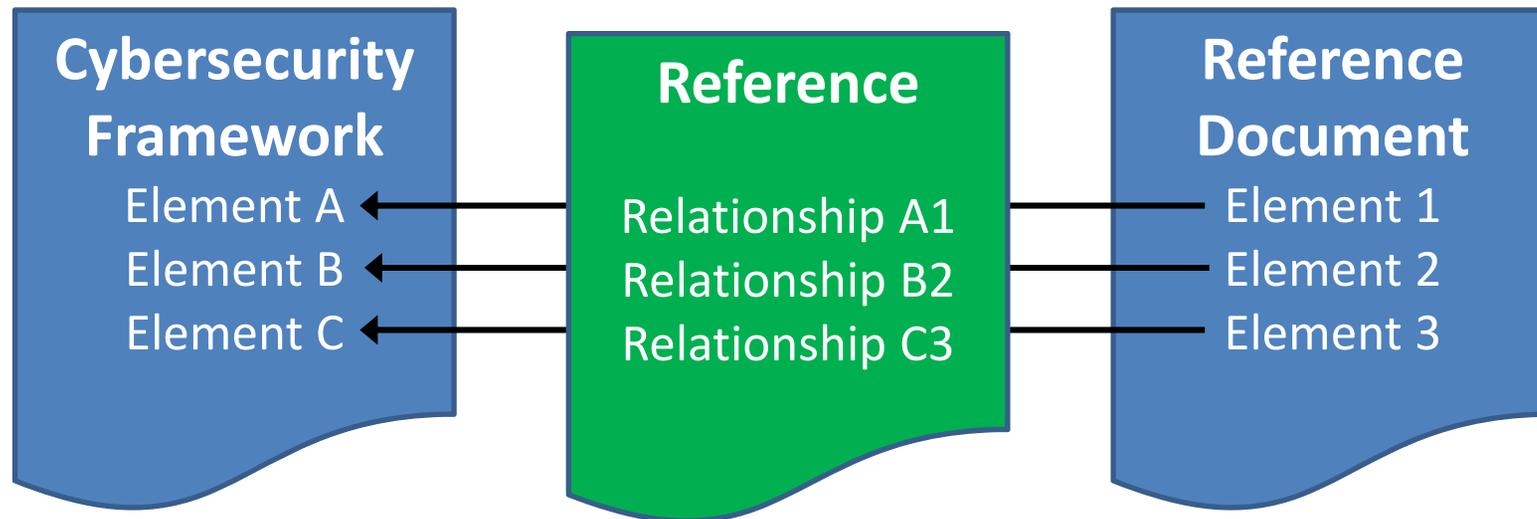
Element 1
Element 2
Element 3

Element

- a logical group of concepts in a given document
- often has an identifier for ease-of-reference
- can be a phrase, sentence, paragraph, or section
- For example:
 - Functions, Categories, Subcategories of Framework
 - Controls of SP 800-53, CobIT, or CIS Top 20
 - Requirements of SP 800-171 or ISO27001

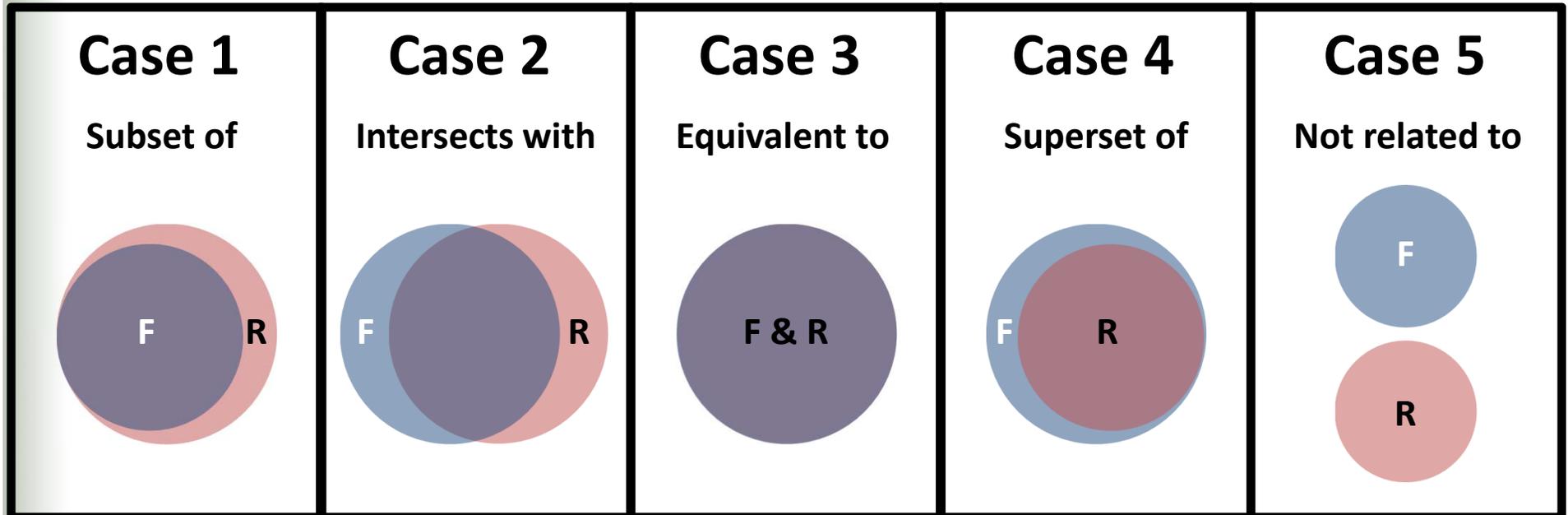
Vocabulary

Online Informative References



Relationship Types

Online Informative References



Key

Framework – blue
Reference Document - red

Near-Term Plan

Online Informative References

- Publish a draft NIST IR 8204
***Cybersecurity Online Informative References (OLIR)
Submissions: Instruction and Definitions for
Completing the OLIR Template***
- Engage “pilot group” to generate References
- Learn & Evolve

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



"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development
(NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674,
Fax: 202-459-9673, Email: nco@nitrd.gov, Website: <https://www.nitrd.gov>

