Framework for Improving Critical Infrastructure Cybersecurity

June 2016

cyberframework@nist.gov

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

National Institute of Standards and Technology (NIST)

About NIST

- NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
  - 3,000 employees
  - 2,700 guest researchers
  - 1,300 field staff in partner organizations
  - Two main locations: Gaithersburg, MD and Boulder, CO

NIST Priority Research Areas

Advanced Manufacturing

IT and Cybersecurity

Healthcare

Forensic Science

Disaster Resilience

Cyber-physical Systems

Advanced Communications

Improving Critical Infrastructure Cybersecurity

"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"

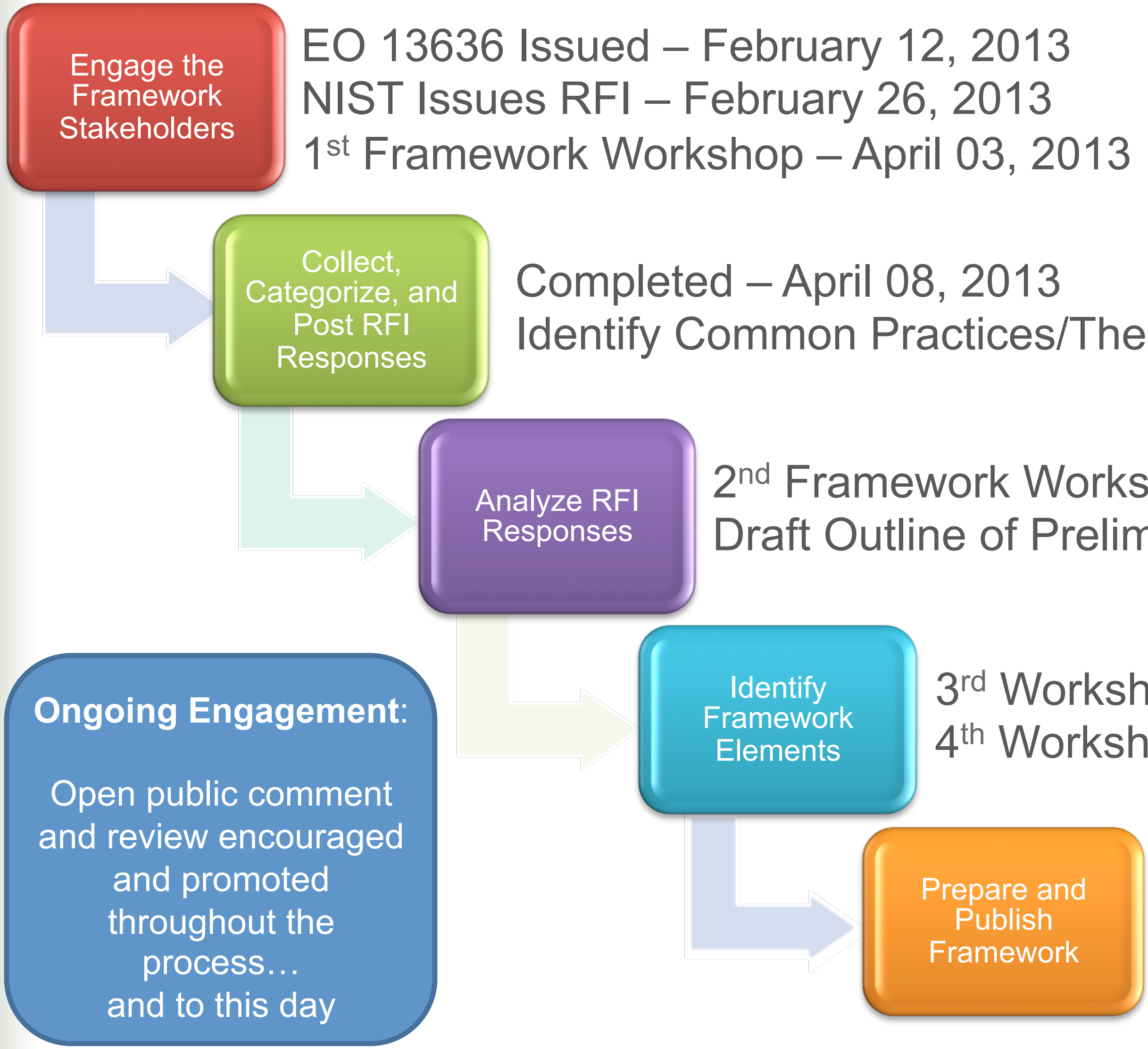
President Barack Obama

Executive Order 13636, 12 February 2013

Based on the Executive Order, the Cybersecurity Framework Must...

- 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

Development of the Framework



Engage the Framework Stakeholders

EO 13636 Issued – February 12, 2013
NIST Issues RFI – February 26, 2013
1st Framework Workshop – April 03, 2013

Collect, Categorize, and Post RFI Responses

Completed – April 08, 2013
Identify Common Practices/Themes – May 15, 2013

Analyze RFI Responses

2nd Framework Workshop at CMU – May 2013
Draft Outline of Preliminary Framework – June 2013

Identify Framework Elements

3rd Workshop at UCSD – July 2013
4th Workshop at UT Dallas – Sept 2013

Prepare and Publish Framework

5th Workshop at NC State – Nov 2013
Published Framework – Feb 2014

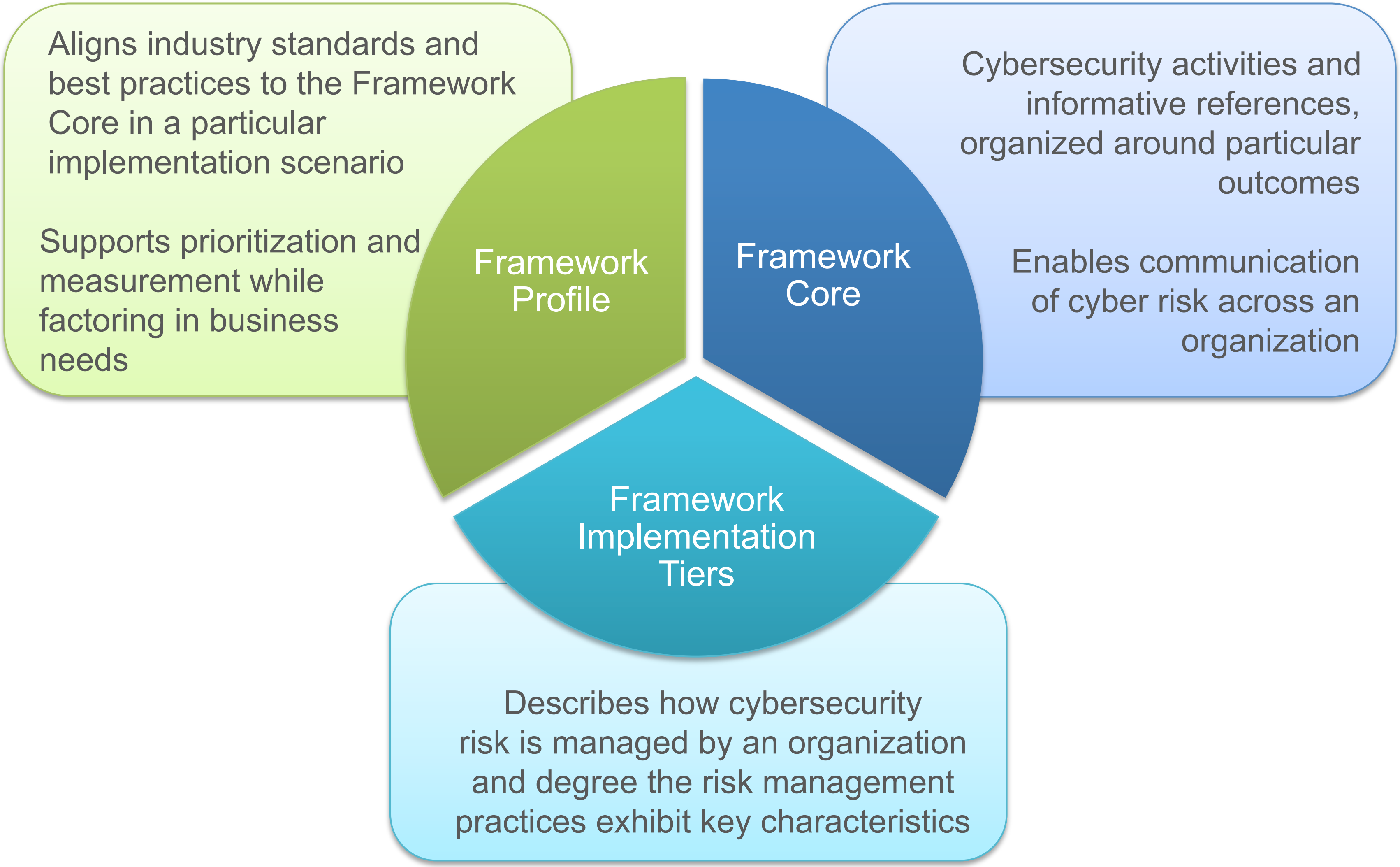
Ongoing Engagement:

Open public comment and review encouraged and promoted throughout the process…
and to this day

The Cybersecurity Framework Is for Organizations…

- Of any size, in any sector in (and outside of) the critical infrastructure
- That already have a mature cyber risk management and cybersecurity program
- That don’t yet have a cyber risk management or cybersecurity program
- With a mission of helping keep up-to-date on managing risk and facing business or societal threats

Cybersecurity Framework Components



Framework Profile

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

Supports prioritization and measurement while factoring in business needs

Framework Core

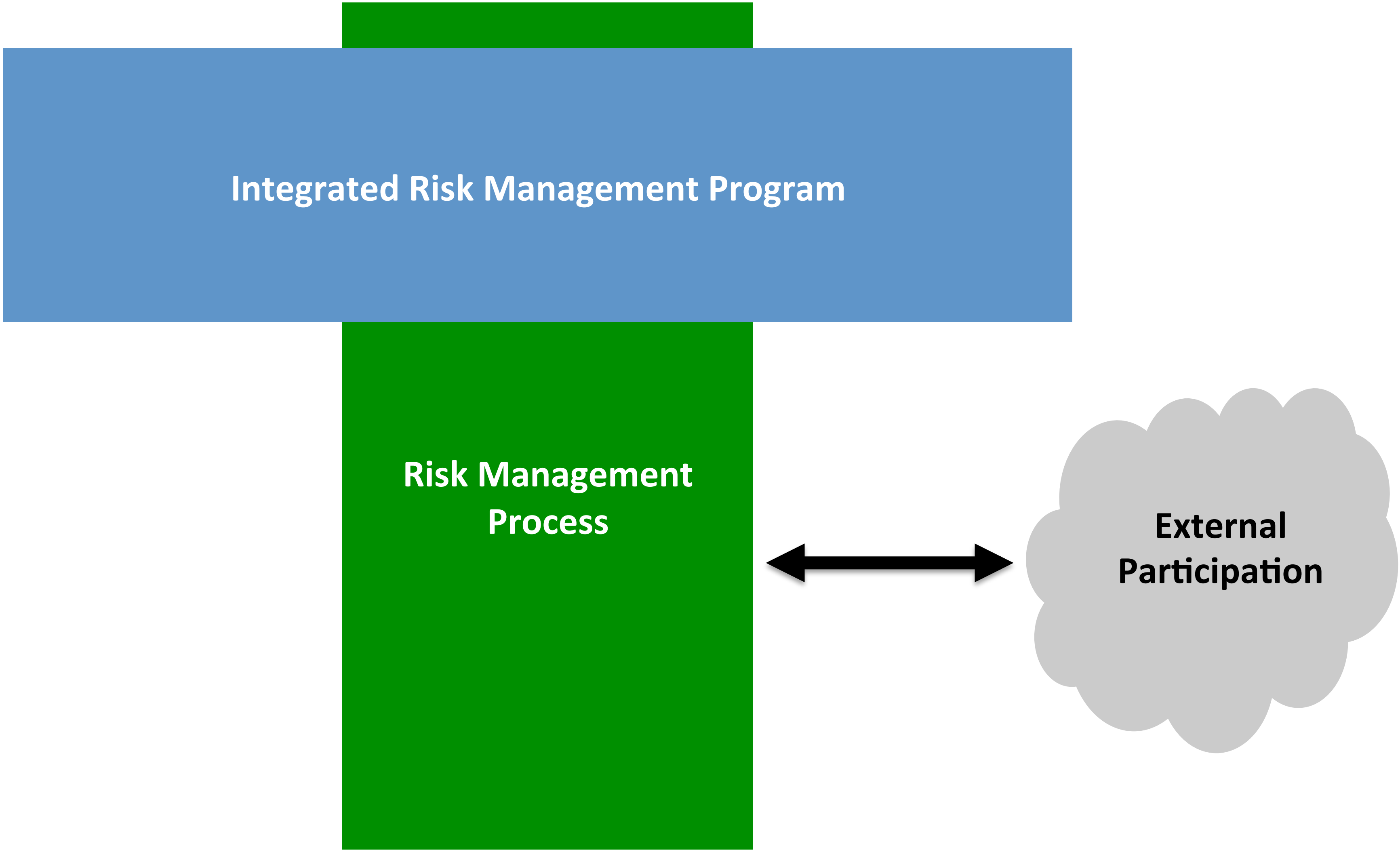
Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Framework Implementation Tiers

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

Key Properties of Cyber Risk Management



Integrated Risk Management Program

Risk Management Process

External Participation

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	2	3	4
Partial	**Risk Informed**	**Repeatable**	**Adaptive**

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

Taxonomy Value Proposition

Plant classification is the placing of known plants into groups or categories to show some relationship. Scientific classification follows a system of rules that standardizes the results, and groups successive categories into a hierarchy.

For example, the family to which lilies belong is classified as:

- **Kingdom:** Plantae
- **Phylum:** Magnoliophyta
- **Class:** Liliopsida
- **Order:** Liliales
- **Family:** Liliaceae
- **Genus:** ……
- **Species:** ……

Value Proposition

- Accurate communication
- Quickly categorize known
- Logically name unknown
- Inherent properties understood based on name

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

Cybersecurity Framework Component

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
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**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
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
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

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

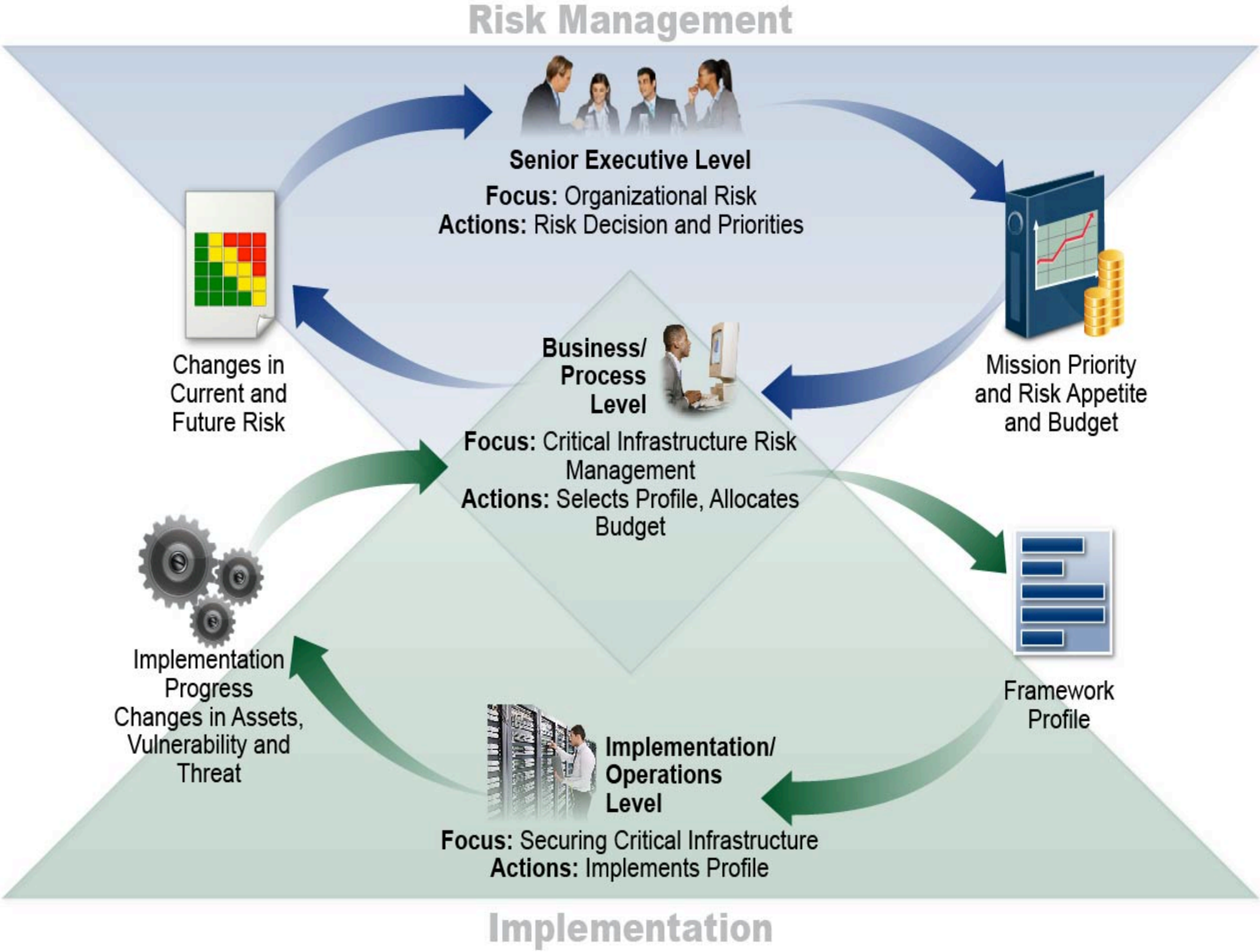
Protect

Detect

Respond

Recover

Supporting Risk Management with Framework



Risk Management

Senior Executive Level

Focus: Organizational Risk
Actions: Risk Decision and Priorities

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

Business/ Process Level

Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget

Implementation Progress Changes in Assets, Vulnerability and Threat

Framework Profile

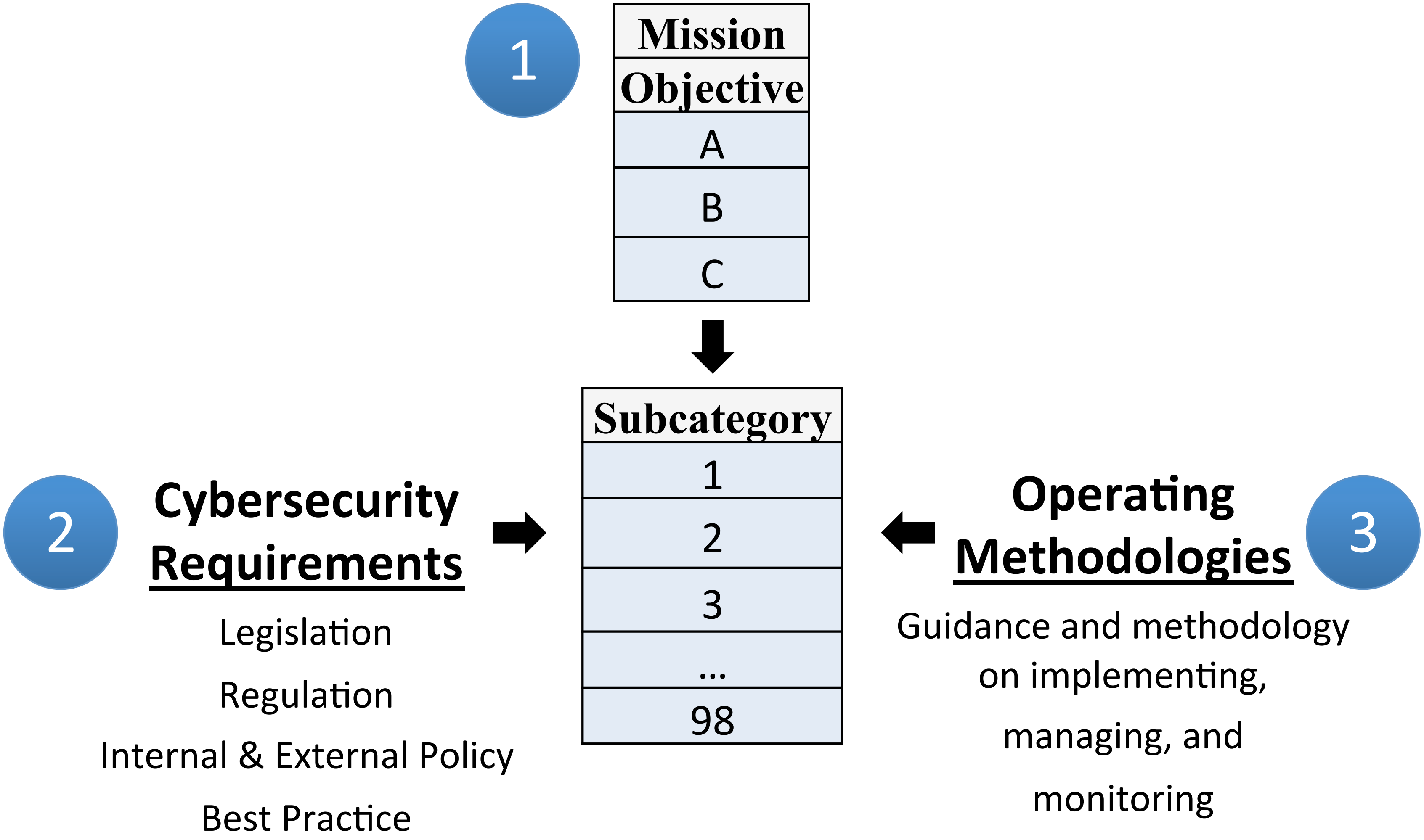
Implementation/ Operations Level

Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

Building a Profile

A Profile Can be Created in Three Steps



1

Mission Objective
A
B
C

Subcategory
1
2
3
…
98

2

Cybersecurity Requirements

Legislation

Regulation

Internal & External Policy

Best Practice

3

Operating Methodologies

Guidance and methodology on implementing, managing, and monitoring

Set Priorities

Use Cybersecurity Framework Profiles to determine Priorities

Subcats	Requirements			
1	High		High	High
2	Mod	High	Mod	Mod
3	Low	Low	Low	
…	…	…	…	…
98			Mod	Mod
	Law	Regulation	Business Objectives	Threat Profile

Static ↔ *Dynamic*

Resource and Budget Decisioning

What Can You Do with a CSF Profile

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	
…	…	…	…		
98	moderate	none	$$		reassess

…and supports on-going operational decisions too

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					

Profile Ecosystem

TAXONOMY

1
2
3
…
98

National Institute of Standards and Technology

Cybersecurity Framework Core

REQUIREMENTS

1	Req A
2	Req B
3	Req C
…	…
98	Req ZZ

Community or Organization

Crosswalks Mappings

PRIORITIES

1	Req A	High
2	Req B	Mod
3	Req C	Low
…	…	…
98	Req ZZ	High

Organization or Community

Cybersecurity Framework Profile

Using Profiles to Drive Incident Resourcing

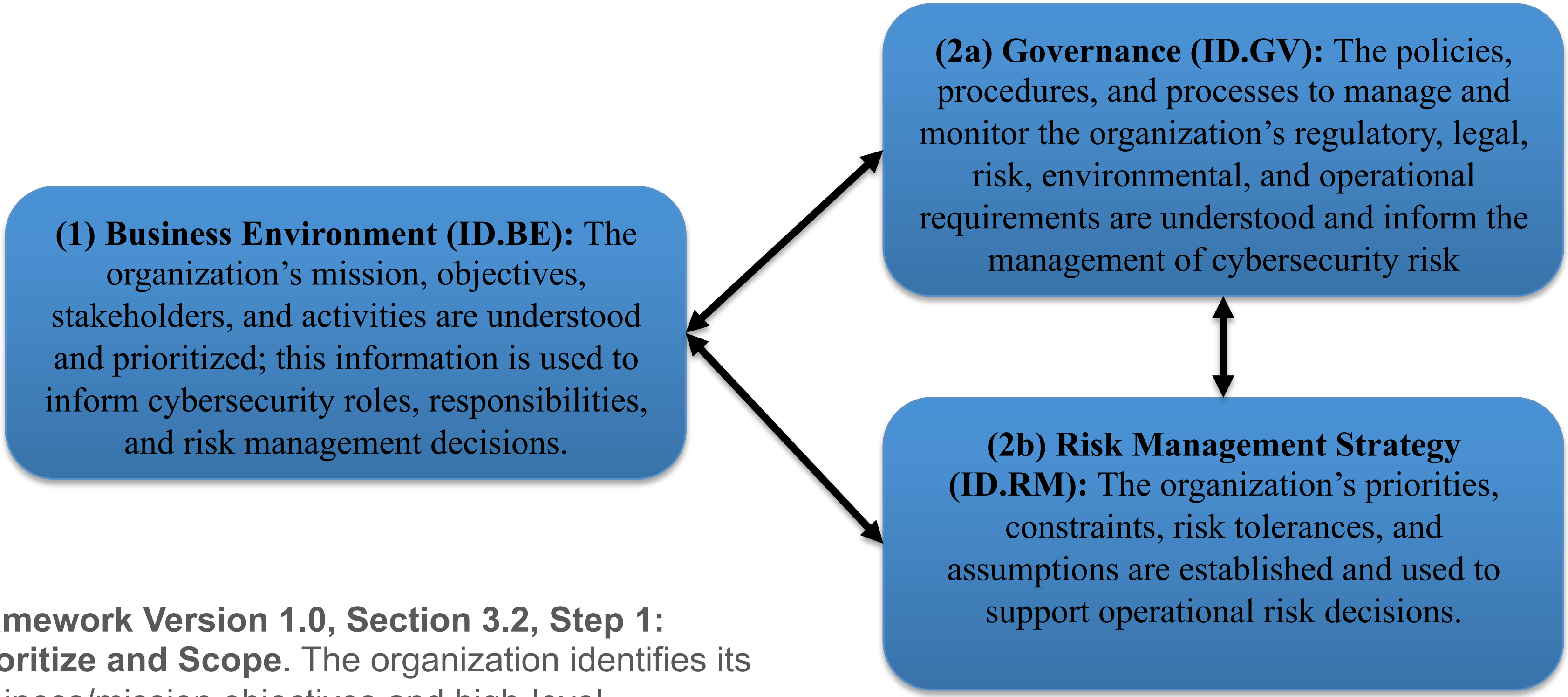
Function	Category	ID	Respond	Recover
Identify	Asset Management	ID.AM		X
	Business Environment	ID.BE		
	Governance	ID.GV		
	Risk Assessment	ID.RA		
	Risk Management Strategy	ID.RM		X
Protect	Access Control	PR.AC	X	
	Awareness and Training	PR.AT		X
	Data Security	PR.DS		X
	Information Protection Processes & Procedures	PR.IP		X
	Maintenance	PR.MA		
	Protective Technology	PR.PT	X	X
Detect	Anomalies and Events	DE.AE		X
	Security Continuous Monitoring	DE.CM	X	
	Detection Processes	DE.DP		X
Respond	Response Planning	RS.RP	X	
	Communications	RS.CO	X	
	Analysis	RS.AN	X	
	Mitigation	RS.MI	X	
	Improvements	RS.IM	X	
Recover	Recovery Planning	RC.RP		X
	Improvements	RC.IM		X
	Communications	RC.CO		X

Key Attributes

- **It's a framework, not a prescription**
  - It provides a common language and systematic methodology for managing cyber risk
  - It is meant to be adapted
  - It does not tell a company *how* much cyber risk is tolerable, nor does it claim to provide "the one and only" formula for cybersecurity
  - Having a common lexicon to enable action across a very diverse set of stakeholders will enable the best practices of elite companies to become standard practices for everyone

- **The framework is a living document**
  - It is intended to be updated over time as stakeholders learn from implementation, and as technology and risks change
  - That's one reason why the framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, and standards will change over time—principals will not

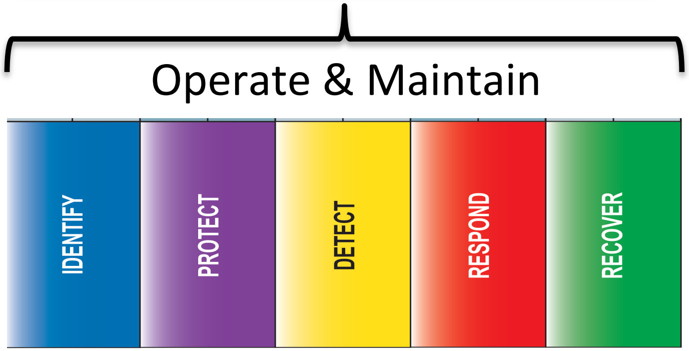
Where Should I Start?



(1) Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

(2a) Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk

(2b) Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.



Framework Version 1.0, Section 3.2, Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

Common Patterns of Use

- Integrate the Functions into Your Leadership Vocabulary and Management Tool Sets
- Determine Optimal Risk Management Using Implementation Tiers
- 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

Examples of Framework Industry Resources

cini Cyber Security National Lab

CIS Sapienza
Cyber Intelligence and Information Security

Italy's National Framework for Cybersecurity

Cybersecurity Guidance for Small Firms

sifma
Invested in America

intel
Look Inside.™

The Cybersecurity Framework in Action: An Intel Use Case

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

CSRIC
Communications Security, Reliability and Interoperability Council

Department of Energy • United States of America

Energy Sector Cybersecurity Framework Implementation Guidance

Examples of U.S. State & Local Use

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

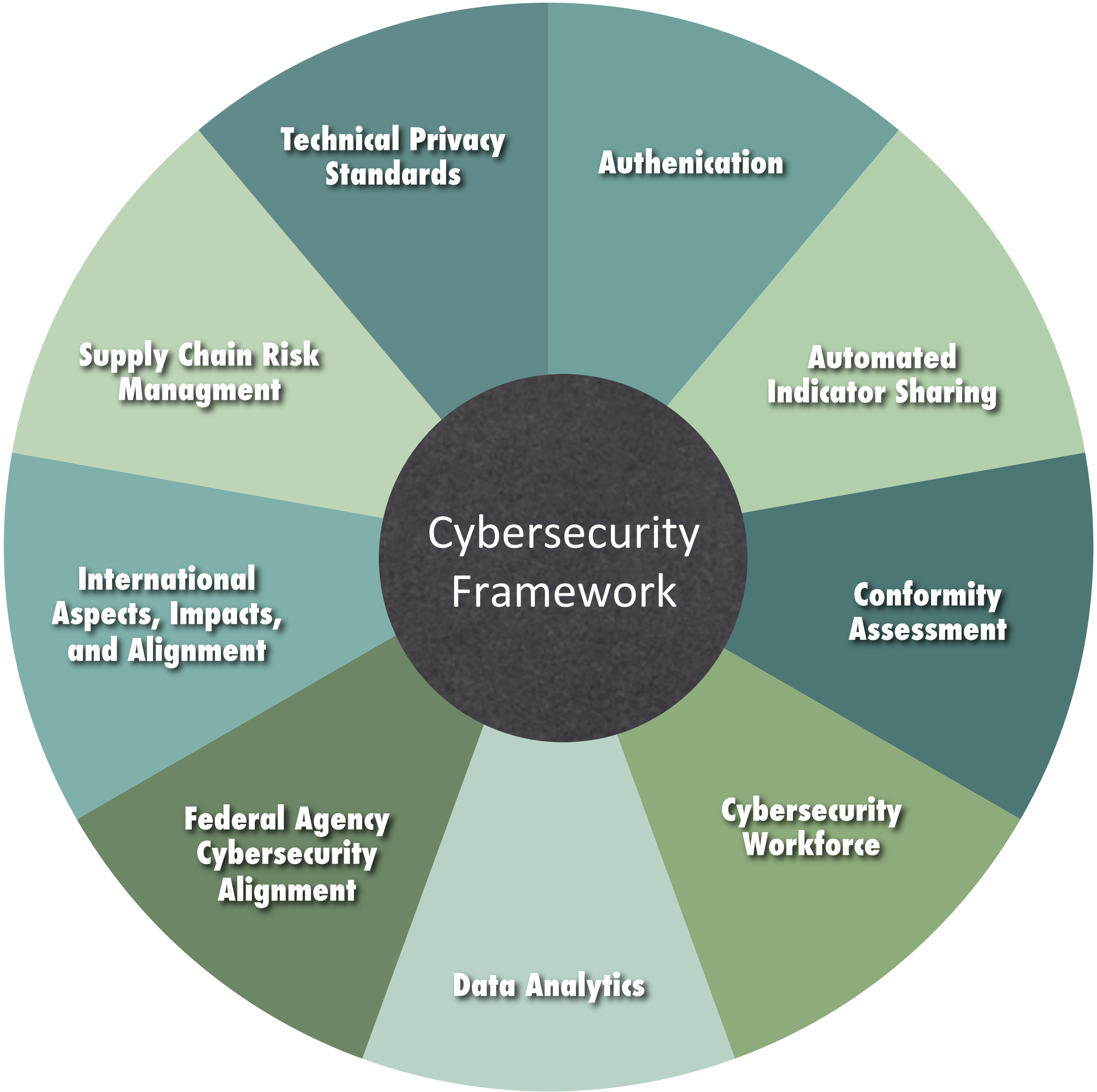
National Association of State CIOs

- 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

Roadmap Items



Cybersecurity Framework

Technical Privacy Standards

Authenication

Automated Indicator Sharing

Conformity Assessment

Cybersecurity Workforce

Data Analytics

Federal Agency Cybersecurity Alignment

International Aspects, Impacts, and Alignment

Supply Chain Risk Managment

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

Recent Framework Related Policy and Legislation

Maritime Transportation Security Act of 2002

- Originally authored with physical security in mind
- Recently clarified to apply to cybersecurity
- Coast Guard publishing Framework Profile to help industry adapt

Cybersecurity Enhancement Act of 2014

- Codified NIST's on-going role facilitating Framework evolution
- Asked NIST to facilitate less redundancies in regulation

OMB Memorandum M-16-03 & 04

- M-16-03: FY 2015-16 Guidance on Federal Information Security and Privacy Management Requirements
- M-16-04: Cybersecurity Strategy and Implementation Plan

Circular A-130 Update

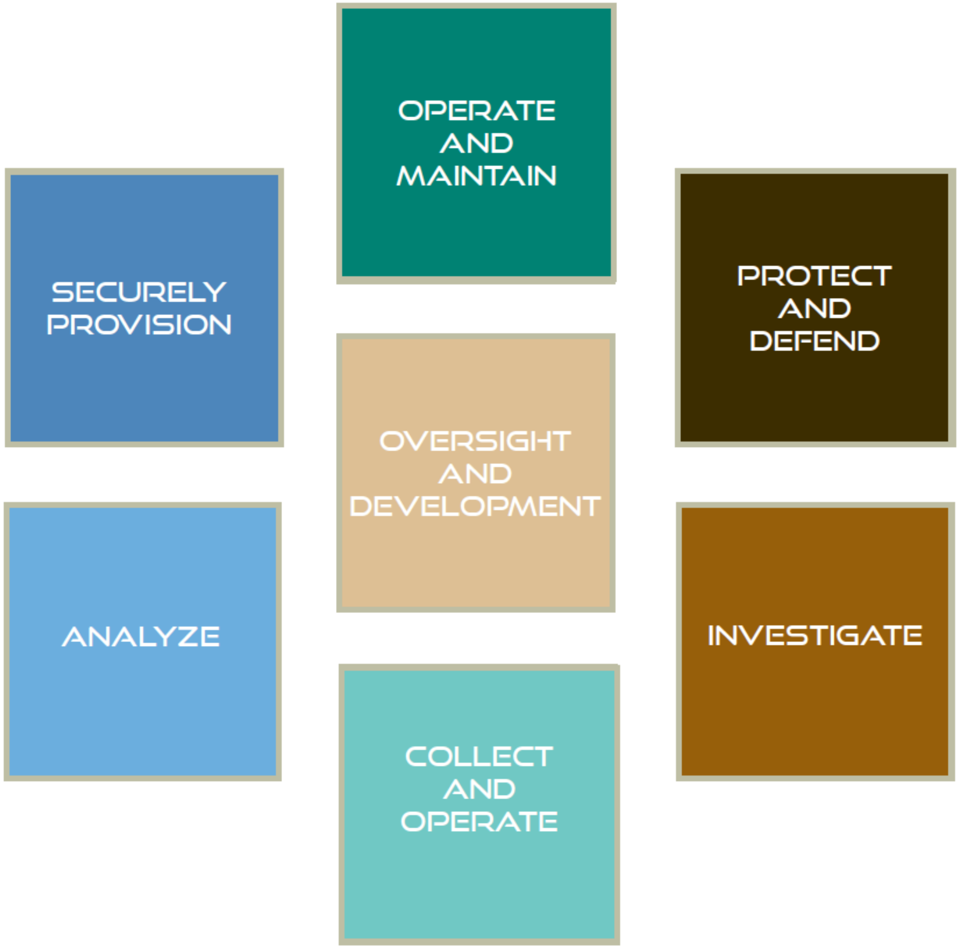
- Provides generalized guidance for use of pre-existing FISMA-based guidance like Risk Management Framework with Cybersecurity Framework
- NIST publishing guidance on using Risk Management Framework and Cybersecurity Framework together

Framework Roadmap Items

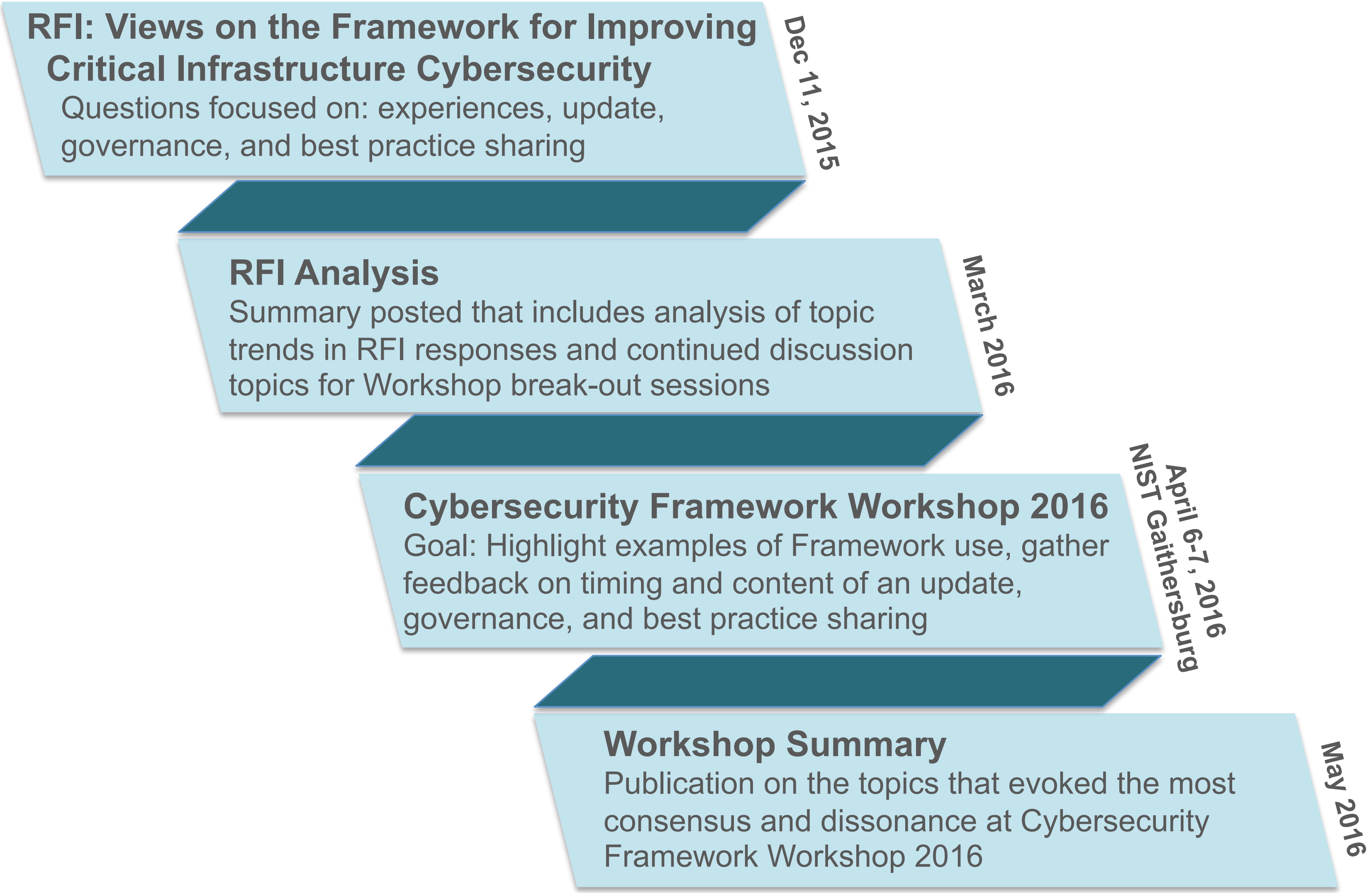
- Authentication
- Automated Indicator Sharing
- Conformity Assessment
- Cybersecurity Workforce
- Data Analytics
- Federal Agency Cybersecurity Alignment
- International Aspects, Impacts, and Alignment
- Supply Chain Risk Management
- Technical Privacy Standards

National Initiative for Cybersecurity Education

- Early stages of collaboration to show the connection points between Cybersecurity Framework and National Initiative for Cybersecurity Education
- Anticipate use cases for
  - Organizing academic curriculum
  - Workforce roles and responsibilities
  - Professional certifications



Recent and Near-Term Framework Events



RFI: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Questions focused on: experiences, update, governance, and best practice sharing

Dec 11, 2015

RFI Analysis

Summary posted that includes analysis of topic trends in RFI responses and continued discussion topics for Workshop break-out sessions

March 2016

Cybersecurity Framework Workshop 2016

Goal: Highlight examples of Framework use, gather feedback on timing and content of an update, governance, and best practice sharing

April 6-7, 2016
NIST Gaithersburg

Workshop Summary

Publication on the topics that evoked the most consensus and dissonance at Cybersecurity Framework Workshop 2016

May 2016

RFI Questions and Workshop Discussion Threads

Request for Information

11 December 2015 – 23 February 2016

https://www.federalregister.gov/articles/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity

RFI Responses: http://csrc.nist.gov/cyberframework/rfi_comments_02_09_16.html

- ways in which the Framework is being used to improve cybersecurity risk management,
- how best practices for using the Framework are being shared,
- the relative value of different parts of the Framework,
- the possible need for an update of the Framework, and
- options for long-term governance of the Framework.

Cybersecurity Framework Workshop 2016

6 & 7 April 2016

Registration: https://appam.certain.com/profile/form/index.cfm?PKformID=0x29774a453

More Info: http://www.nist.gov/cyberframework

Program Eras

Feb 2013 *Feb 2014* *Feb 2016*

	Develop	Support	Update
Key Milestones	Five Workshops Request for Information Request for Comment Publication	Request for Information Workshop Speaking Events	Request for Information Workshop **Request for Comment** **Publication**
NIST is:	Adjudicating Stakeholder Input Crafting Version 1.0	Educating Building a Knowledge Base and Resource Catalog	Adjudicating Stakeholder Input Crafting Version Next
Stakeholders are:	Participating in the development process	Understanding and Piloting Framework Sharing Work Products	Expanding Framework Implementations Participating in the Update Process

Resources

Where to Learn More and Stay Current

The National Institute of Standards and Technology Web site is available at http://www.nist.gov

NIST Computer Security Division Computer Security Resource Center is available at http://csrc.nist.gov/

The *Framework for Improving Critical Infrastructure Cybersecurity* and related news and information are available at www.nist.gov/cyberframework

For additional Framework info and help
cyberframework@nist.gov