Framework for Improving Critical Infrastructure Cybersecurity

26 August 2015

cyberframework@nist.gov

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

Agenda

- Background and Information
- General Uses
- NIST's Activities
- Roadmap Items
  - Cybersecurity Workforce
  - International
  - Federal
- Near-Term Industry Dialog

Executive Order: Improving Critical Infrastructure Cybersecurity

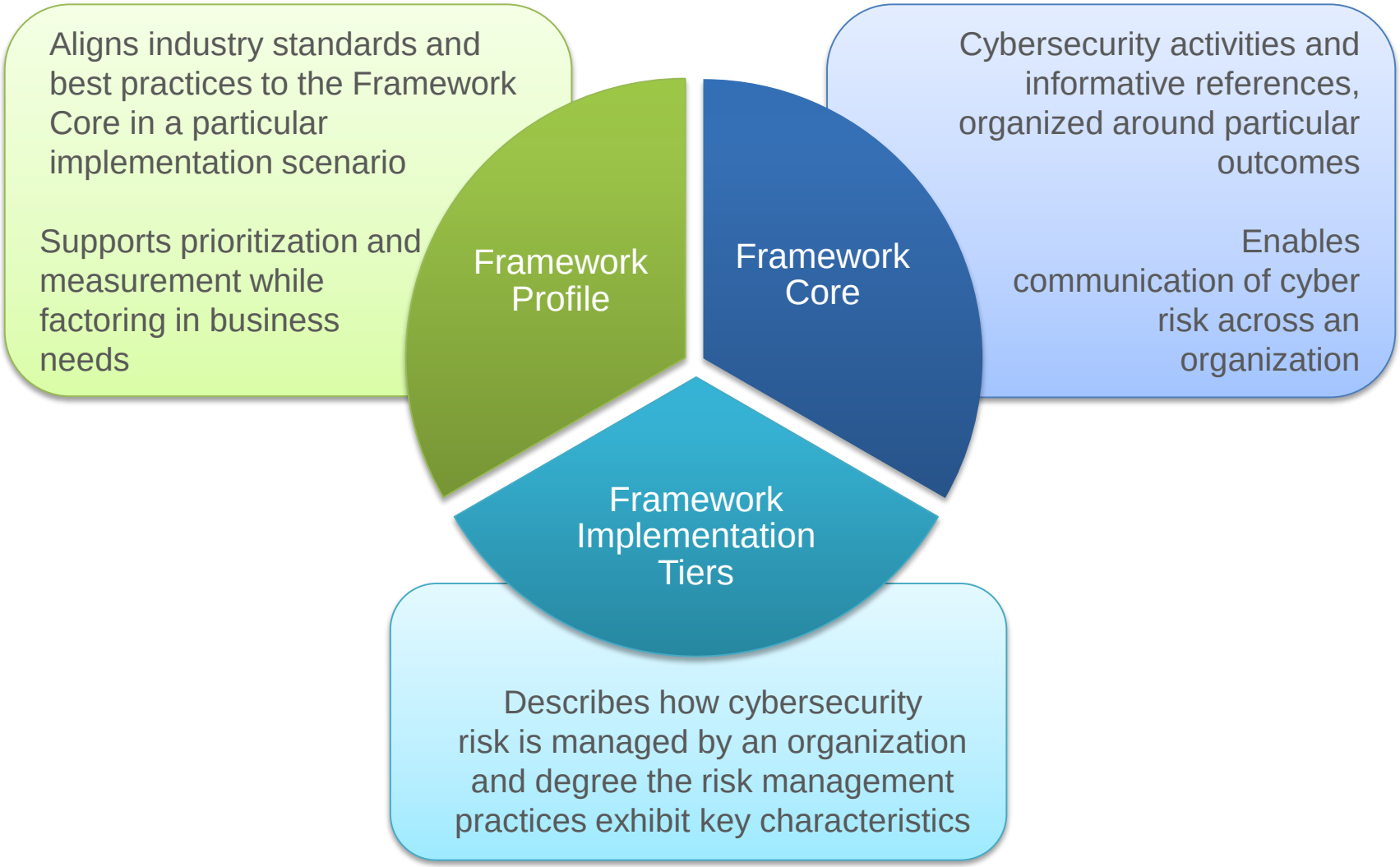
"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

President Barack Obama

Executive Order 13636, *Feb. 12, 2013*

- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work

Cybersecurity Framework Components



Framework Core

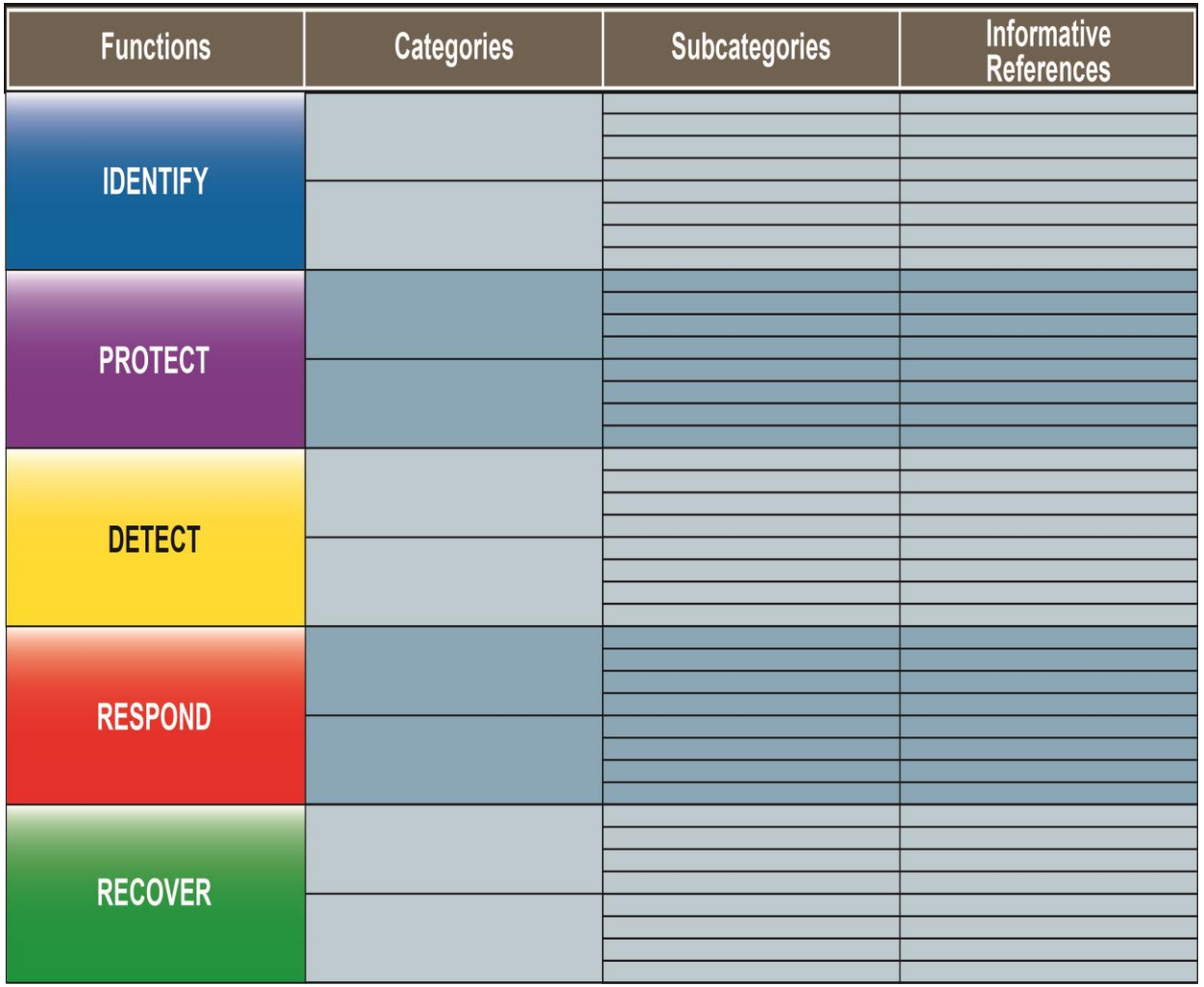
What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?



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 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector 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-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	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-5: Resilience requirements to support 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

Profile

Cybersecurity Framework Component

To maximize value, do the following things with your security requirements using a Profile:

1) Align
2) De-conflict
3) Prioritize

- Alignment of Functions, Categories, and Subcategories with business requirements, risk tolerance, and resources of the organization
- Enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities
- Can be used to describe current state or desired target state of cybersecurity activities

Cybersecurity Framework 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 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector 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-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	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-5: Resilience requirements to support 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

Cybersecurity Framework Profile

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	Priority	Cyber Security Requirements
1	Moderate	A B
2	High	C D E
3	Moderate	F G
4	Low	H
5	Low	I J K
6	Moderate	L M

Gap Analysis, Resourcing, and Resolution

What Can You Do with a CSF Profile

Subcat	Priority	Cyber Sec Reqmts	Gaps
1	Moderate	A B	small
2	High	C D E	large
3	Moderate	F G	medium
4	Low	H	none
5	Low	I J K	large
6	Moderate	L M	medium

Year 1 Activities

Subcategory 2

Subcategory 3

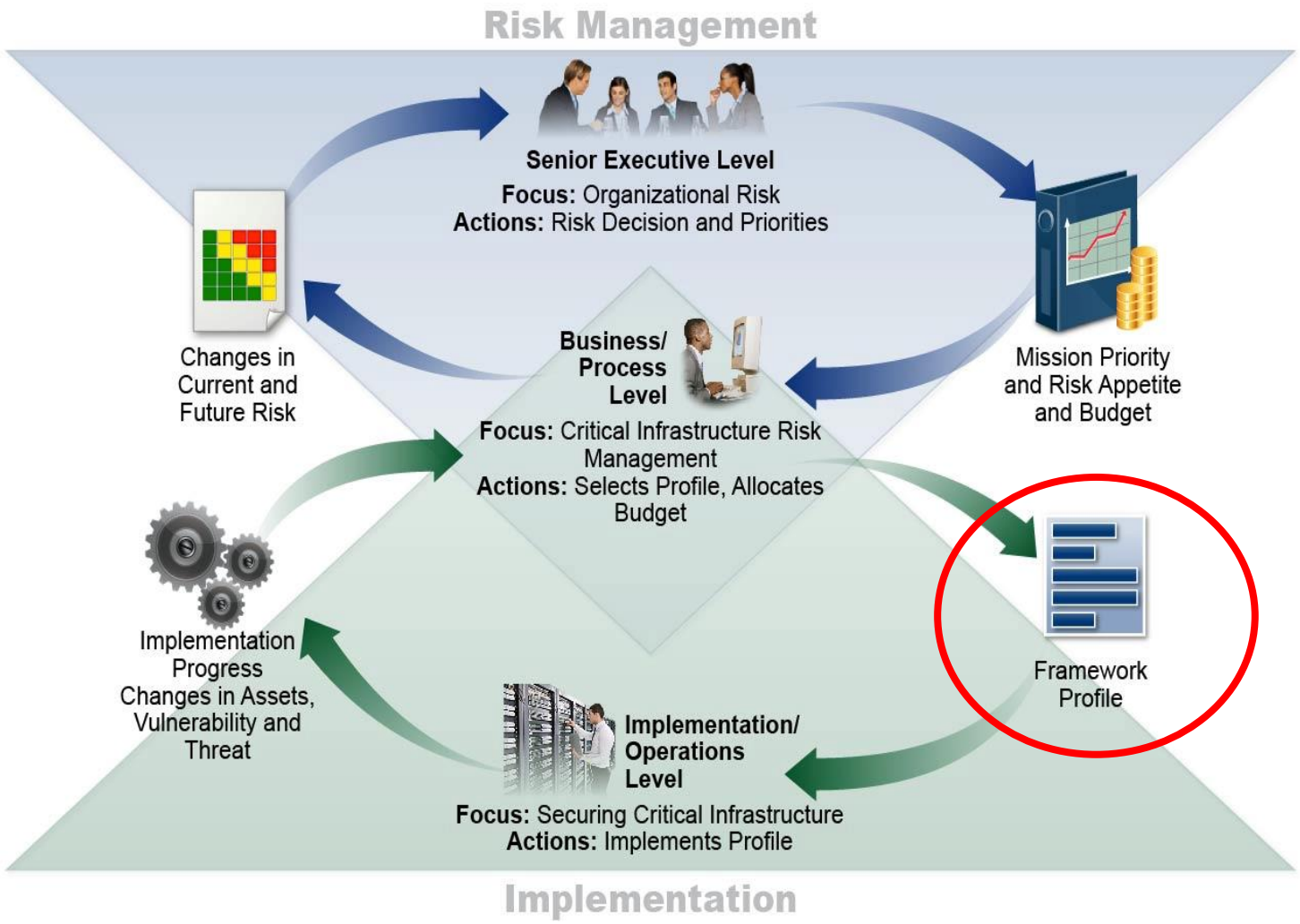
Year 2 Activities

Subcategory 1

Subcategory 5

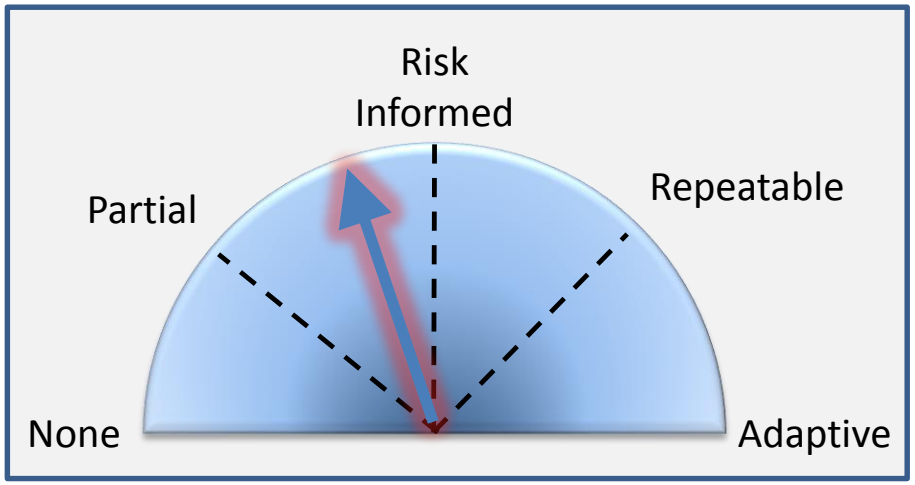
Subcategory 6

Using Profiles to Communicate Priorities



Implementation Tiers

Cybersecurity Framework Component



- Allow for flexibility in implementation and bring in concepts of maturity models
- Reflect how an organization implements the Framework Core functions and manages its risk
- Progressive, ranging from Partial (Tier 1) to Adaptive (Tier 4), with each Tier building on the previous Tier
- Characteristics are defined at the organizational level and are applied to the Framework Core to determine how a category is implemented.

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

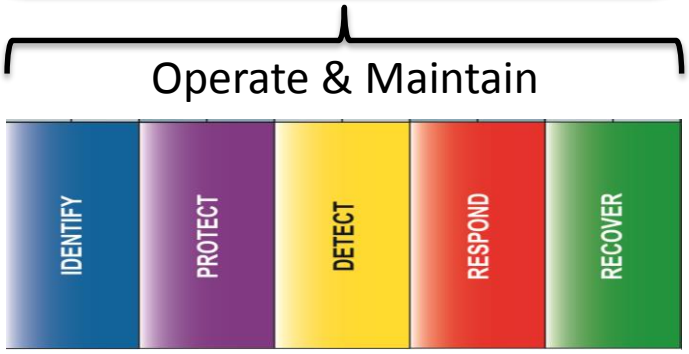
- **The framework is a living document**
  - It is intended to be updated over time as stakeholders learn from implementation, and as technology and risks change
  - That's one reason why the framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, 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.

Key Questions for New Technologies

Overarching Question	Question	Who	Decision Materials
Proceed?	Will implementing the technology help me fulfill mission priorities?	Mission	ID.BE-3
	Will implementing the technology adversely affect the mission function of my current systems?	Technology	ID.AM-5
	Will implementing the technology introduce untenable risk?	Cyber Security	ID.RM-2/Profile *Inherent risks*
Proceed now?	Is it possible to implement this technology given my current infrastructure?	Technology	ID.AM-1, 2, & 3
	How can I minimize risk associated with this new technology: • in a way that supports my organization's requirements, and • within my finite budget?	Cyber Security	ID.RM-2/Profile *Inherent risks*
	How much security is 'enough' to implement this new technology?	Cyber Security	ID.RM-2/Profile
Hand-off to operations	What do I need to do to ensure on-going risk management of this new technology?	Cyber Security	*Remaining Categories*

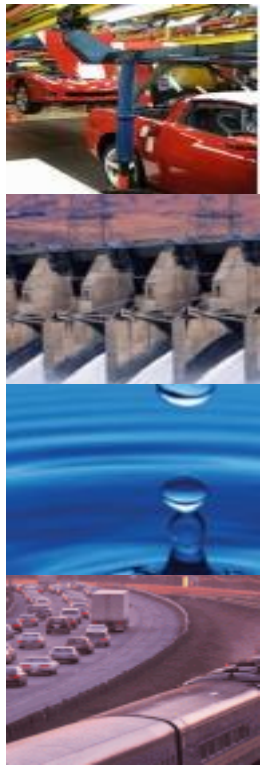
Industry Use

The Framework is designed to complement existing business and cybersecurity operations, and has been used to:

- Self-Assessment, Gap Analysis, Budget & Resourcing Decisions
- Standardizing Communication Between Business Units
- Harmonize Security Operations with Audit
- Communicate Requirements with Partners and Suppliers
- Describe Applicability of Products and Services
- Identify Opportunities for New or Revised Standards
- Categorize College Course Catalogs
- As a Part of Cybersecurity Certifications
- Categorize and Organize Requests for Proposal Responses
- Consistent dialog, both within and amongst countries
- Common platform on which to innovate, by identifying market opportunities where tools and capabilities may not exist today

Current & Near-Term Framework Activities

Collect, **Reflect**, and **Connect** – understand where industry is having success, help others understand those successes, and facilitate relationships that support use and implementation



- Continue education efforts, including creation of self-help and re-use materials for those who are new to the Framework

- Continue awareness and outreach with an eye toward industry communities who are still working toward basal Framework knowledge and implementation

- Educate on the relationship between Framework and the larger risk management process, including how organizations can use Tiers

Since the Release of the Cybersecurity Framework…

Request for Information: Experience with the Cybersecurity Framework
Questions focused on: awareness, experiences, and roadmap areas

August 26, 2014

6th Cybersecurity Framework Workshop
Goal: Raise awareness, encourage use as a tool, highlight examples of sector-specific efforts, implementation efforts, gather feedback

Oct. 29-30, 2014
Florida Center for Cybersecurity

Update on the Cybersecurity Framework
Summary posted that includes analysis of RFI responses, feedback from the 6th workshop, an update on Roadmap areas, and next steps

December 5, 2014

February 13, 2015
White House Releases Fact Sheet on Cybersecurity and Consumer Protection

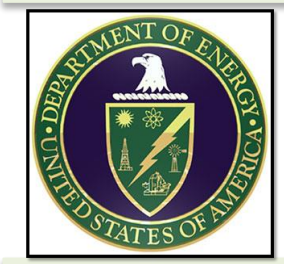
1 Year Anniversary of the Release
NIST Cybersecurity Framework site update to include: FAQs, Upcoming Events, and Industry Resources. Ongoing, targeted outreach continues

February 12, 2015

Examples of Industry Resources

The Cybersecurity Framework in Action: An Intel Use Case

Cybersecurity Guidance for Small Firms



Energy Sector Cybersecurity Framework Implementation Guidance

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

CFORUM and other online communities of interest

On-Going NIST Community Dialogs

- Standards Organizations
  - British Standards Institute, Cloud Security Alliance, AXELOS, etc.
- Domestic Industry
  - Not only Critical Infrastructure, but also Non-CI
  - Product and Services
- Regulator
  - Every Federal Financial Services regulator
- Auditor
  - Information Systems Audit and Control Association
  - “The Big 4” Audit Firms
- Insurance
- Legal

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

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

International Dialogs

Twenty four (24) countries have participated in discussion with NIST, including dialog with:

- The European Union, and 11 out of 28 Member States
- 4 out of 5 of the Five Eyes
- 5 countries in Asia
- 4 countries in the Middle East
- The U.S. and the U.K. continue the dialog about harmonizing the U.K. Cyber Essentials with the Cybersecurity Framework
- And three additional Nations next week!

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

Standards/Guidelines for FISMA & RM

FIPS - Federal Information Processing Standards

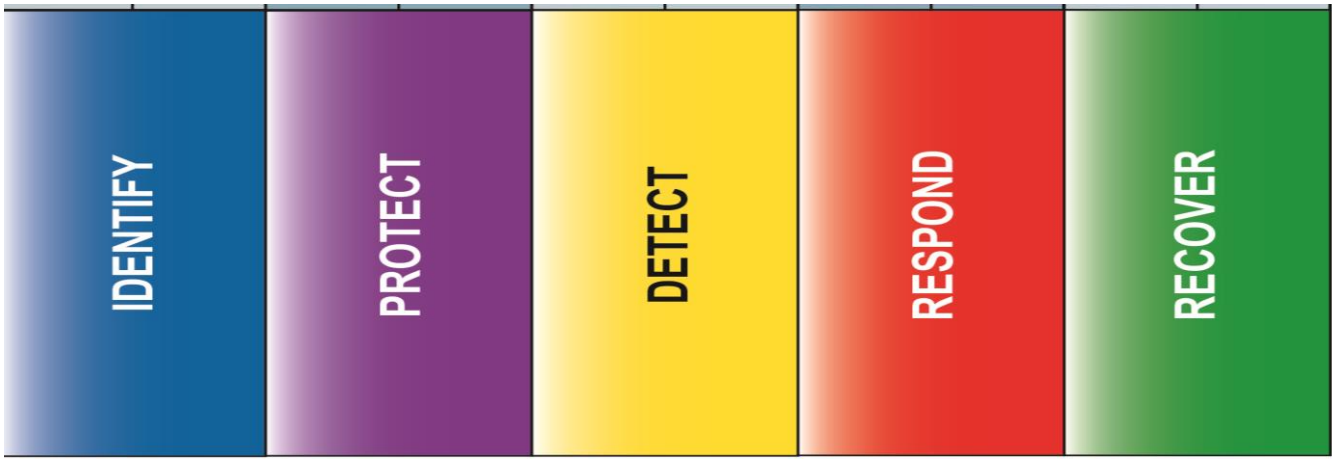
- FIPS 199 – Standards for Security Categorization
- FIPS 200 – Minimum Security Requirements

SPs – Special Publications

- SP 800-18 – Guide for System Security Plan development
- **SP 800-30 – Guide for Conducting Risk Assessments**
- SP 800-34 – Guide for Contingency Plan development
- **SP 800-37 – Guide for Applying the Risk Management Framework**
- **SP 800-39 – Managing Information Security Risk**
- **SP 800-53/53A – Security controls catalog/assessment procedures**
- SP 800-60 – Mapping Information Types to Security Categories
- SP 800-128 – Security-focused Configuration Management
- SP 800-137 – Information Security Continuous Monitoring
- Many others for operational and technical implementations

Organizing and Communicating SP 800-53 Security Controls

Use Case for FISMA-Cybersecurity Framework Combined Use



SP 800-53 security controls
CobIT controls
ISO 27002 controls
Etc…

Supporting the RMF Categorize Step

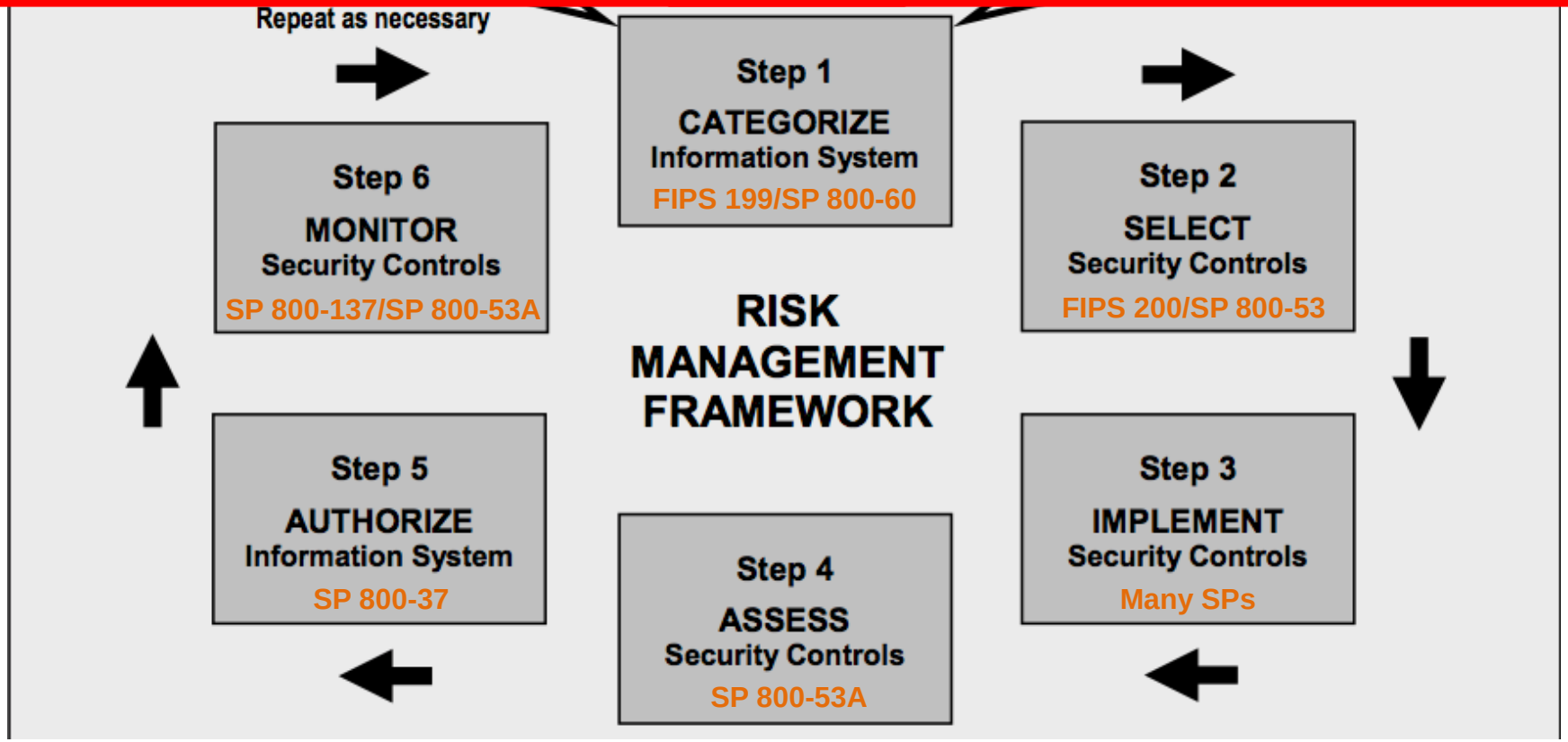
Profile

A sector, subsector, or organization's cu
of the Core for their purposes. Aligns,
conflicts in organizational inputs, and
cyber objectives commensurate with
objectives

Category

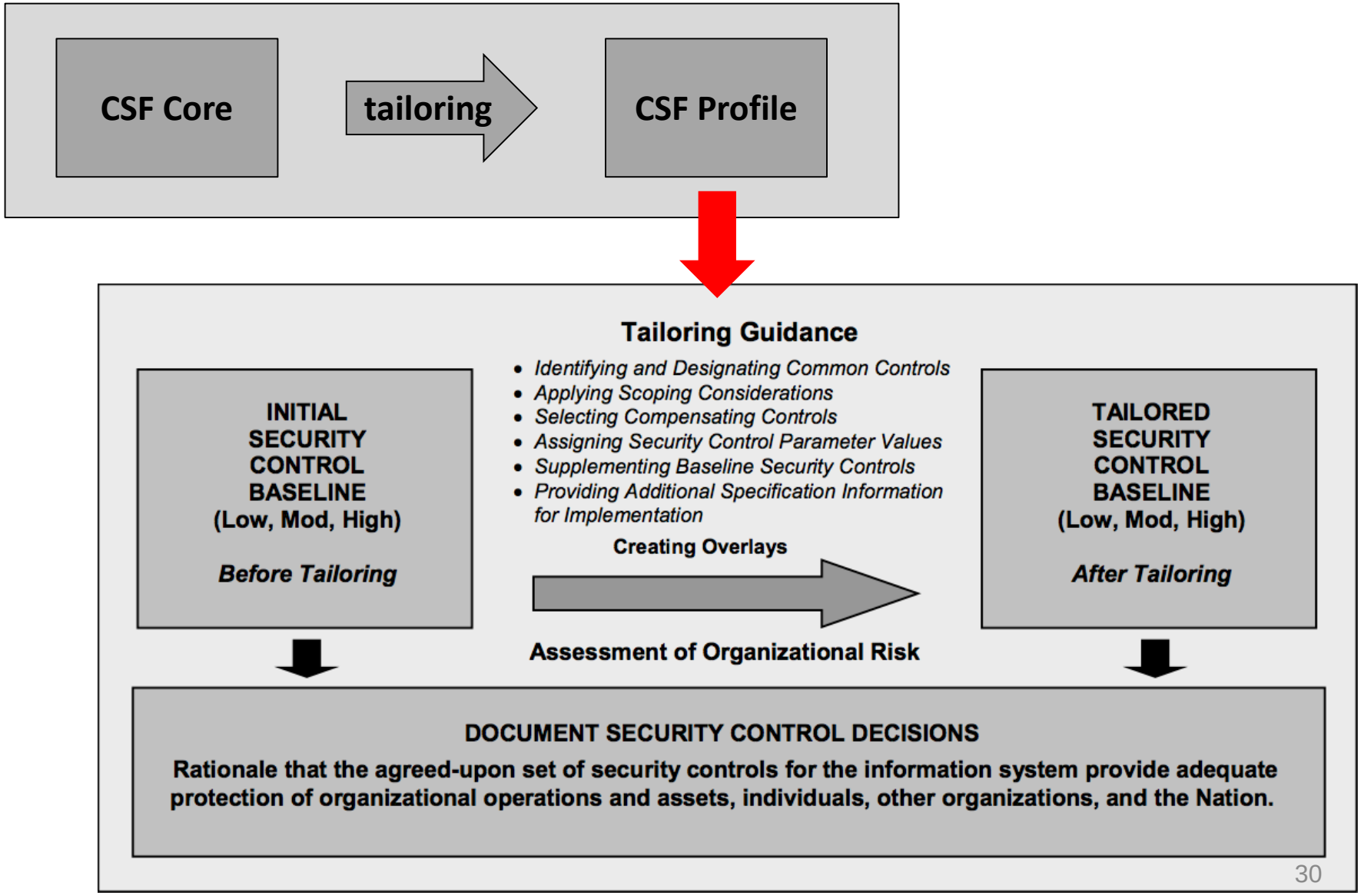
Business Environment (ID.BE)

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.



Tailoring SP 800-53 Security Controls

Use Case for FISMA-Cybersecurity Framework Combined Use



Industry Dialog

Will it soon be time for a Framework update?

What governance models do you believe will work for future Framework maintenance and evolution?

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