Framework for Improving Critical Infrastructure Cybersecurity

April 2016

cyberframework@nist.gov

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

Pre-Cybersecurity Framework Threat Landscape

- 79% of reported victims were targets of opportunity
- 96% of reported attacks in 2012 were NOT difficult
- 85% of reported breaches took weeks or more to discover
- 97% of reported breaches were avoidable through simple or intermediate controls

Statistics are from the 2012 Verizon Data Breach Investigative Report

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"

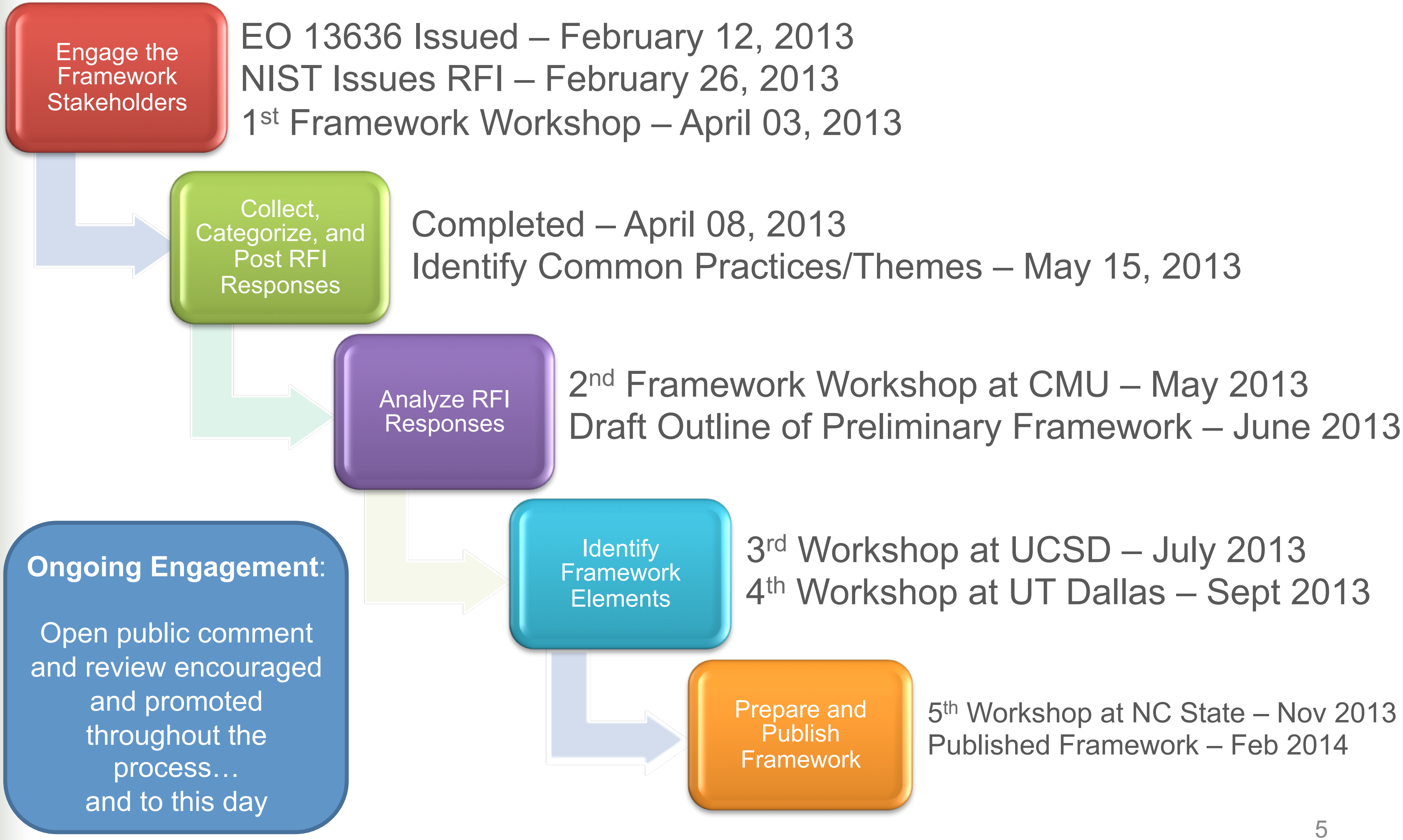
President Barack Obama

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

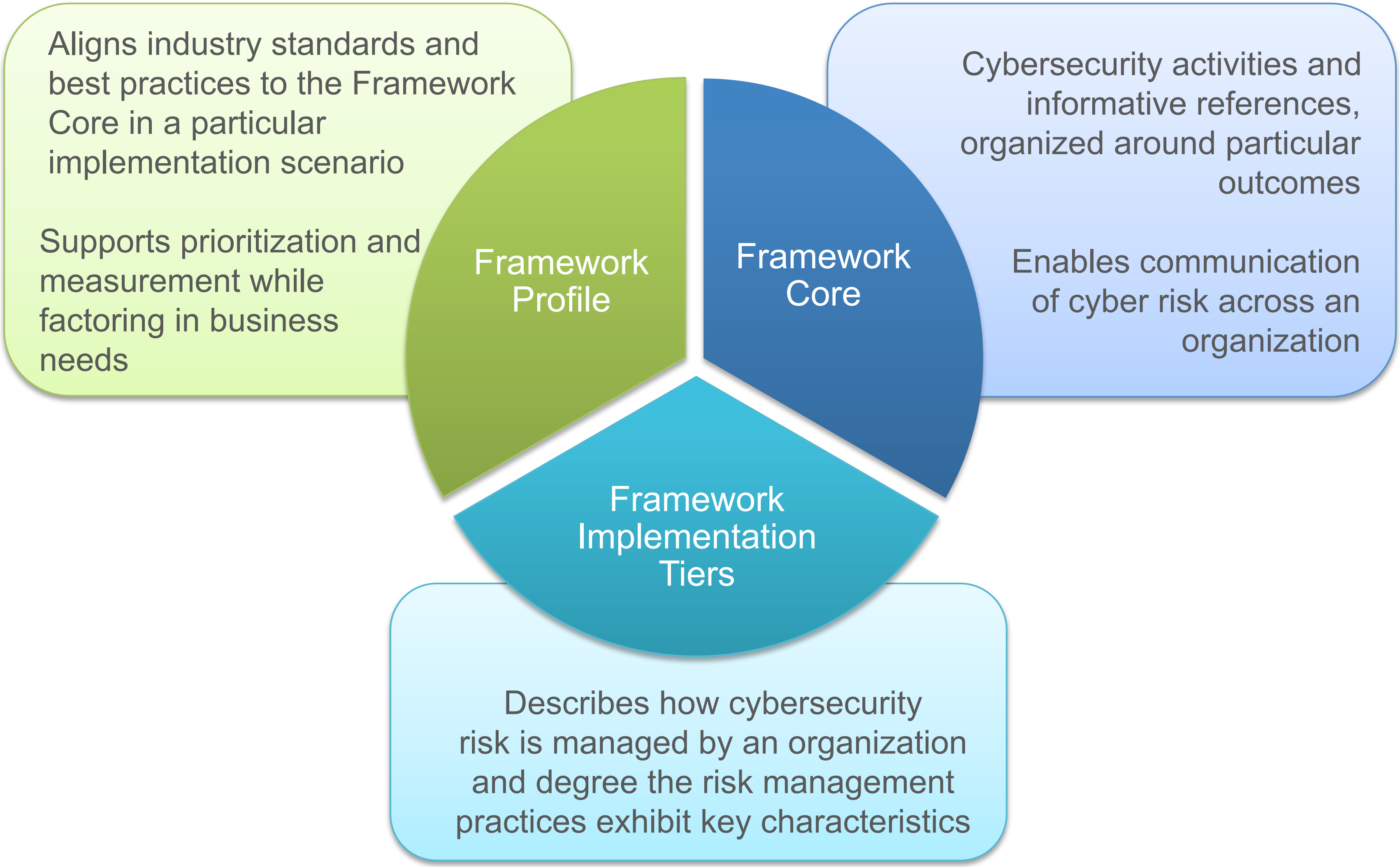
Ongoing Engagement:

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

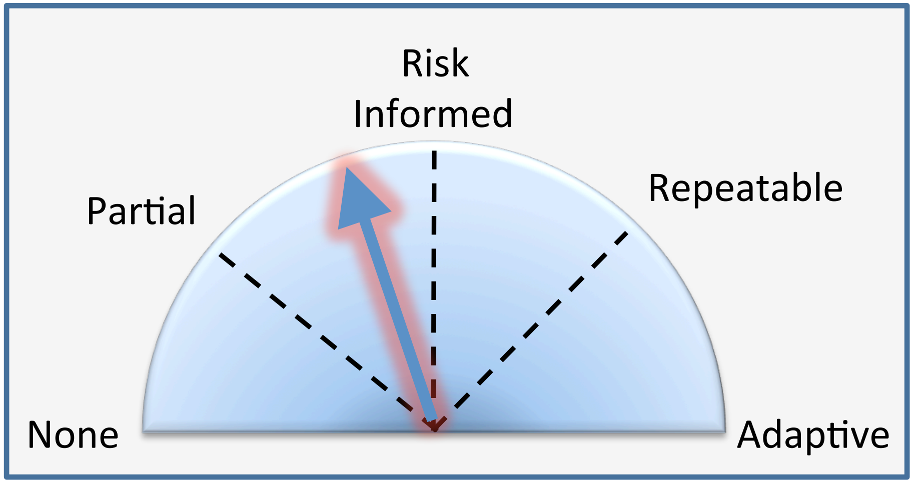
Enables communication of cyber risk across an organization

Framework Implementation Tiers

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

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.

Implementation Tiers

Cybersecurity Framework Component

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

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:** ......

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

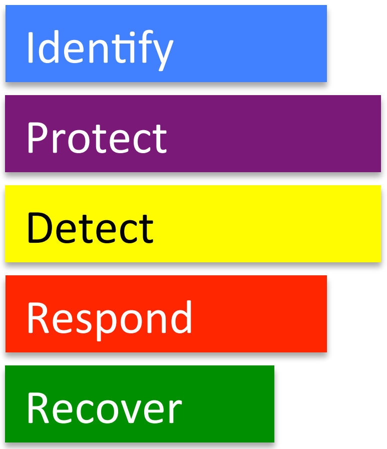
Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & 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:



Identify

Protect

Detect

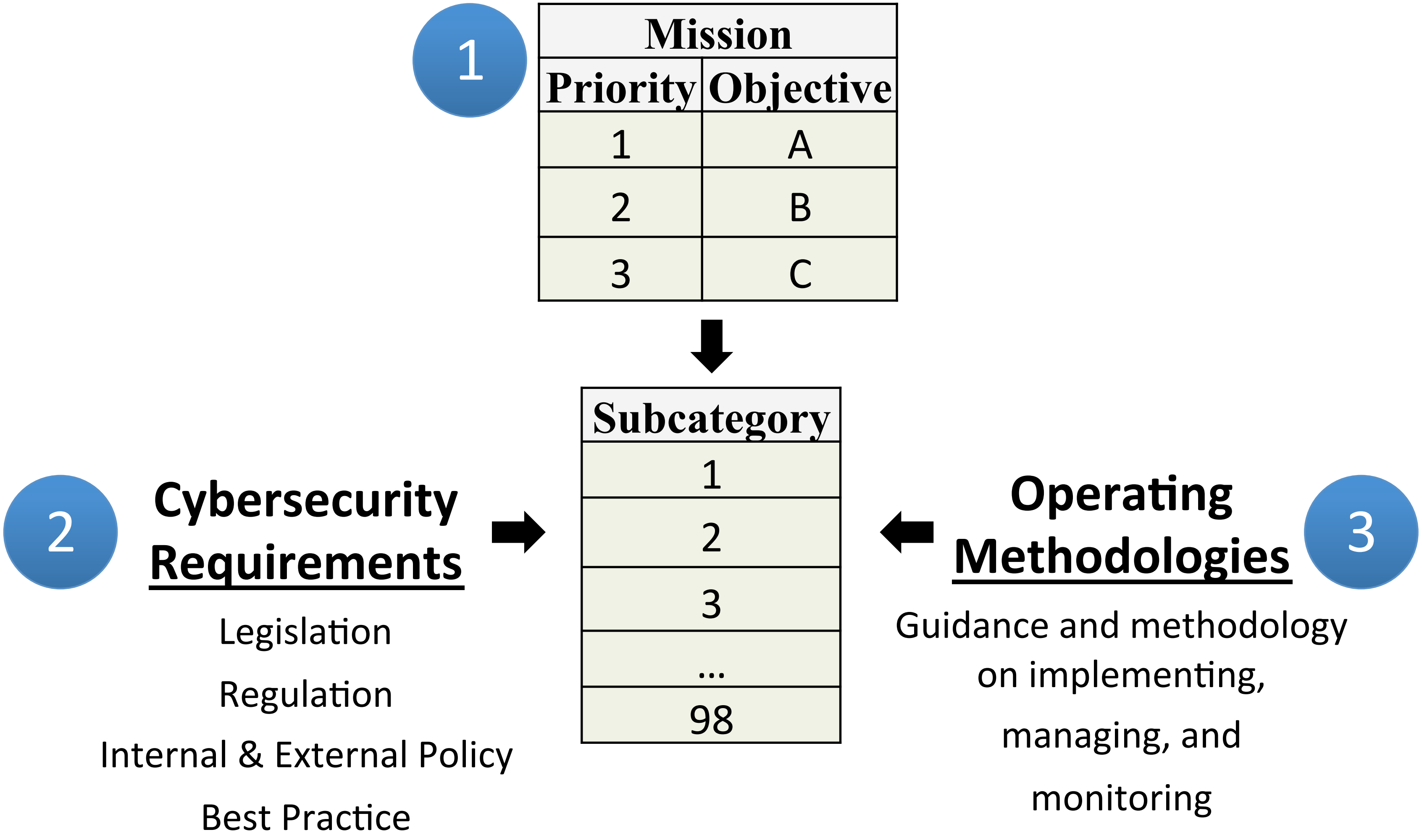
Respond

Recover

- 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

Building a Profile

A Profile Can be Created in Three Steps



1

Mission	
Priority	Objective
1	A
2	B
3	C

Subcategory
1
2
3
…
98

2

Cybersecurity Requirements

Legislation

Regulation

Internal & External Policy

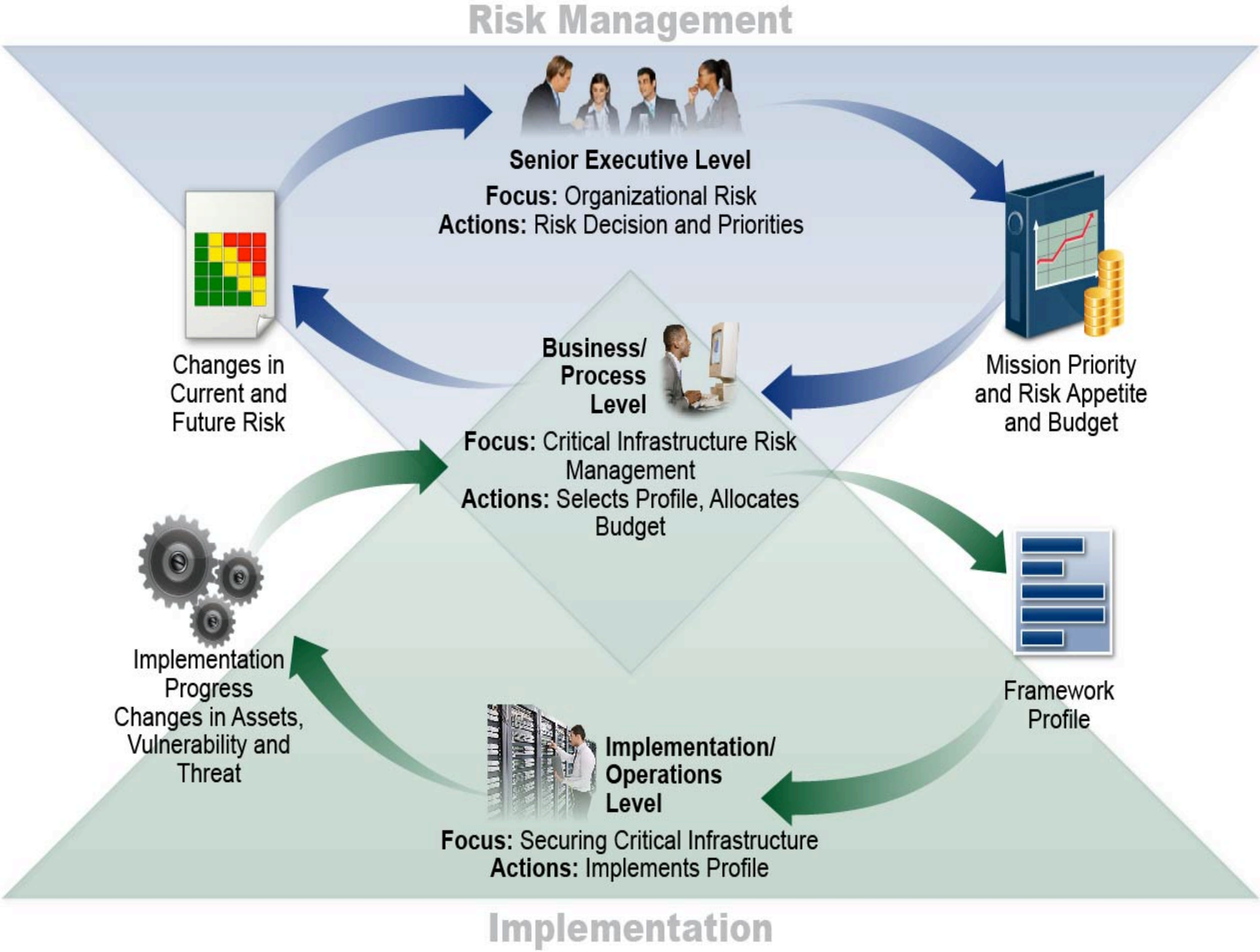
Best Practice

3

Operating Methodologies

Guidance and methodology on implementing, managing, and monitoring

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

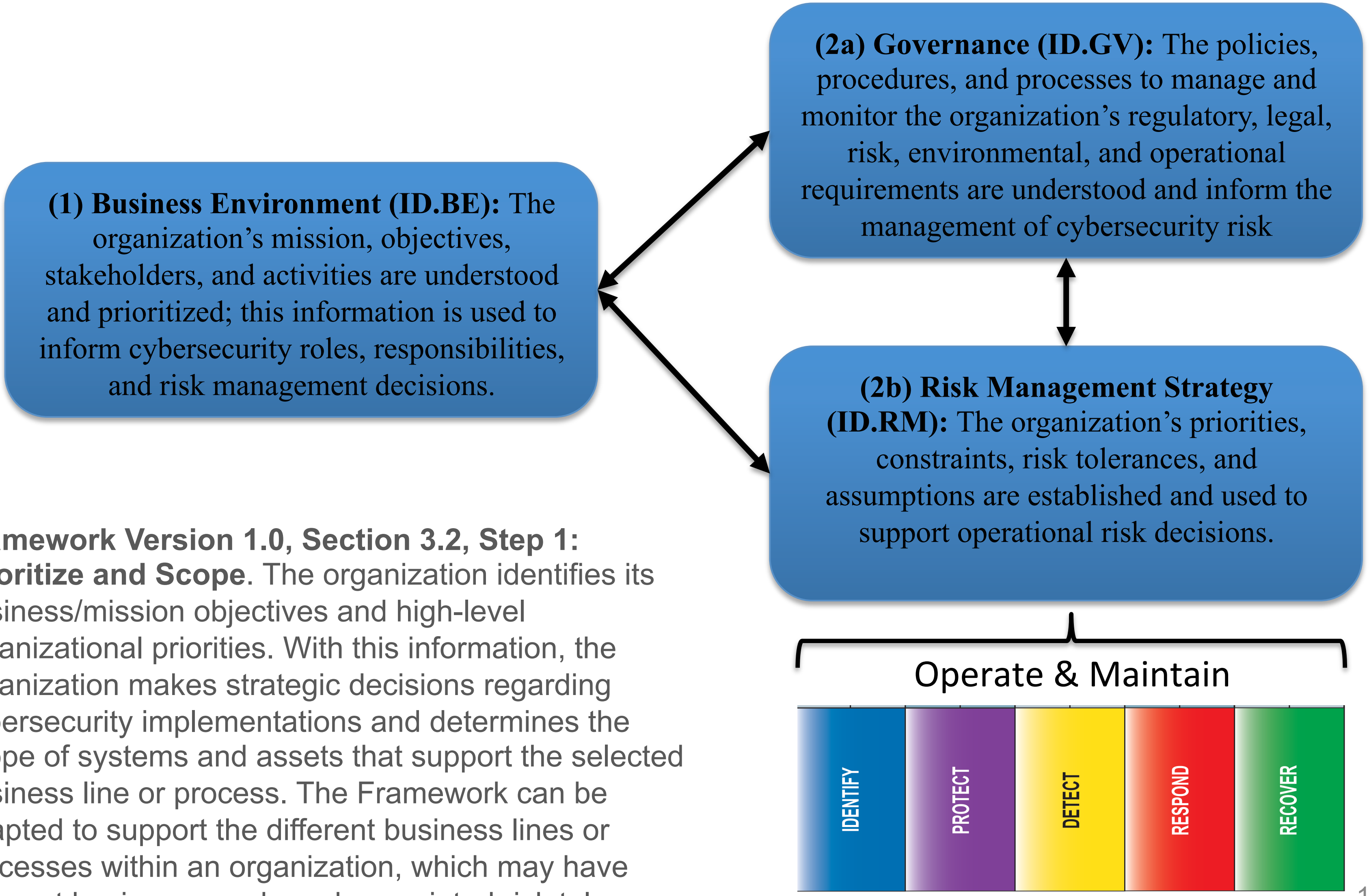
Implementation

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.

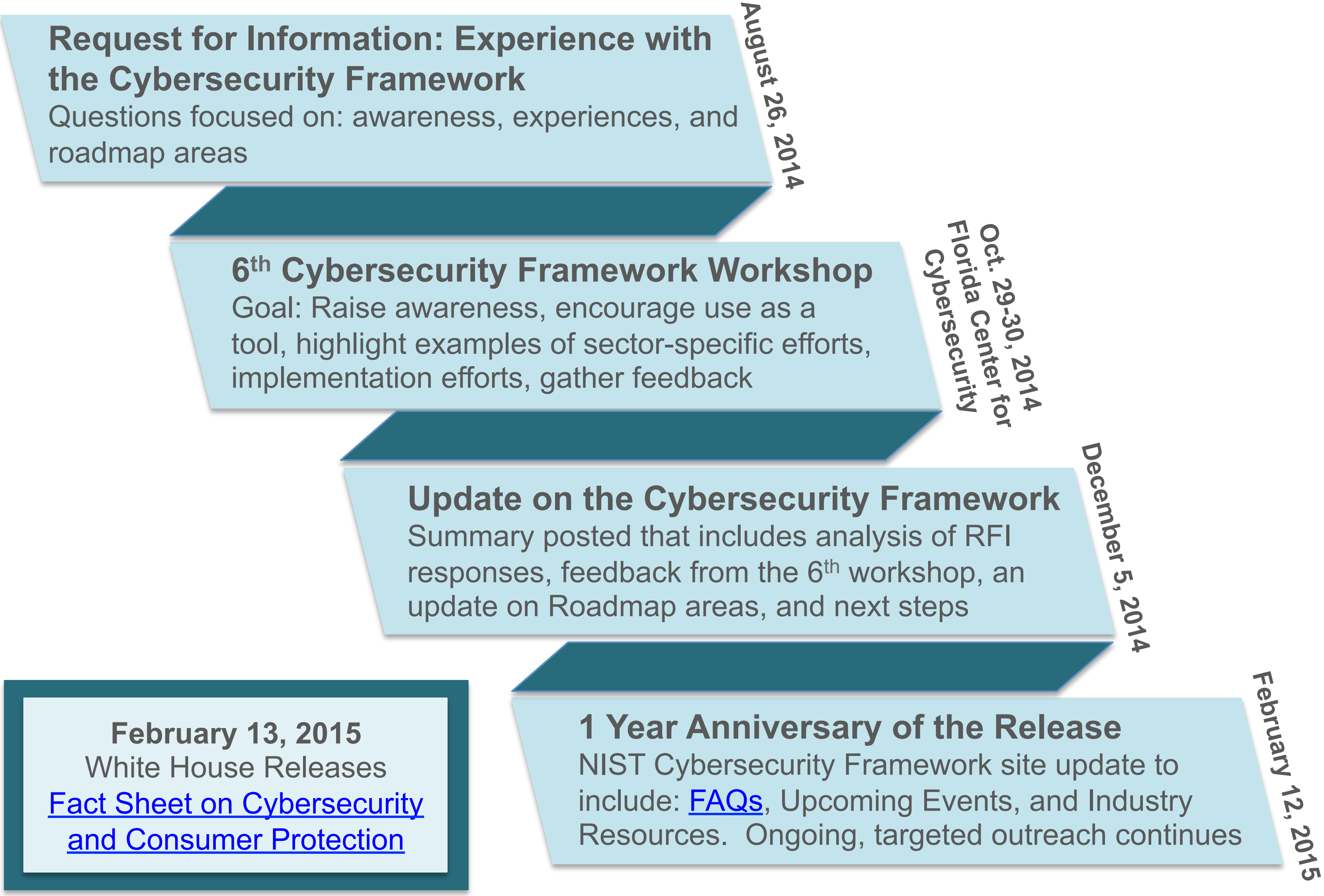
Framework Version 1.0, Section 3.2, Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of 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.

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

Framework – One Year After Release



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

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

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

Examples of Industry Resources

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

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

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

Recent Framework Related Policy and Legislation

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

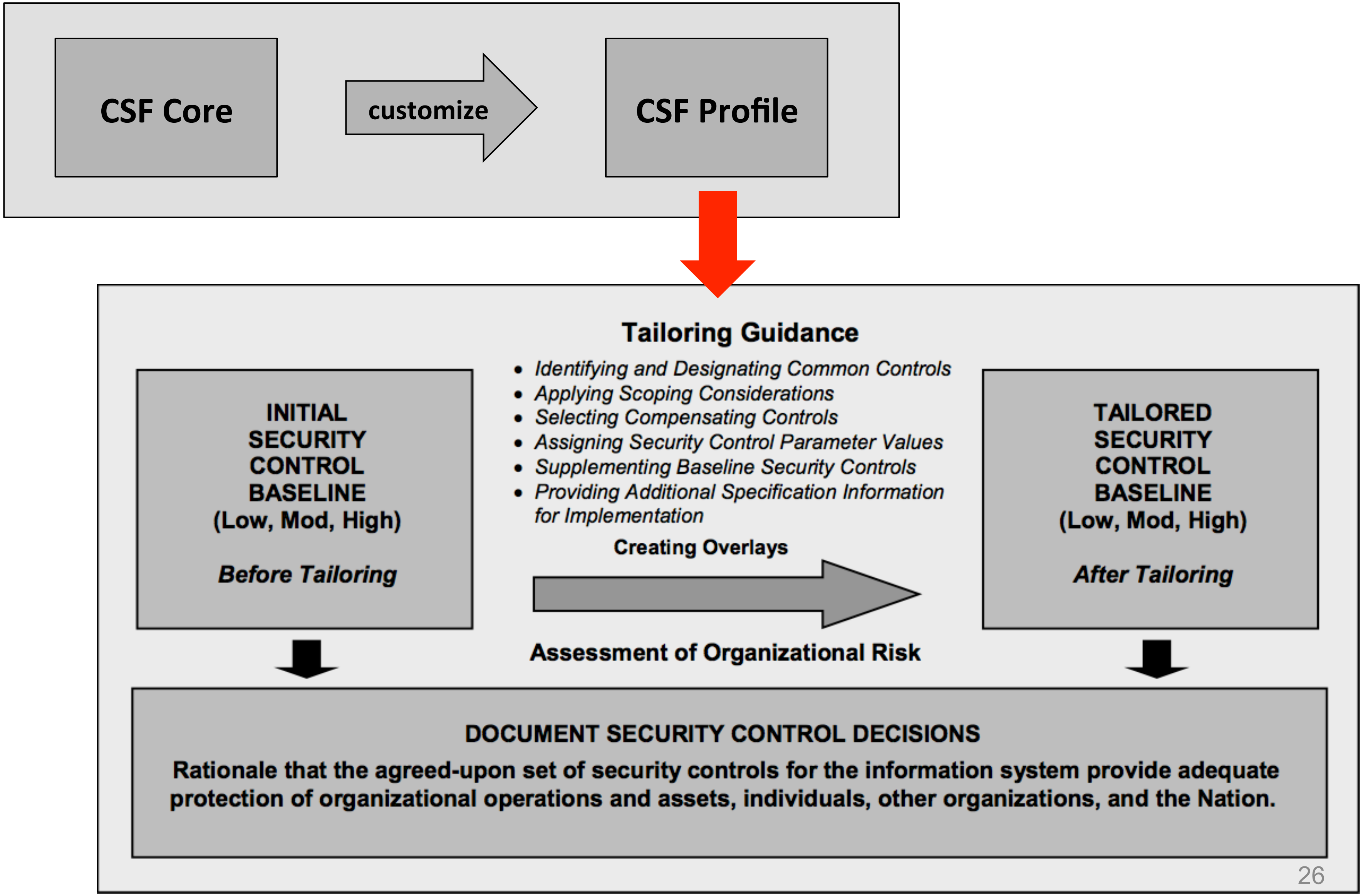
- M-16-03: FY 2015-16 Guidance on Federal Information Security and Privacy Management Requirements
- M-16-04: Cybersecurity Strategy and Implementation Plan

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

Tailoring SP 800-53 Security Controls

Use Case #3 for Risk Management Framework & Cybersecurity Framework



CSF Core

customize

CSF Profile

Tailoring Guidance

- *Identifying and Designating Common Controls*
- *Applying Scoping Considerations*
- *Selecting Compensating Controls*
- *Assigning Security Control Parameter Values*
- *Supplementing Baseline Security Controls*
- *Providing Additional Specification Information for Implementation*

Creating Overlays

INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)

Before Tailoring

TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)

After Tailoring

Assessment of Organizational Risk

DOCUMENT SECURITY CONTROL DECISIONS

Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.

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 eight (28) countries have participated in discussion with NIST, including dialog with:

- The European Union, and 14 out of 28 Member States
- 4 out of 5 of the Five Eyes
- 6 countries in Asia
- 5 countries in the Middle East

Emerging International Use - Italy

Italy’s ***National Framework for Cybersecurity***:

- http://www.cybersecurityframework.it/
- Adopted 100% of the NIST Cybersecurity Framework
- Extended NIST Cybersecurity Framework
- Created with industry and academia
- Published in both Italian and English

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