Framework for Improving Critical Infrastructure Cybersecurity

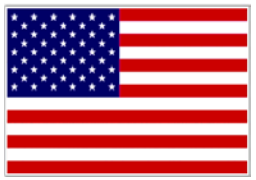
March 2018

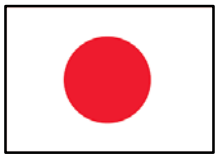
cyberframework@nist.gov

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

Cybersecurity Framework Use

Framework for Improving Critical Infrastructure Cybersecurity





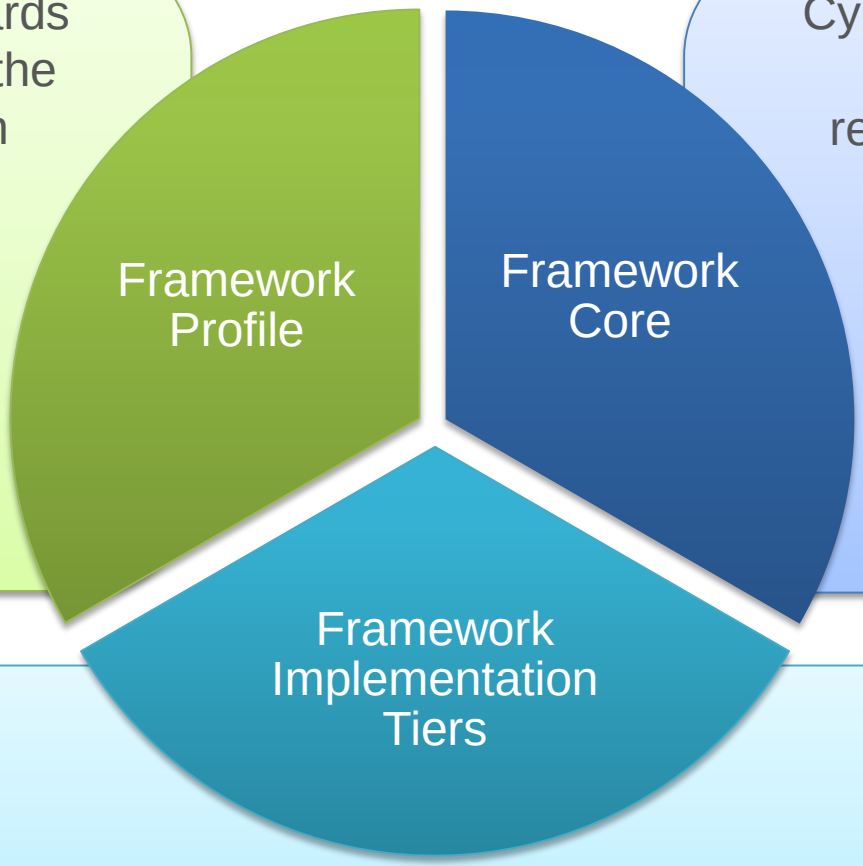
NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

AT&T

Cybersecurity Framework Components

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

Supports prioritization and measurement while factoring in business needs



Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

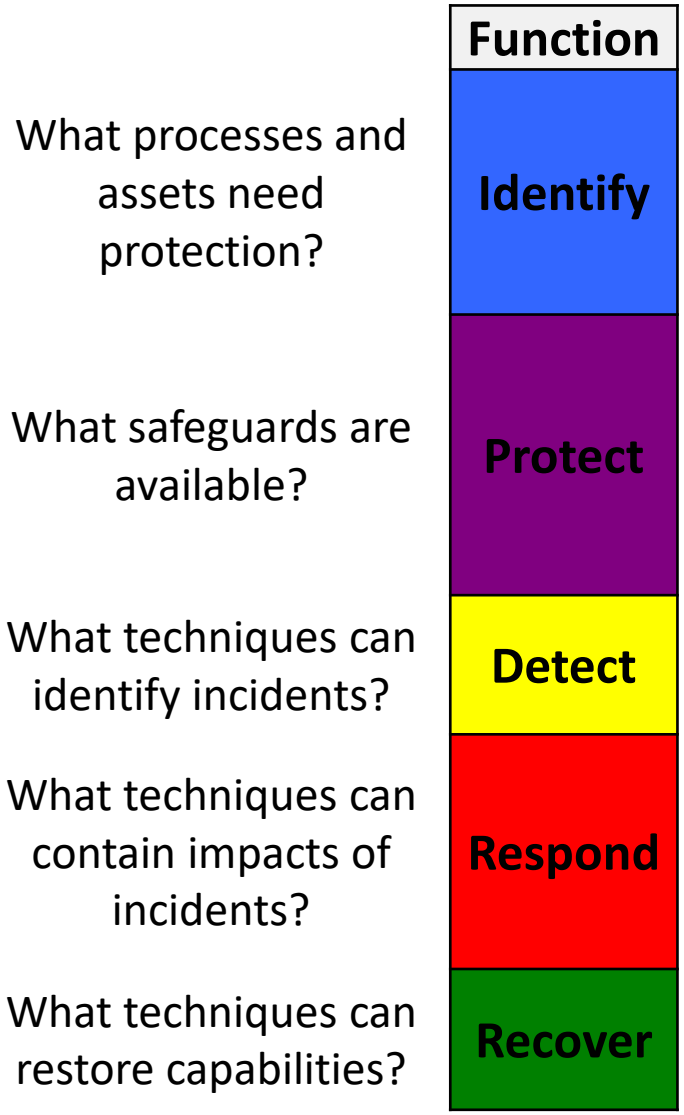
Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

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



- 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

7

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	• **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	• **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	• **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

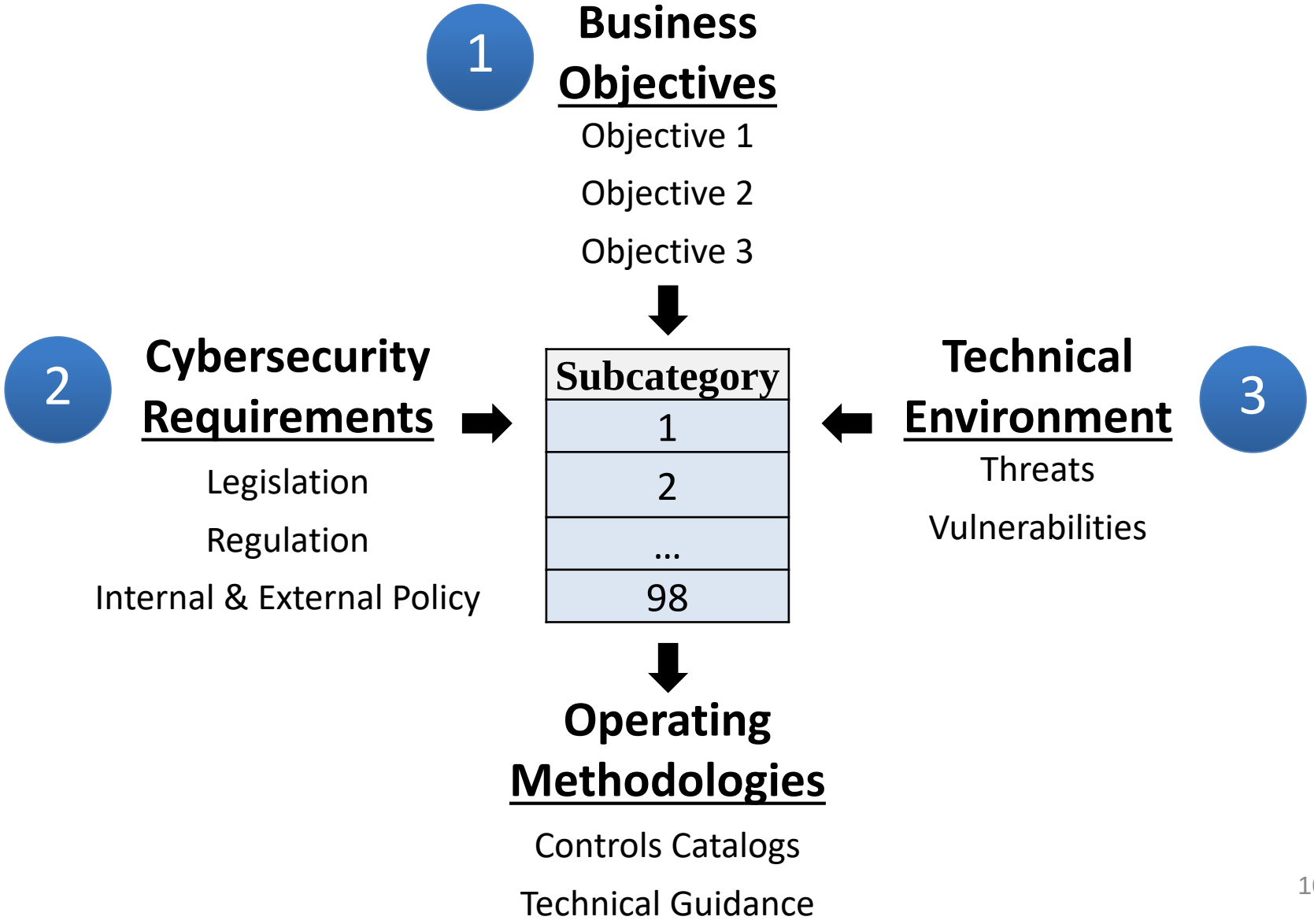
Cybersecurity Framework Component

Ways to think about a Profile:

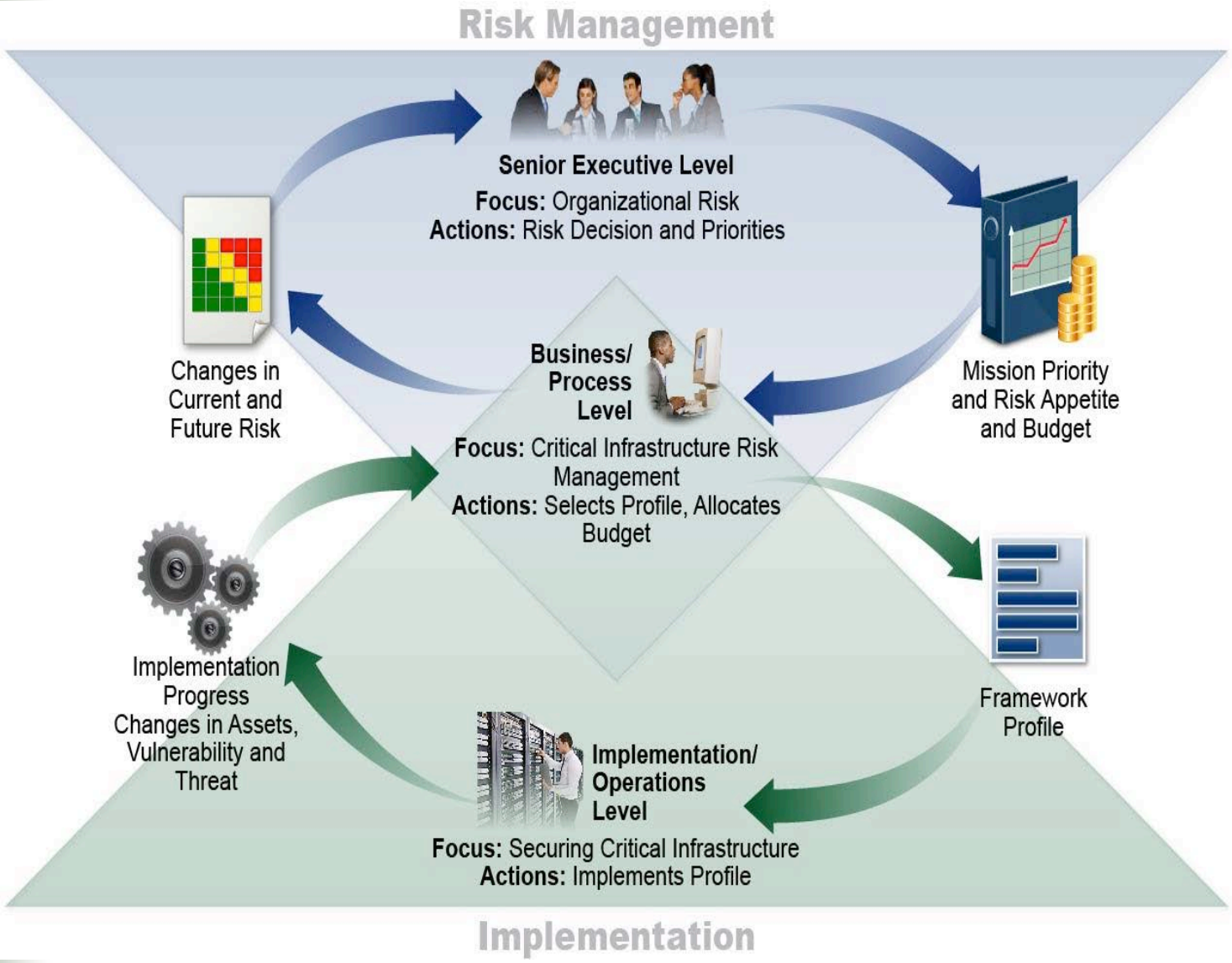
- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity risk management

Profile Foundational Information

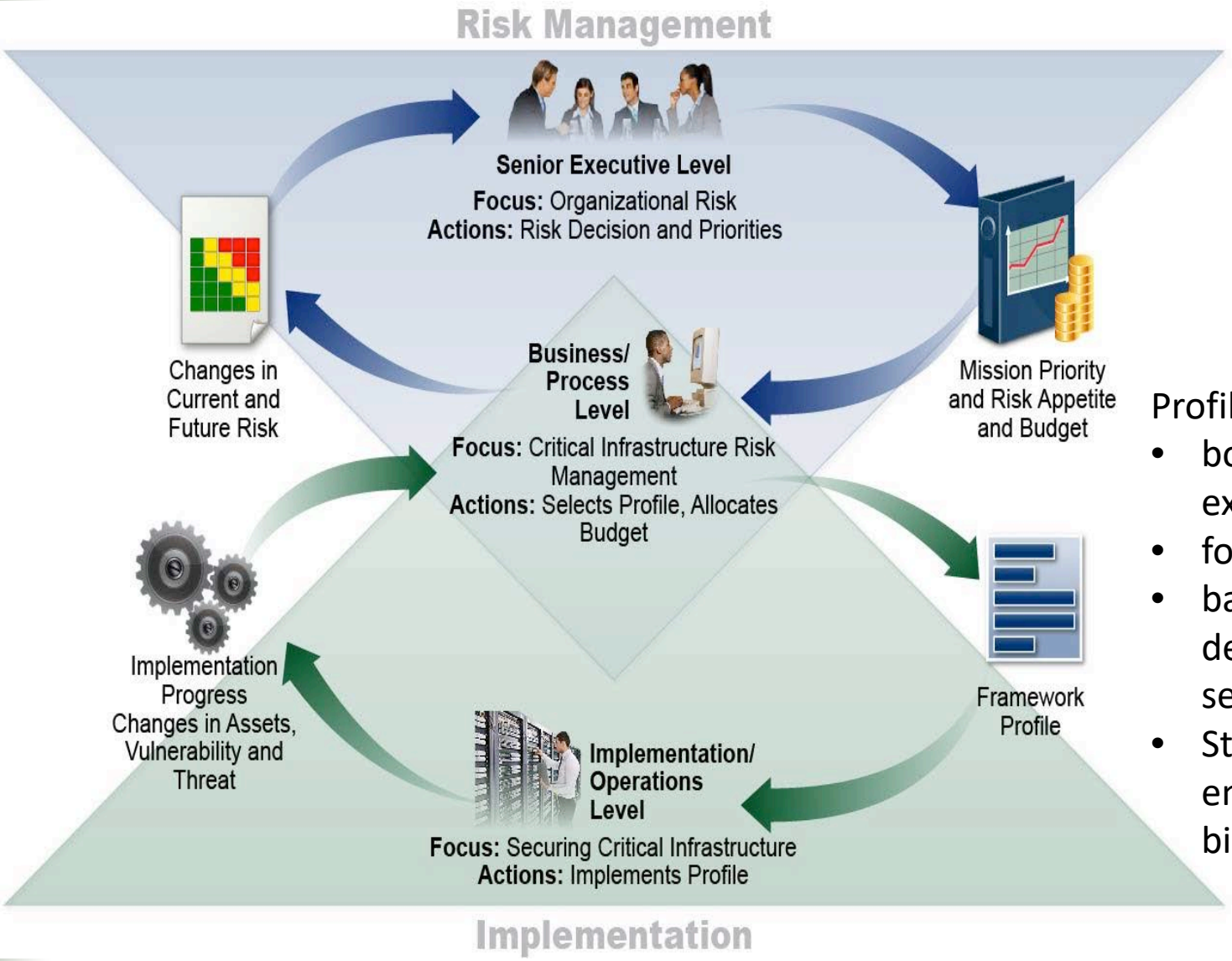
A Profile Can be Created from Three Types of Information



Supporting Risk Management with Framework



Supporting Risk Management with Framework



Profiles are used:

- both internal and external
- for gap analysis
- basis for rational and defensible time sequencing
- Structure for empowering/accountability

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)*

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*

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

COMMUNICATIONS SECTOR

- Federal Communications Commission (FCC) Communications, Security, Reliabilit
  (CSRIC) Cybersecurity Risk Management and Best Practices Working Group 4: Fina

CRITICAL MANUFACTURING SECTOR

- Department of Homeland Security's Critical Manufacturing Sector Cybersecurity
  Guidance
- An Intel Use Case for the Cybersecurity Framework in Action
- NIST's Manufacturing Profile
  (A Manufacturing-Sector tailored approach to protecting against cyber risk)

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.**	800-63-3	Digital Identity Guidelines
		800-63A	Digital Identity Guidelines: Enrollment and Id
		800-63B	Digital Identity Guidelines: Authentication an Management
		800-63C	Digital Identity Guidelines: Federation and As
		800-46 Rev. 2	Guide to Enterprise Telework, Remote Access, Device (BYOD) Security

Over 100 Unique Resources for Your Understanding and Use!

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