Part I

Framework for Improving Critical Infrastructure Cybersecurity

September 2017

cyberframework@nist.gov

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

Cybersecurity Framework 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)

Why Cybersecurity Framework?

Cybersecurity Framework Uses

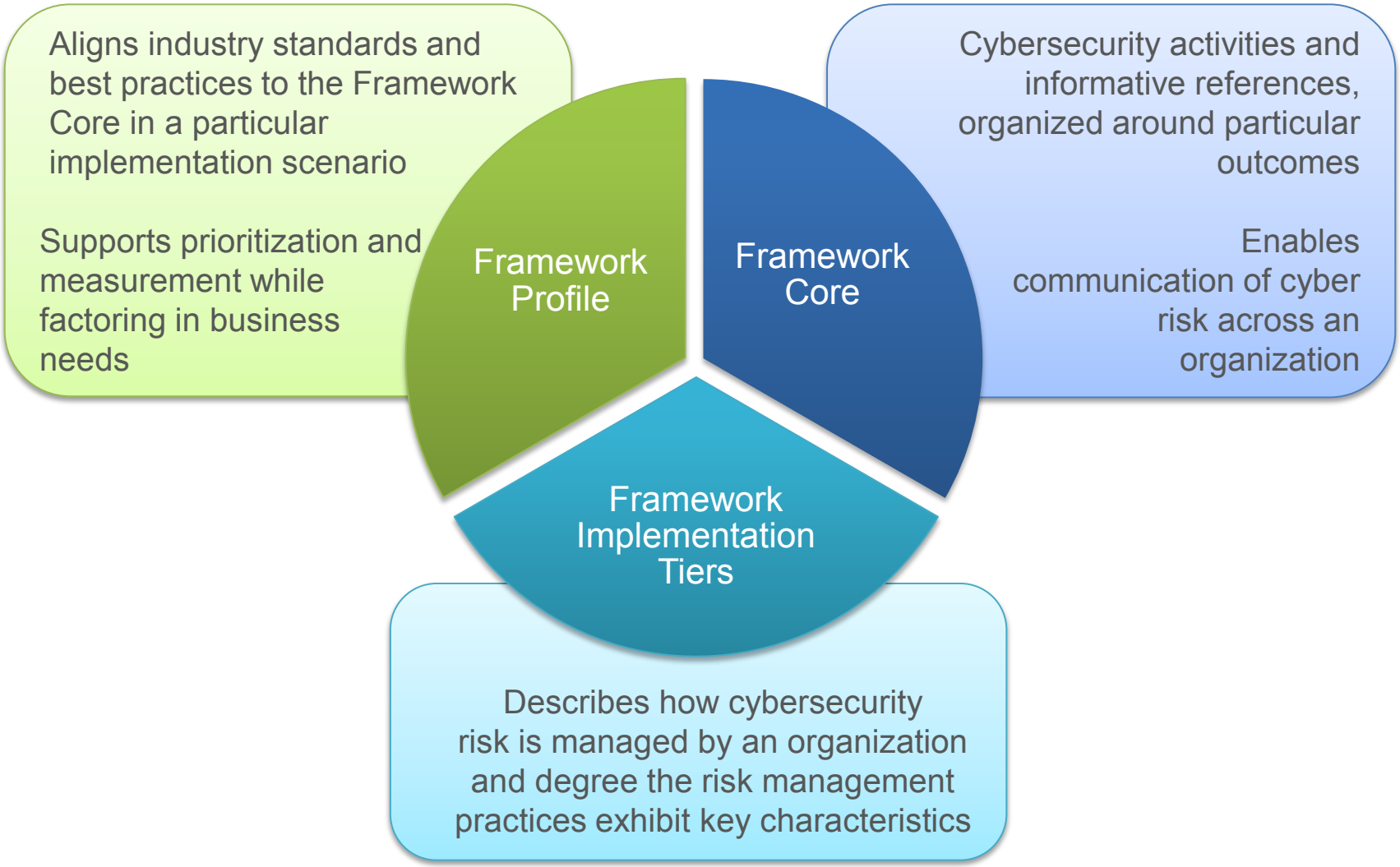
Who uses it?

- Inside of critical infrastructure
- Outside of critical infrastructure including:
  - State & local governments
  - U.S. federal agencies
  - Governments of other nations
- That have a mature cybersecurity risk management program
- That don't yet have a cybersecurity risk management program
- Of any size

What do they use it for?

- Identify affect of cybersecurity on business
- Align and de-conflict cybersecurity requirements
- Prioritize cybersecurity outcomes
- Organize, authorize, task, and track work
- Express risk disposition
- Understand gaps between current and target

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

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

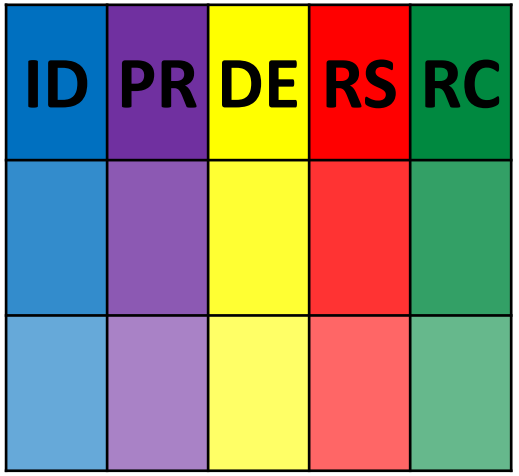
Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes &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

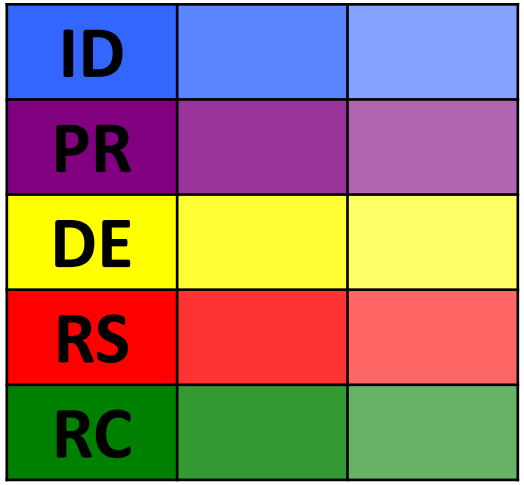
A Common Language

Foundational for Integrated Multi-Disciplinary Teams

Senior Executives



IT, Contracts, Marketing, Business Professionals



Cybersecurity Professionals

Highly technical and specialized language

Profile

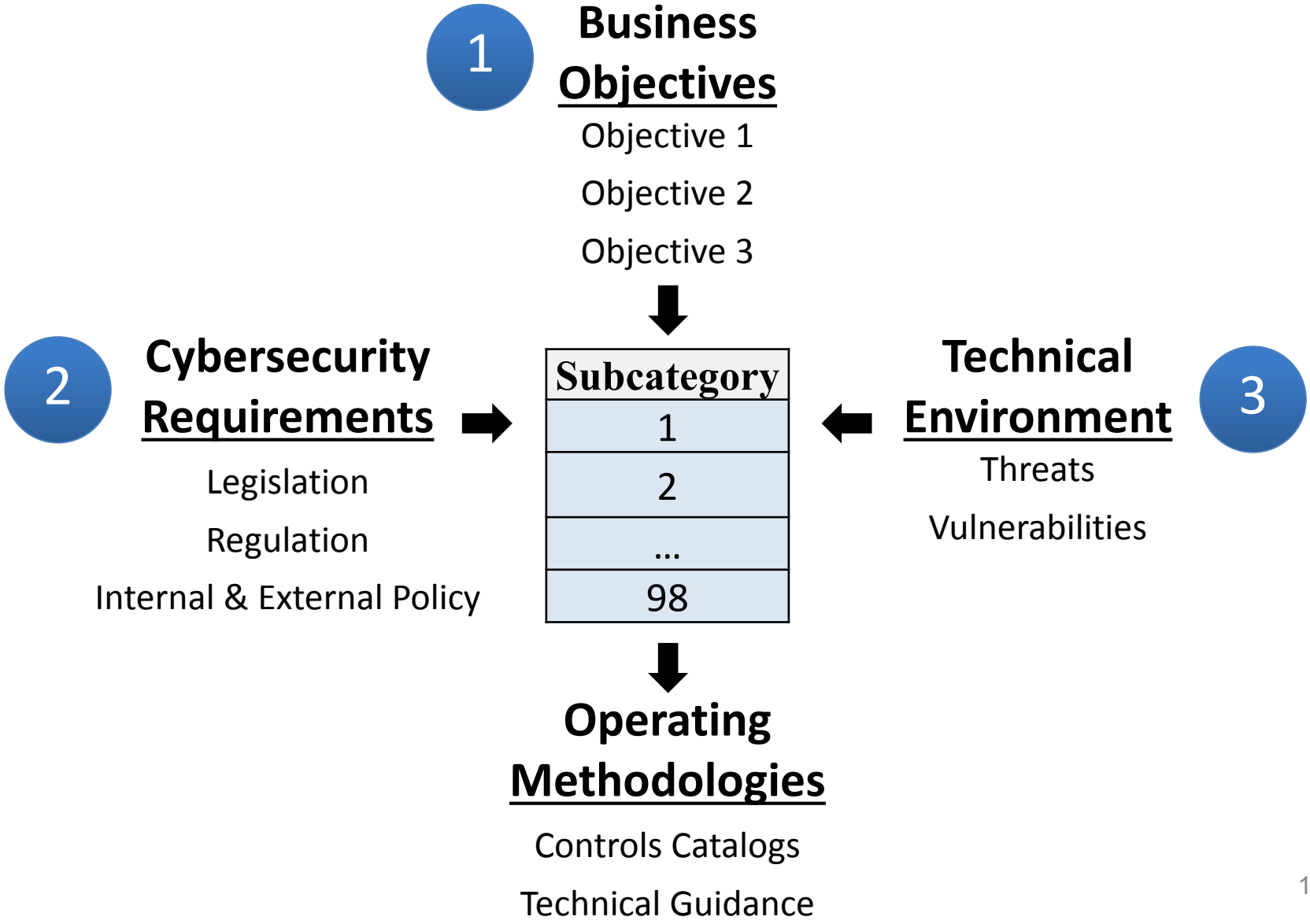
Cybersecurity Framework Component

Ways to think about a Profile:

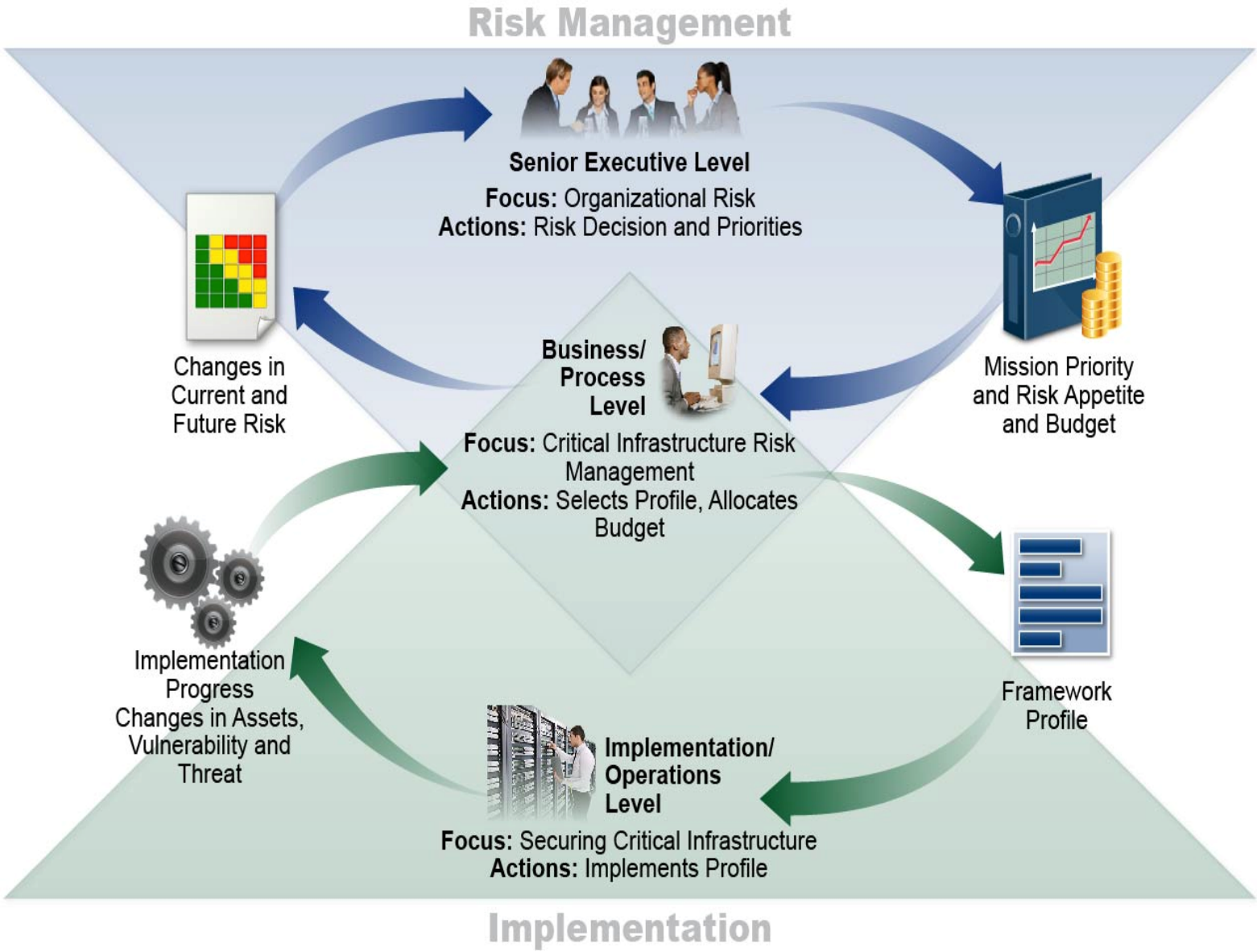
- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity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

Profile Foundational Information

A Profile Can be Created from Three Types of Information



Supporting Risk Management with Framework



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

…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

Key Attributes

It's voluntary

- Is meant to be *customized*.

It's a framework, not a prescriptive standard

- Provides a *common language* and systematic methodology for managing cyber risk.
- Does not tell an organization *how* much cyber risk is tolerable, nor provide "the one and only" formula for cybersecurity.
- Enable best practices to become *standard practices for everyone* via common lexicon to enable action across diverse stakeholders.

It's a living document

- Can be updated as stakeholders *learn from implementation*
- Can be updated as *technology and threats* changes.

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