Framework for Improving Critical Infrastructure Cybersecurity

October 2016

cyberframework@nist.gov

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

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"

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

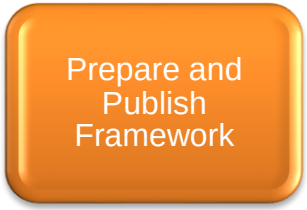
Development of the Framework

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

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

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

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

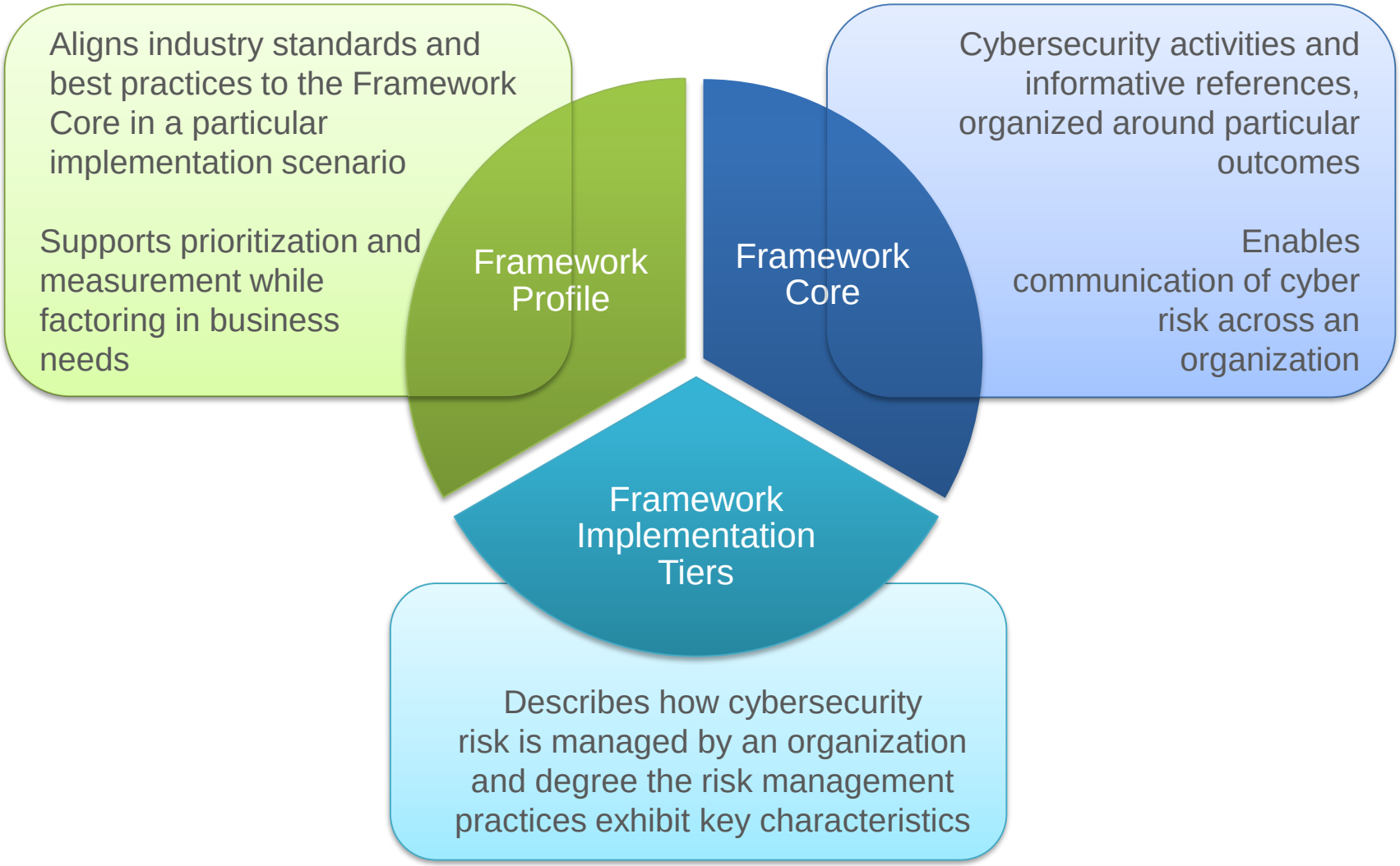


5th Workshop at NC State – Nov 2013
Published Framework – Feb 2014

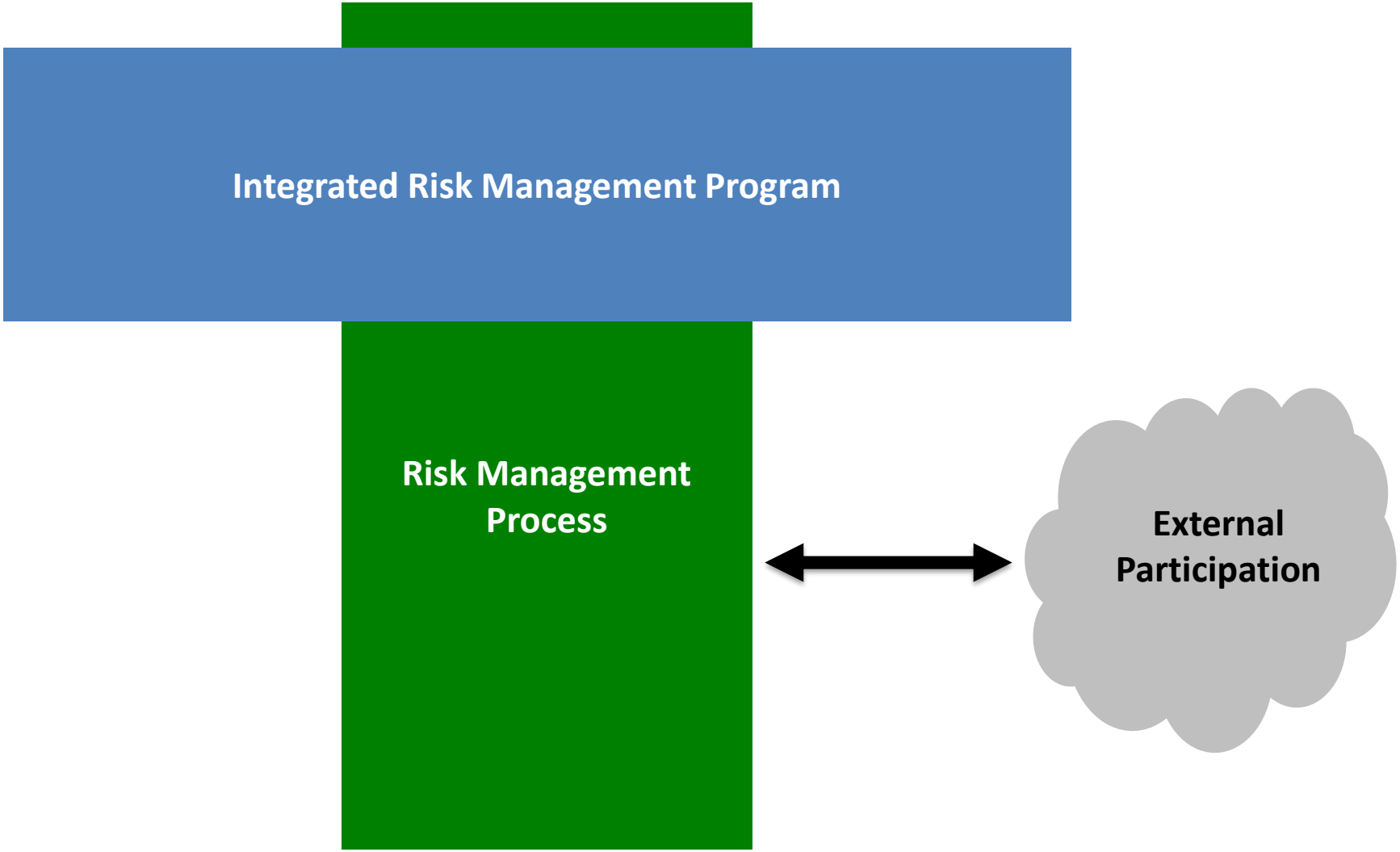
The Cybersecurity Framework Is for Organizations…

- 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



Key Properties of Cyber Risk Management



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			

Adaptation of Implementation Tiers

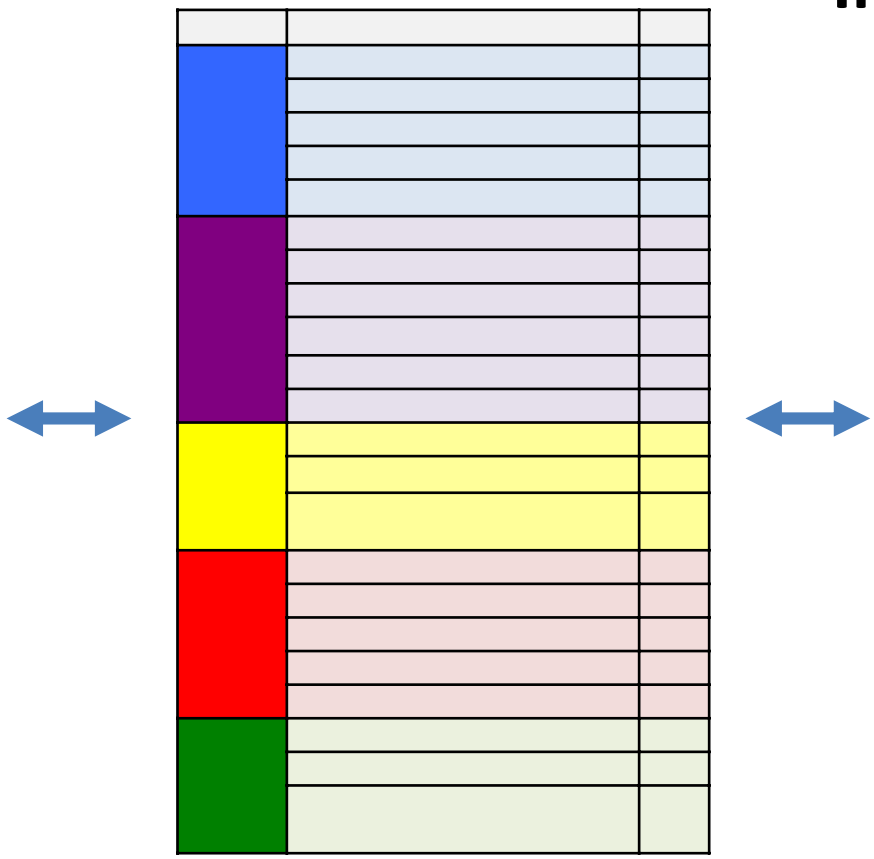
	1 Partial	2 Risk Informed	3 Repeatable	4 Adaptive
People	Whether people have assigned roles, regular training, take initiative by becoming champions, etc.			
Process	*NIST Risk Management Process* + *NIST Integrated Risk Management Program*			
Technology	Whether tools are implemented, maintained, evolved, provide effectiveness metrics, etc.			
Ecosystem	*NIST External Participation* + Whether the organization understands its role in the ecosystem, including external dependencies with partners			

Core

Cybersecurity Framework Component

Senior Executives

- Broad enterprise considerations
- Abstracted risk vocabulary



Implementation/ Operations

- Deep technical considerations
- Highly specialized vocabulary

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**

Connecting Technologists and Leadership

Cybersecurity Framework

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

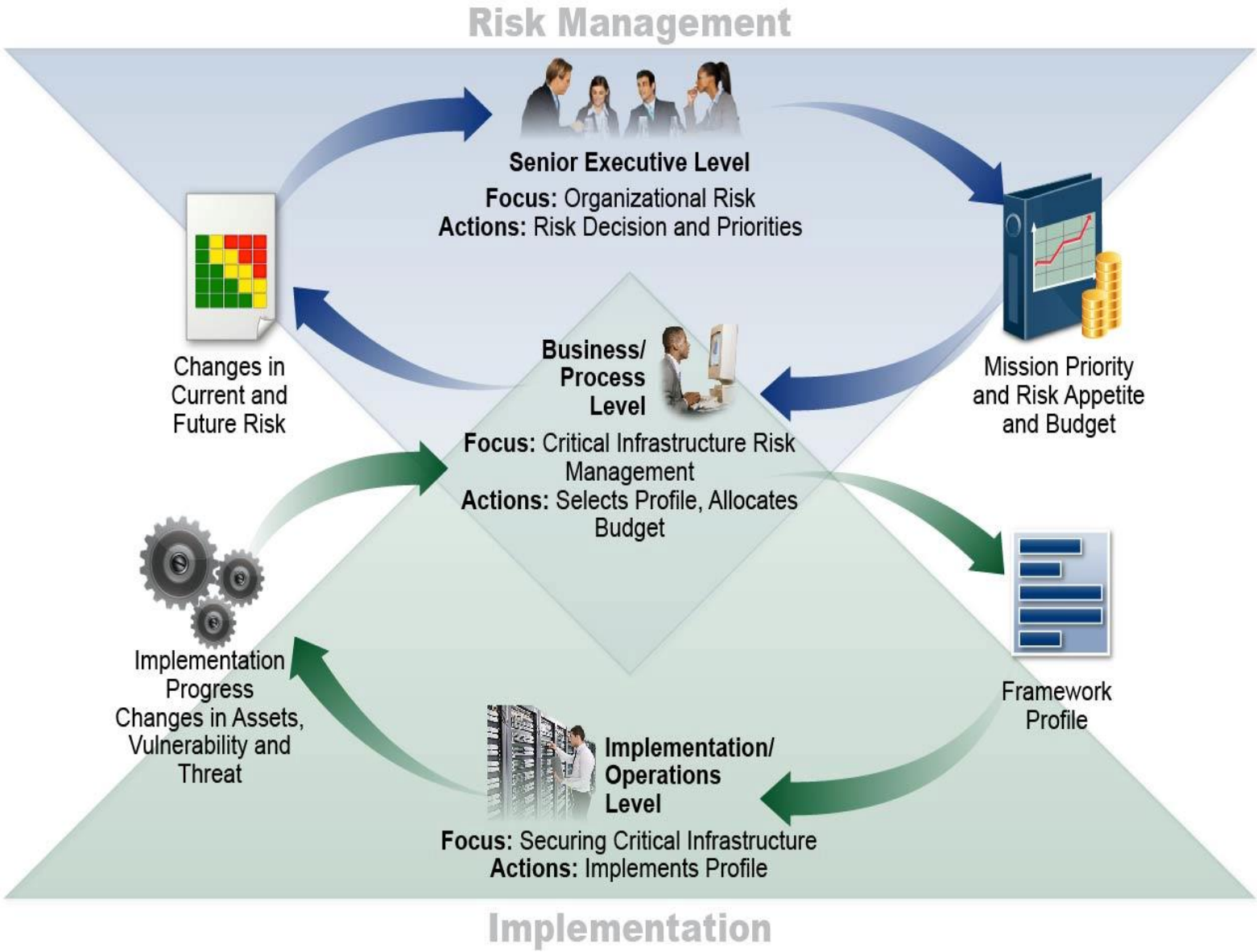
Profile

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

Supporting Risk Management with Framework



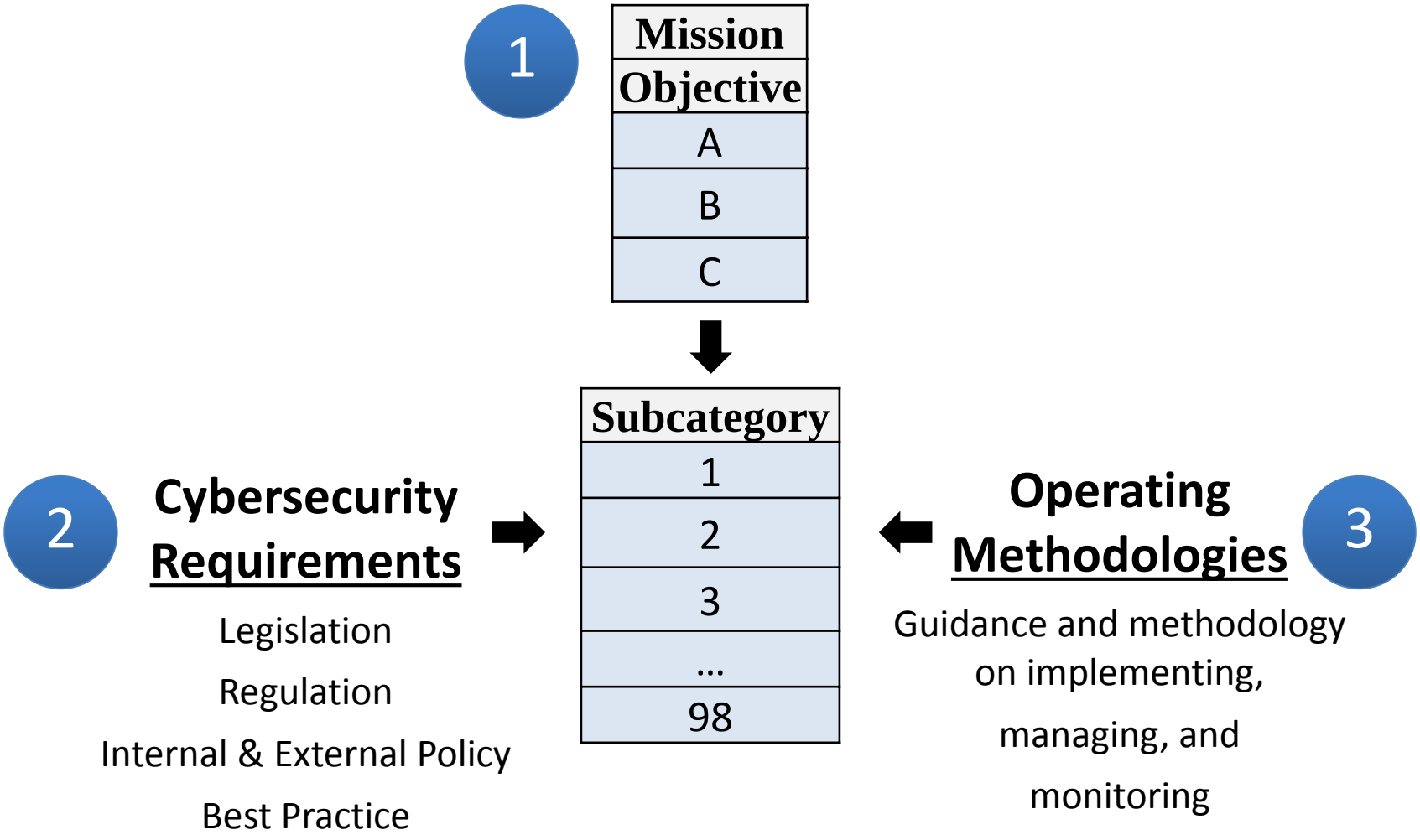
Framework 7 Step Process

3.2 Establishing or Improving a Cybersecurity Program

- 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

Building a Profile

A Profile Can be Created in Three Steps



Reconcile Requirements

Use Cybersecurity Framework Profiles to Align and Deconflict Requirements

Subcats	Requirements			
1	A		B	
2	C	D	E	F
3	G	H	I	J
…	…	…	…	…
98	XX		YY	ZZ
	Law	Regulation	Org Policy	Environment

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

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

Profile Ecosystem

TAXONOMY
1
2
3
…
98

REQUIREMENTS	
1	Req A
2	Req B
3	Req C
…	…
98	Req ZZ

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

National Institute of Standards and Technology

Community

Organization or Community

Cybersecurity Framework Core

Crosswalks Mappings

Cybersecurity Framework Profile

Guidance on OMB Circular A-130 Update

Roadmap Item - Federal Agency Cybersecurity Alignment

Updated OMB Circular A-130 Appendix III

Responsibilities for Protecting Federal Information Resources

Section 4.n The Framework is not intended to duplicate the current information security and risk management practices in place within the Federal Government. However, in the course of managing information security risk using the established NIST Risk Management Framework and associated security standards and guidelines required by FISMA, agencies can leverage the Cybersecurity Framework to complement their current information security programs.

Interim guidance: http://www.nist.gov/cyberframework/cybersecurity-framework-faqs-relationship-between-the-framework-and-other-approaches-and-initiatives.cfm#sp800-37

In the near future, "NIST will provide additional guidance on how agencies can use the Cybersecurity Framework and in particular, how the two frameworks can work together to help agencies develop, implement, and continuously improve their information security programs."

International Dialogs

Roadmap Item – International Aspects, Impacts, and Alignment

Twenty nine (29) countries have participated in discussion with NIST, including dialog with:

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

Common Patterns of Use

- Integrate the Functions into Your Leadership Vocabulary and Management Tool Sets
- Determine Optimal and 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

NIST Baldrige Excellence Builders

Baldrige Cybersecurity Excellence Builder

Manufacturing

Service

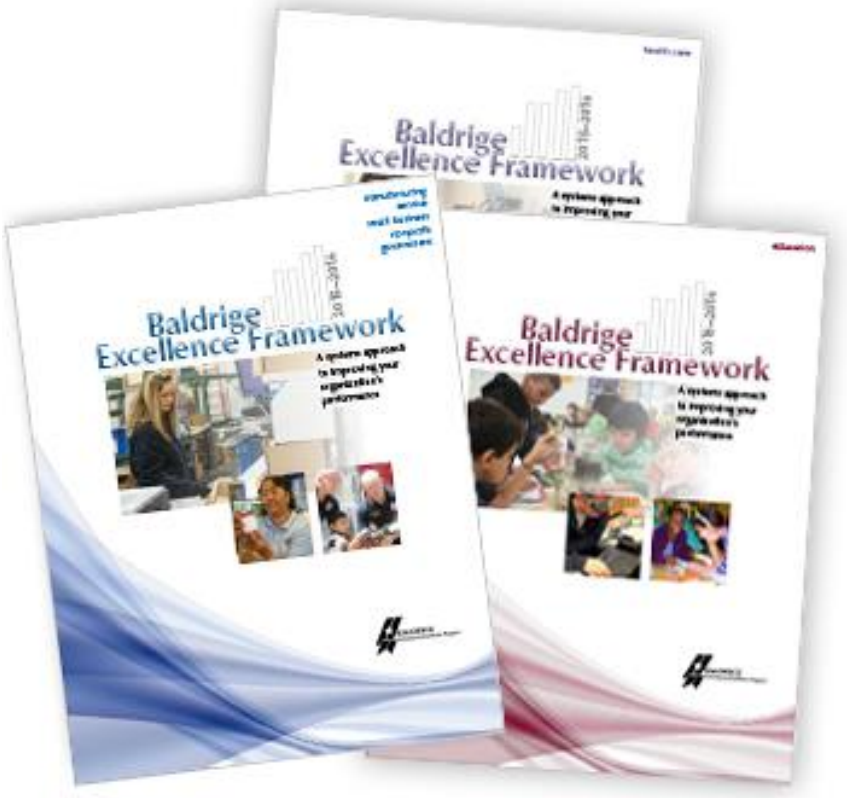
Small Business

Education (1999)

Healthcare (1999)

Non-profit (2007)

Cybersecurity (2016)



"*There is no question that setting the bar high by using the Baldrige Criteria and seeking this award made an enormous difference in our performance. The results show that we've outgrown our target competitors, exceeded margin expectations, and built a great workforce.*" - Scott McIntyre, Managing Partner, PWC Public Sector Practice

NIST Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Utilizing CSF Informative References to create tailored language for the manufacturing sector

- NIST SP 800-53
- NIST SP 800-82
- ISA / IEC 62443

System Categorization

NIST Discrete Manufacturing Profile

		Maintain Personnel Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
	Category	Subcategories				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3
		ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4
		ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5
		ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6
	Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1
		ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2
		ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3
		ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4
		ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5
	Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1
		ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4
	Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1
		ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2
		ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3
		ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4
		ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5
		ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6
	Risk Management Strategy	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1
		ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2
		ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3

System Categorization

NIST Discrete Manufacturing Profile

Possible Definitions for Manufacturing System Impact Levels Based on ISA99

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	$1,000	$100,000	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

Possible Definitions for Manufacturing System Impact Levels Based on Product Produced and Industry Concerns

Category	Low-Impact	Moderate-Impact	High-Impact
Product Produced	Non-hazardous materials or products Non-ingested consumer products	Some hazardous products or steps during production High amount of proprietary information	Critical infrastructure (e.g., electricity) Hazardous materials Ingested products
Industry Examples	Plastic injection molding Warehouse applications	Automotive metal industries Pulp and paper Semiconductors	Utilities Petrochemical Food and beverage Pharmaceutical

Examples of Framework Industry Resources

Italy's National Framework for Cybersecurity

American Water Works Association's *Process Control System Security Guidance for the Water Sector*

The Cybersecurity Framework in Action: An Intel Use Case

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

Energy Sector Cybersecurity Framework Implementation Guidance

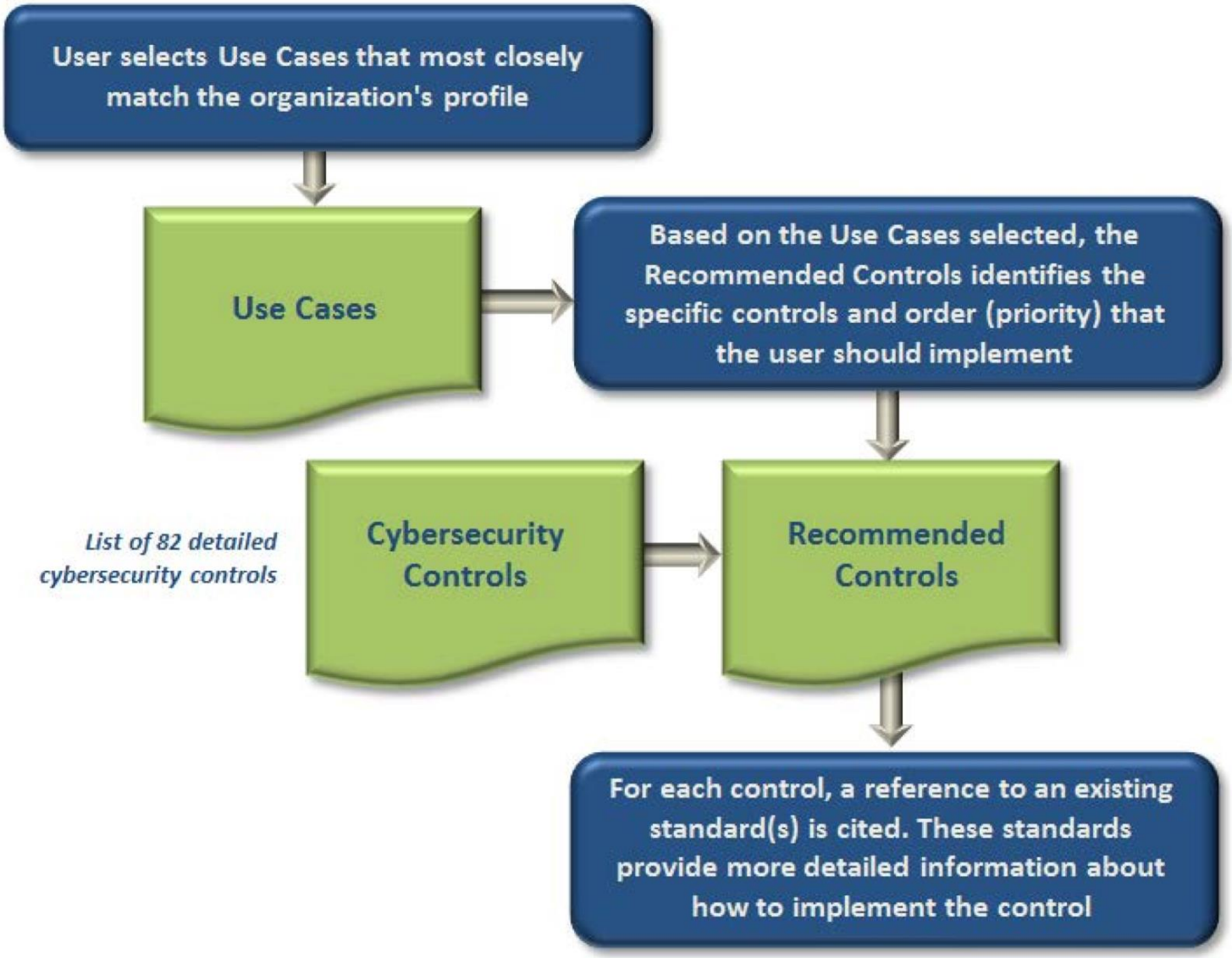
American Water Works Association

Process Control System Security Guidance for the Water Sector

- A 29 page security guide
- Recommended Security Practices for Water Sector – a list of 12 major ‘to dos’
- A Cybersecurity Guidance Tool to simplify guidance landscape
- Crosswalk of Framework to AWWA Guidance Control

Cybersecurity Guidance Tool

Process Control System Security Guidance for the Water Sector



CGT Use Case Examples

Process Control System Security Guidance for the Water Sector

Table 3-1

Use Cases

Category/ Code	Use Case	Description	Security Considerations
User Access			
UA1	Control room system access with control	Access to system with full read-write capability from "control room" (on-plant, physically secured) location.	Minimal access control needed here. Other issues like thumb drives and DVD usage may become a problem.
UA2	Plant system access with control	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor).	Medium network security needed here. Other issues like thumb drives and DVD usage may become a problem.
UA3	Remote system access with control	Access from location outside "control room" environment and located outside the physical perimeter of the facility.	Very rigorous access control and monitoring needed to authenticate remote users. Network topology is an issue; control of traffic into PCS network is needed.
UA4	Remote system access with view-only	Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility.	Special one way controls are needed. One way data flow can be done by ACLs or specialized equipment.
UA5	Remote system access with web view	Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility.	High network security needed. Network topology is an issue; control of traffic into PCS network is needed.
PLC Programming and Maintenance			
PLC1	Local PLC programming and maintenance	Access to program PLC located in immediate vicinity of user (serial or network).	Recommended practice.
PLC2	Plant PLC programming and maintenance	Access to program PLC located on same facility from centralized location.	Careful implementing authentication.
PLC3	Remote PLC programming	Access to program PLC located in another physical facility.	Not a recommended practice; two factor authentication should be in place. Dangerous!
Network Management			
NM1	Local network management	Access to configure network infrastructure located in immediate vicinity of user (serial or network).	Basic access control needed. Network equipment managed from SCADA facilities only, over SCADA network infrastructure
NM2	Plant network management	Access to configure network infrastructure located on same facility from centralized location.	Medium security needed.
NM3	Remote network management	Access to configure network infrastructure located in another physical facility.	High security needed. High reliability on authentication of users.

Referenced Standards

Process Control System Security Guidance for the Water Sector

Table 3-3
List of Standards & Guidance

	Name	Overview
DHS-CAT	U.S. Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendations for Standards Developers	A body of recommended practices across industries and agencies to prevent cyber-attacks.
DHS DID	DHS Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies	A body of recommended practices specific to ICS and emphasizing Defense in Depth Strategies.
NIST 800-82	National Institute of Standards and Technology (NIST) SP800-82 Guide to Industrial Control Systems (ICS) Security	The canonical standard for ICS systems.
NIST 800-53	NIST SP800-53 Rev. 3 with Appendix I Recommended Security Controls for Federal Information Systems and Organizations	A comprehensive framework of controls to be used to create complex security controls and monitoring systems.
NIST 800-34	NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems	Instructions and recommendations to implement short term recovery of damaged systems after an attack.
NIST 800-124	NIST Special Publication 800-124r1 Guidelines for Managing the Security of Mobile Devices in the Enterprise	Considerations and guidelines for the implementation of mobile systems
ANSI/AWWA G430-09	Security Practices for Operations and Management	Considerations and guidelines for the implementation of action for security of PCS systems.
*ANSI/AWWA G440-11	Emergency Preparedness Practices	Considerations and guidelines for the implementation of action for security of PCS systems.
*ANSI/AWWA J100-10	Risk and Resilience Management for Water and Wastewater Systems	Considerations of response and recovery actions that may include cyber-attack scenario.
*WRF/EPA/AWWA	Business Continuity Planning for Water Utilities	Considerations of disaster response plan for critical business enterprise systems including IT and PCS.
ISA-62443	ISA-99: Industrial Automation and Control Systems Security, ANSI/ISA 99	Considerations and guidelines for the implementation of PCS systems
ISO/IEC 27K	ISO/IEC 27000-27007 + 15408: Information technology - Security techniques - Code of practice for information security management (formerly ISO/IEC 17799:2000)	A certifiable framework to implement security programs.

Intel

The Cybersecurity Framework in Action: An Intel Use Case

- A 10 page Framework case study
- Pilot in Intel's Office of Enterprise Infrastructure
- Customized Implementation Tiers
- Interviewed subject matter experts to assign Tier scores at the Category level
- Compared to an optimal Tier assignments at the category level to determine gaps

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			

Adaptation of Implementation Tiers

	1 Partial	2 Risk Informed	3 Repeatable	4 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			

Category Gap Analysis

The Cybersecurity Framework in Action: An Intel Use Case

Individual Score (1–4) Heat Map

Evaluating by functional area provides greater insight

Comparing Scores

Significant differences can highlight visibility issues and focus areas

	SME INDIVIDUAL FUNCTIONAL AREA SCORES						SCORES		RESULTS		
IDENTIFY	**POLICY**	**NETWORK**	**ENDPOINT/ DATA PROTECTION**	**IDENTITY**	**OPs**	**APPs**	**SME AVERAGE**	**CORE GROUP**	**COMBINED SCORE SME AND CORE**	**TIER TARGET SCORE**	**RISK GAP**
Business Environment	3	3	3	2	3	2	3	2	2	3	1
Asset Management	3	2	2	2	1	3	2	3	3	3	0
Governance	3	2	3	2	2	2	2	2	2	2	0
Risk Assessment	2	2	2	2	2	3	2	1	2	3	1
Risk Management Strategy	4	3	2	2	2	2	3	2	2	4	2
PROTECT											
Access Control	2	3	2	2	3	2	3	2	2	3	1
Awareness/Training	2	3	3	2	3	3	3	3	3	4	1
Data Security	2	2	2	2	3	2	2	3	3	3	0
Protective Process/Procedures	2	2	2	2	2	2	2	2	2	4	2
Maintenance	3	2	2	2	2	4	2	1	2	3	1
Protective Technologies	2	2	1	3	1	2	2	3	2	3	1
DETECT											
Anomalies/Events	2	3	1	2	2	4	2	2	2	4	2
Security Continuous Monitoring	2	2	1	2	1	1	1	2	2	4	2
Detection Process	2	3	2	2	3	2	2	4	3	3	0
Threat Intelligence	3	3	3	2	2	2	3	3	3	3	0
RESPOND											
Response Planning	2	2	3	2	3	2	3	2	2	4	2
Communication	2	2	3	2	2	3	3	1	2	3	1
Analysis	2	3	3	2	3	3	3	2	2	3	1
Mitigations	2	3	1	2	3	1	2	3	3	3	0
Improvements	3	3	3	3	3	3	2	1	2	2	0
RECOVER											
Recovery Planning	2	3	3	2	3	2	3	3	3	3	0
Improvements	1	3	2	1	3	2	2	1	2	2	0
Communications	2	2	3	2	1	3	2	3	3	3	0

Mapping highlighted outliers and major differences

Focus areas stand out (large Δ)

Significant differences between Core and Individual scores can highlight visibility issues

FOR ILLUSTRATIVE PURPOSES ONLY

Italy

National Framework for Cybersecurity

- A 121 page national framework
- Based 100% on NIST Framework
- Created with industry and academia
- Published in both Italian and English
- Suggested Subcategory Priorities for Small and Medium Enterprises (SME)
- Qualitative Assessment Criteria
- Capture an approach to risk management that is beyond NIST Framework

Suggested Priorities for SMEs

National Framework for Cybersecurity

Function	Category	Subcategory	Priority	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**HIGH**	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	**HIGH**	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	**LOW**	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**NOT SELECTED**	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**MEDIUM**	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · **Mandatory for the Governative Agencies according to 50-bis, comma 3, lett. A of CAD**

cini Cyber Security National Lab

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

Qualitative Assessment Criteria

National Framework for Cybersecurity

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
IDENTIFY (ID)	ID.AM-1: Physical devices and systems within the organization are inventoried	Table 6.1: Assets identification (IA)	Assets inventory, classification and update (intended as information, applications, available systems and equipment) are performed mainly manually according to a defined and controlled process	Assets inventory, classification and update are performed in part in automatic mode that allows at least to automate the "discovery" phase of systems connected to the network, by detecting their characteristics (installed hardware, software, configurations, etc.) and registering the target inventory in a central repository	Inventory, classification and update of assets is done completely in automatic mode, allowing to manage the entire lifecycle of an asset (identification, assignment, status changes, removal, etc.)
	ID.AM-2: Software platforms and applications within the organization are inventoried	Table 6.1: Assets identification (IA)	See ID.AM-1	See ID.AM-1	See ID.AM-1
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers,	Table 6.2: Responsibility assignment (AR)	The Company Owner and/or the Top Management designates the representative for Cyber Security, formally defining its tasks. They also establish technical specifications for an adequate use of	A Company Policy document for the Cyber Security defining and clearly formalizing roles, responsibilities and activities required to all involved parties, clearly communicating to	N/A

Communications Security, Reliability, and Interoperability Council

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

- A 400 page security guide
- Profiles for five different telecommunications segments – Broadcast, Cable, Satellite, Wireless, Wireline
- Requirements and Barriers to Implementation
- Small and Medium Business guidance

Subcategory Scope, Criticality, and Difficulty - Cable Segment

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

	Scoping		Prioritization	
	In Scope/Out of Scope	Application	Criticality	Difficulty
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
information are conducted, maintained and tested periodically		within the core network are maintained and tested periodically.		
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	In Scope	Physical operating environment for the core infrastructure.	3	3
PR.IP-6: Data is destroyed according to policy	In Scope	We destroy IP data mappings as defined by policy.	NA	NA

Prioritized Practices - Cable Segment

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

Level 1	Level 2	Level 3
ID.AM-1: Physical devices and systems within the organization are inventoried	ID.AM-4: External information systems are catalogued	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources
ID.AM-2: Software platforms and applications within the organization are inventoried	ID.BE-2: Organization's place in critical infrastructure and its industry sector is identified and communicated	ID.RA-3: Threats, both internal and external, are identified and documented
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	ID.BE-5: Resilience requirements to support delivery of critical services are established	ID.RM-2: Organizational risk tolerance is determined and clearly expressed
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
ID.GV-1: Organizational information security policy is established	ID.GV-4: Governance and risk management processes address cybersecurity risks	PR.AT-1: All users are informed and trained
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties
PR.AC-1: Identities and credentials are managed for authorized devices and users	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	DE.CM-5: Unauthorized mobile code is detected

Requirements and Barriers to Implementation

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

Relevant Categories:	Primary Barrier:
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**Financial:** Barriers are dependent on the size of an organization, and costs are not linear. Marginal cost for improving Tier position is often exponential. Nonetheless, enterprises should use the NIST framework's Tier definitions to determine their current posture, and where they want to be. (FINANCIAL)
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.	**Technology:** There is no specific set of technologies for implementing the framework, as they are evolving and changing. Barrier is the complexity of the problem. Nonetheless, full assessment of the Business Environment should be undertaken as a starting point for risk management calculations. (TECHNOLOGY)
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.	**Legal/Policy:** Difficulties in differentiating between what is classified and what is non-classified information. For segments like Satellite, differentiation between the federal government (classified) and consumer/enterprise markets (unclassified) makes governance determinations more

Department of Energy

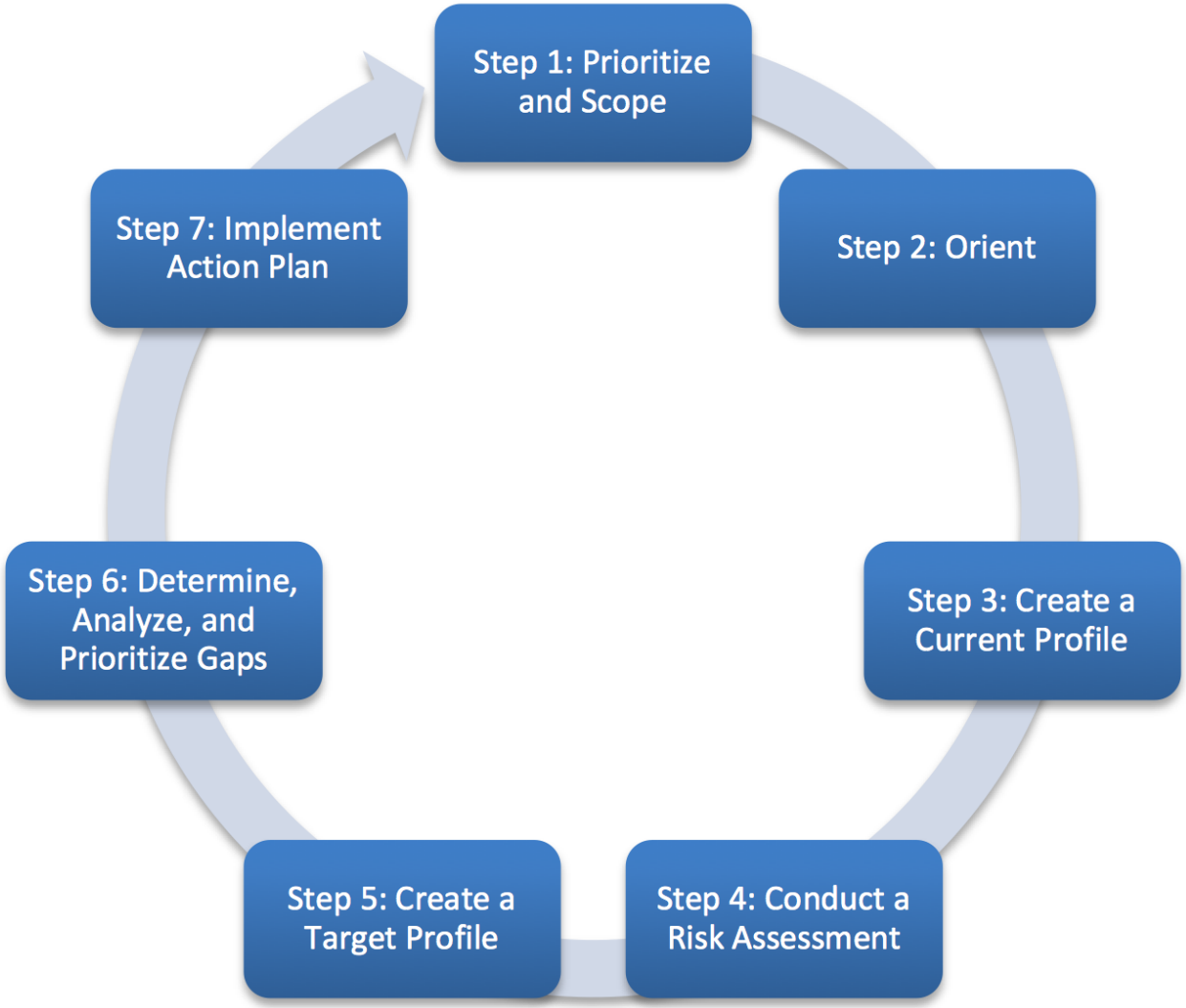
Energy Sector Cybersecurity Framework Implementation Guidance

- A 49 page Framework implementation guide
- Heavy emphasis on mapping Framework to Cybersecurity Capability Maturity Model (C2M2)
- A view of organizational approaches to gap analysis
- Provides additional detail for 7 Step Framework process
- Maps Framework Implementation Tiers to C2M2 MILs
- Maps Framework Implementation Tiers to C2M2 MILs

DoE Framework Implementation Approach

Energy Sector Cybersecurity Framework Implementation Guidance

- An effective communications and an iterative feedback loop for continuous improvement
- Similar to Electricity Subsector Cybersecurity Risk Management Process Guideline [RMP; DOE 2012b]



Detailed 7 Step Framework Process

Energy Sector Cybersecurity Framework Implementation Guidance

Step 1: Prioritize and Scope		
Inputs	**Activities**	**Outputs**
1. Risk management strategy 2. Organizational objectives and priorities 3. Threat information	1. Organization determines where it wants to apply the Framework to evaluate and potentially guide the improvement of the organization's cybersecurity capabilities	1. Framework usage scope
Step 2: Orient		
Inputs	**Activities**	**Outputs**
1. Framework usage scope 2. Risk management strategy	1. Organization identifies in-scope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and Informative References (e.g., cybersecurity and risk management standards, tools, methods, and guidelines)	1. In-scope systems and assets 2. In-scope requirements (i.e., regulatory, company, organizational) 3. In-scope cybersecurity and risk management standards, tools, methods, and guidelines 4. Evaluation approach
Step 3: Create a Current Profile		
Inputs	**Activities**	**Outputs**
1. Evaluation approach 2. In-scope systems and assets 3. In-scope regulatory requirements 4. In-scope cybersecurity and risk management standards, tools, methods,	1. Organization identifies its current cybersecurity and risk management state	1. Current Profile 2. Current Implementation Tier

Gap Analysis by Organization Approach

Energy Sector Cybersecurity Framework Implementation Guidance

Organization 1
Internal Controls Approach

Function	Category	Subcategory	Profiles	
			Current	Target
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination • *Supervisor signature required before VPN account issued* • *Bi-annual review of authorized VPN account list*

Organization 2
Standards Based Approach

Function	Category	Subcategory	Profiles	
			Current	Target
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • *NIST SP 800-53 Rev 4 AC-17 (3)* • *NIST SP 800-53 Rev 4 AC-17 (4)* • NIST SP 800-53 Rev 4 AC-19 • *NIST SP 800-53 Rev 4 AC-19 (5)* • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1) • *NIST SP 800-53 Rev 4 AC-20 (2)*

Organization 3
Exception Approach

Function	Category	Subcategory	Profiles	
			Current	Target
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Not Applicable - No remote access available for in-scope assets and systems	• Not Applicable - No remote access available to in-scope assets and systems

Implementation Tiers – to – C2M2 MILs

Energy Sector Cybersecurity Framework Implementation Guidance

Framework Implementation Tier	Tier Category	Characteristics	C2M2 Reference		
			MIL 1	MIL 2	MIL3
Tier 2: Risk Informed	Risk Management Process	Risk management practices are approved by management but may not be established as organizational-wide policy.		RM-3a* RM-3b*	
		Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.			RM-1c
	Integrated Risk Management Program	There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established.	RM-2a RM-2b		
		Risk informed, management - approved processes and procedures are defined and implemented, and staff has	CPM-2a CPM-2b	RM-3a RM-3b RM-3c	RM-1c

Framework Core – to – C2M2 MILs

Energy Sector Cybersecurity Framework Implementation Guidance

Framework Core			C2M2 Practices		
Function	**Category**	**Subcategory**	MIL 1	MIL 2	MIL3
DETECT (DE)	Security Continuous Monitoring (CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	SA-2a SA-2b	SA-2e SA-2f TVM-1d	SA-2g SA-2i
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	SA-2a SA-2b	SA-2e	SA-2i
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	SA-2a SA-2b	SA-2e	SA-2i
		DE.CM-4: Malicious code is detected	SA-2a SA-2b	SA-2e CPM-4a	SA-2i
		DE.CM-5: Unauthorized mobile code is detected	SA-2a SA-2b	SA-2e	SA-2h SA-2i
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	EDM-2a SA-2a SA-2b	SA-2e	EDM-2j EDM-2n

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

Stakeholder Recommended Actions

NIST applauds stakeholders for their efforts around the Framework thus far. To sustain the growth of a healthy Framework ecosystem, NIST asks that stakeholders:

- Customize the Framework for your sector or community
- Publish a sector or community Profile or relevant "crosswalk."
- Advocate for the Framework throughout your sector or community, with related sectors and communities.
- Publish "summaries of use" or case studies of your Framework implementation.
- Share your Framework resources with NIST at cyberframework@nist.gov.

Framework Next Steps

NIST will proceed with a **Minor** update that aims to **clarify and refine** the Framework while **minimizing** disruption to stakeholders.

Updates may include:

- *Updating the Informative References*
- *Clarifying guidance on the Implementation Tiers*
- *Cyber Threat Intelligence in the Core*
- *Guidance for applying the Framework in supply chain risk management*
- *And more…..*

Look for refinement to take place **outside of the Core** as well.

- *The Framework Roadmap*
- *Frequently Asked Questions*
- *Related work products and NIST publications*
- *Framework Governance Methodology*
- *Framework Self-assessment criteria*

NIST seeks to release a Framework draft for comment in early **2017**

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