Framework for Improving Critical Infrastructure Cybersecurity

Implementation of Executive Order 13636

NARUC Winter Committee Meeting

Committee & Staff Committee on Critical Infrastructure

February 15, 2015

cyberframework@nist.gov

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

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"

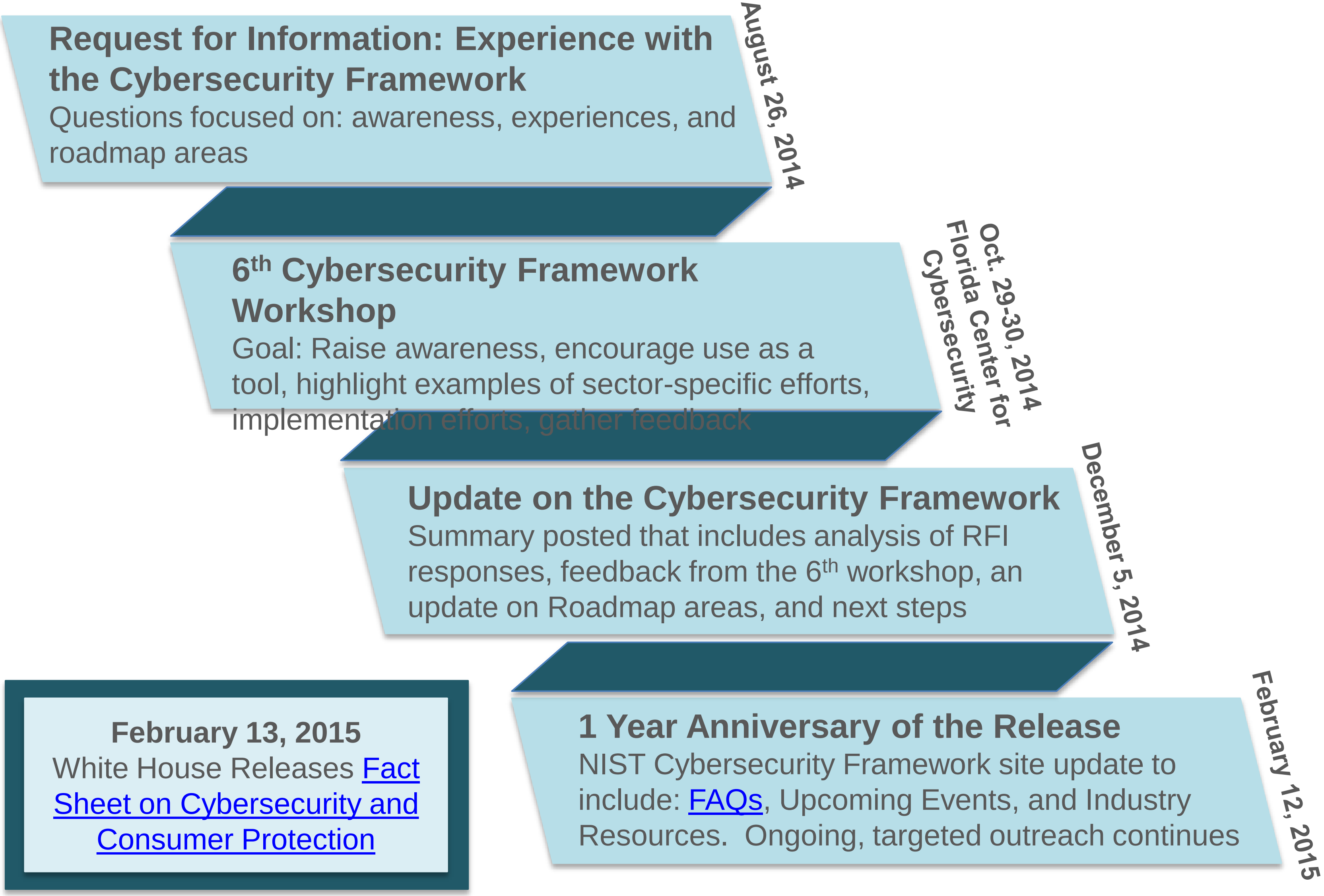
President Barack Obama

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

Since the February 12, 2014 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

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

Some Additional Cybersecurity Framework Resources Developed by Industry

The Cybersecurity Framework in Action: An Intel Use Case

Cybersecurity Guidance for Small Firms

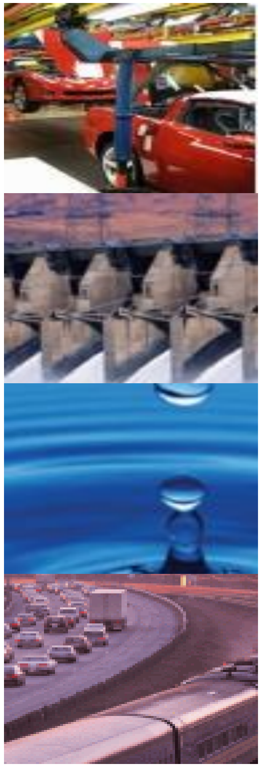
Energy Sector Cybersecurity Framework Implementation Guidance

Process Control System Security Guidance for the Water Sector

Other online communities of interest

Near Term Framework Activities

In summary, “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
- To allow for adoption, Framework version 2.0 is not planned for the near term

Where to Learn More and Stay Current

The *Framework for Improving Critical Infrastructure Cybersecurity*, the *Roadmap*, related news and information are available at:www.nist.gov/cyberframework

Email: cyberframework@nist.gov

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

Back-Up Slides

- Cybersecurity Framework Background
- Introduction to the Components of the Cybersecurity Framework

Based on the Executive Order, the Cybersecurity Framework Must

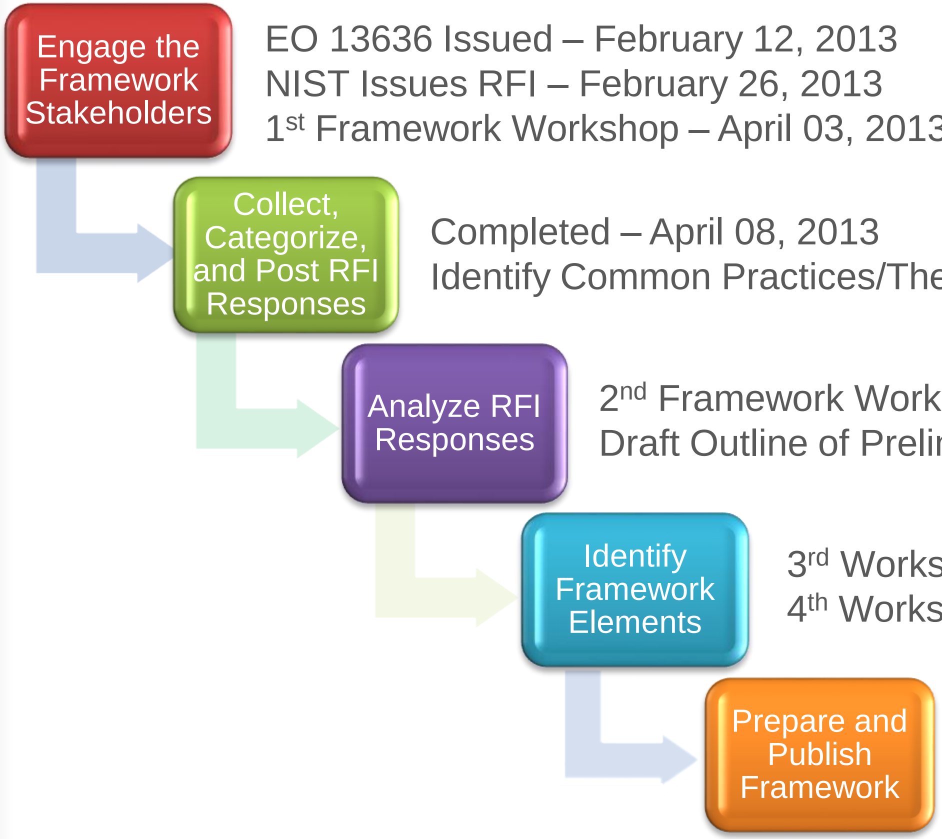
- Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks

- 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 – September 2013

Prepare and Publish Framework

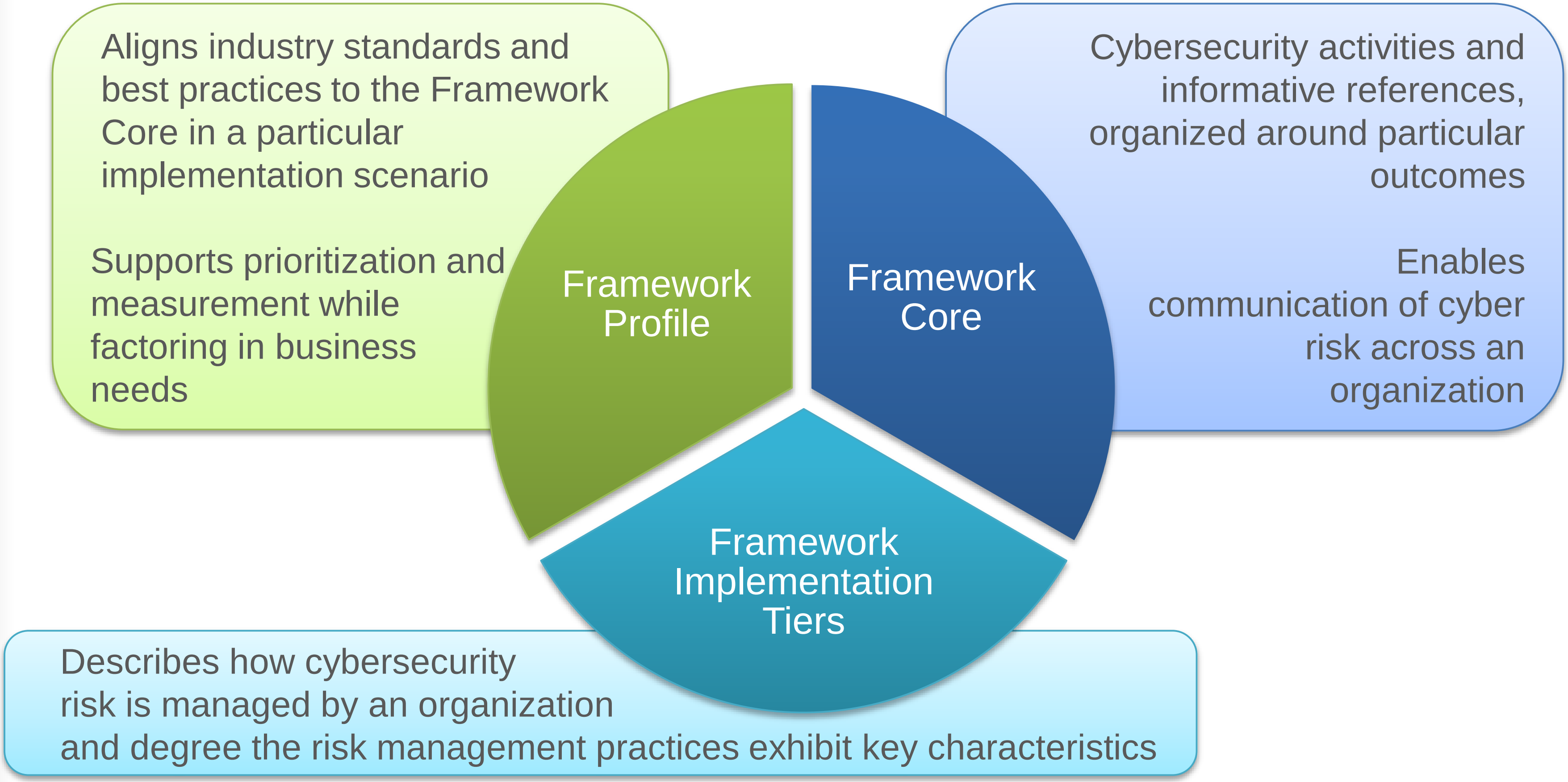
5th Workshop at NC State – November 2013
Published Framework – February 2014

Ongoing Engagement:

Open public comment and review encouraged and promoted throughout the process

cyberframework@nist.gov

Framework Components



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 Profile

Framework Core

Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

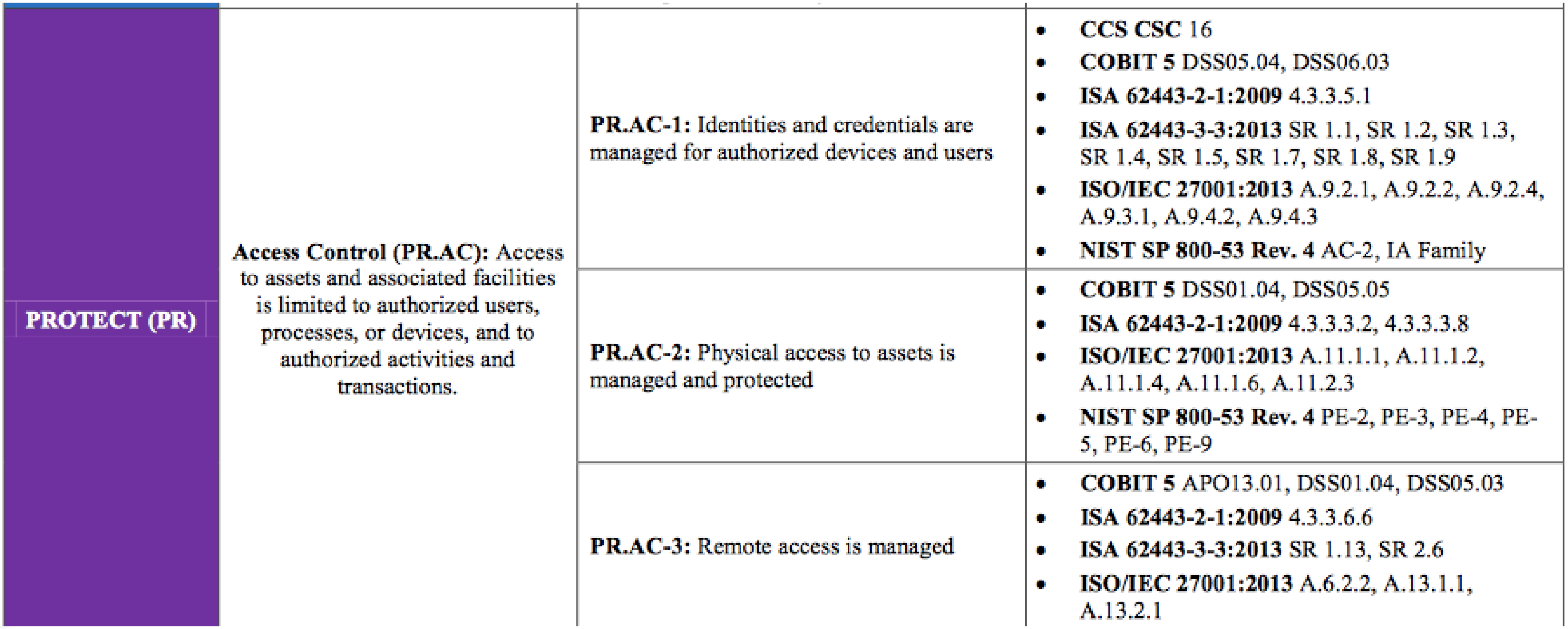
Framework Implementation Tiers

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

Framework Core

	Functions	Categories	Subcategories	Informative References
What assets need protection?	IDENTIFY			
What safeguards are available?	PROTECT			
What techniques can identify incidents?	DETECT			
What techniques can contain impacts of incidents?	RESPOND			
What techniques can restore capabilities?	RECOVER			

Framework Core - Sample



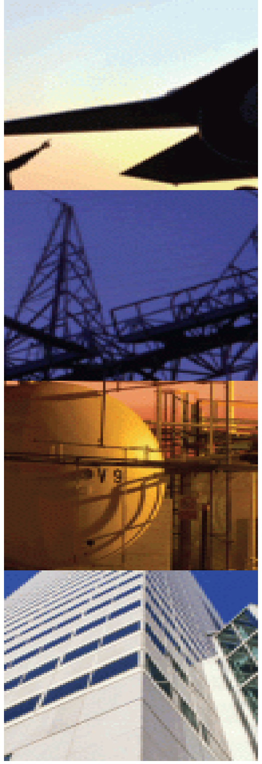
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **CCS CSC** 16 • **COBIT 5** 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

Framework Profile

- 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



Framework Implementation Tiers

- Feedback indicated the need for the Framework to allow for flexibility in implementation and bring in concepts of maturity models.
- Responding to feedback, Framework Implementation Tiers were proposed to reflect how an organization implements the Framework Core functions and manages its risk.
- The Tiers are progressive, ranging from Partial (Tier 1) to Adaptive (Tier 4), with each Tier building on the previous Tier.
- The Tier characteristics are defined at the organizational level and are applied to the Framework Core to determine how a category is implemented.

Why You Should Consider Adopting the Framework

Benefits	Features
• Reduces time and expense of starting an information security program • Reduces risk within current information security programs by identifying areas for improvement • Increases efficiencies and reduce the possibility of miscommunication within your information security program and with other organizations such as partners, suppliers, regulators, and auditors	• Organizes reconciliation and de-confliction of legislation, regulation, policy, and industry best practice (Core) • Guides organization and management of and information security program (Core) • Measures current state and expresses desired state (Profile) • Enables investment decisions to address gaps in current state (Profile) • Communicates cybersecurity requirements with stakeholders, including partners and suppliers (Profile) • Enables informed trade-off analysis of expenditure versus risk (Tiers)

Key Points about the Cybersecurity Framework

- **It’s a framework, not a prescription**
  - It provides a common language and systematic methodology for managing cyber risk
  - 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