Applying the Framework for Improving Critical Infrastructure Cybersecurity

April 11, 2018

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

Greg Witte
Senior Security Engineer
G2 Inc. &
Guest Researcher, NIST IT Laboratory

Audience Poll:

How many here are using the NIST Framework?

There Are Actually Several Relevant Frameworks to Leverage

- Cyber-Physical Systems (CPS) Framework
- Privacy Engineering Framework
- Baldrige Excellence Framework
- Framework for Improving Critical Infrastructure Cybersecurity (or the Cybersecurity Framework)
- Risk Management Framework
- NICE Framework (Workforce)

We have several objectives to cover during the workshop

- Learn a little of the history of the Cybersecurity Framework and why it has been developed in the way that it has
- Learn how the Cybersecurity Framework helps an enterprise to develop a business-centric view of information security
- Learn how the elements of the Cybersecurity Framework can be applied to help your organization understand and manage risk
- Identify pointers to many resources that are available to help organizations implement the Cybersecurity Framework
- Understand how to use the 7 CSF Steps – especially the Profile component - to help the organization document status and goals

Cybersecurity Framework Charter

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)):

"…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

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

Executive Order 13636 asked for the creation of a Cybersecurity Framework applicable to all sectors

- Executive Order
  - Be flexible
  - Be non-prescriptive
  - Leverage existing approaches, standards, practices
  - Be globally applicable
  - Focus on risk management vs. rote compliance
- Framework for Improving Critical Infrastructure Cybersecurity
  - Referred to as “The Cybersecurity Framework”
  - Informally referred to as the NIST CSF
  - Issued by NIST on February 12, 2014

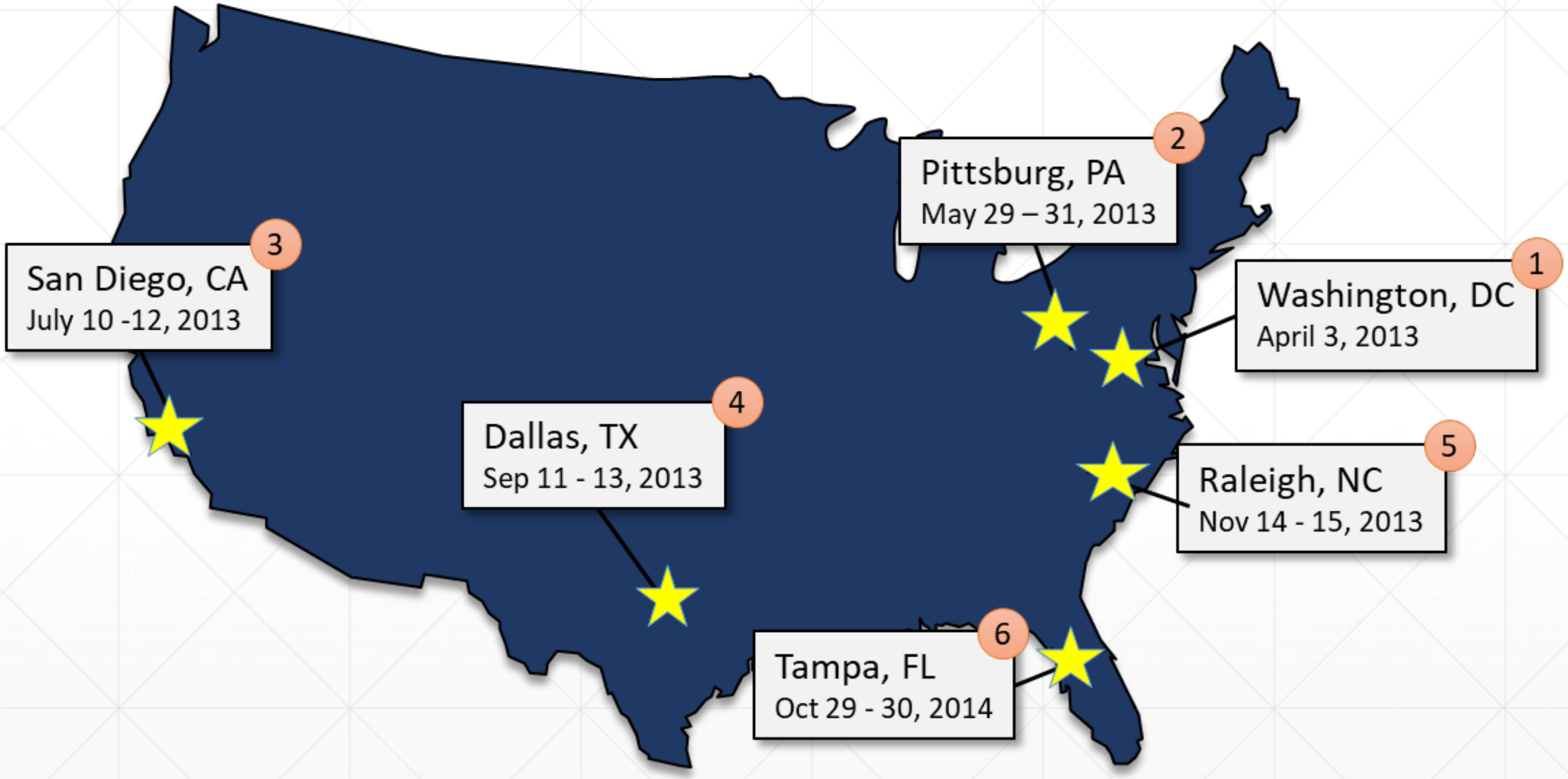
CORE
TIERS
NIST
CYBERSECURITY FRAMEWORK
PROFILE

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

One More Pop Quiz …

Who wrote the NIST Cybersecurity Framework?

The Framework was developed in partnership among industry, academia, and government

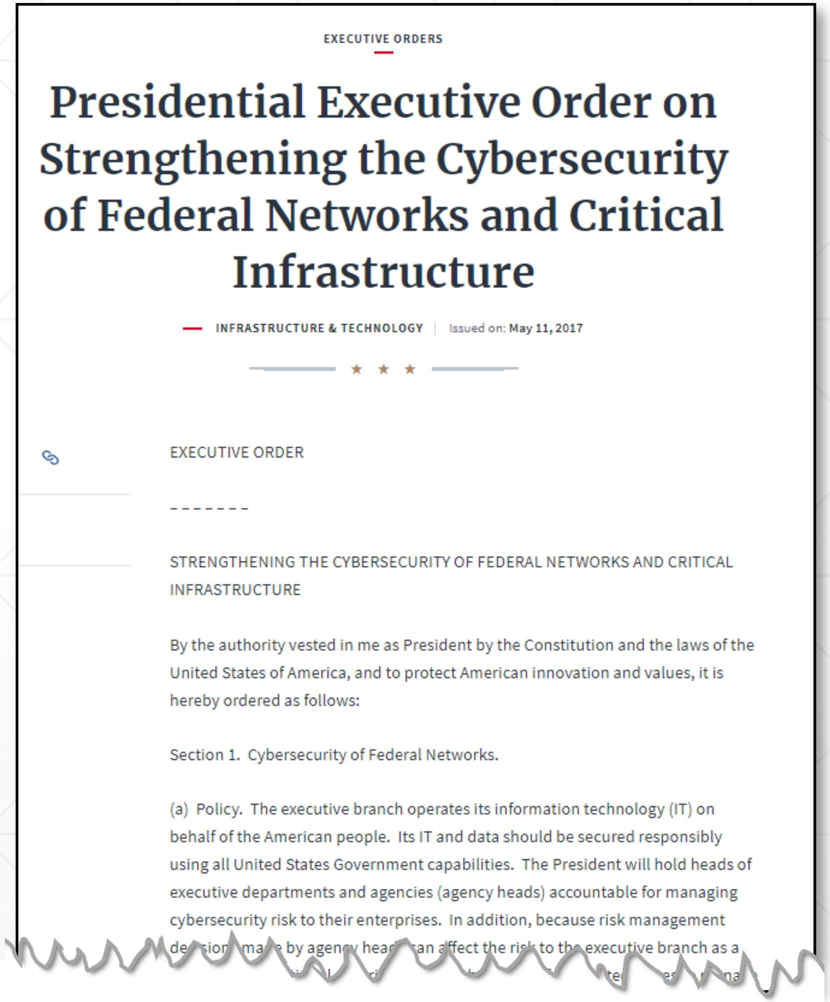


NIST National Institute of Standards and Technology U.S. Department of Commerce

HOTSOS 2018

Executive Order 13800 reconfirmed commitment to strengthening cybersecurity for Federal and CI

- EO 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- Risk Management
  - (ii) "…agency head shall use The Framework" and
  - "…provide a risk management report within 90 days containing a description of the "…agency's action plan to implement the Framework."
- Signed: May 11, 2017



EXECUTIVE ORDERS

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

INFRASTRUCTURE & TECHNOLOGY | Issued on: May 11, 2017

★ ★ ★

EXECUTIVE ORDER

- - - - - - -

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

Section 1. Cybersecurity of Federal Networks.

(a) Policy. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a

Defining cybersecurity programs is often about compliance

HIPAA
Health Insurance Portability and Accountability Act

FedRAMP℠

Information Security Management System
ISO
27001
Certified

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

NIST
National Institute of Standards and Technology

NERC CIP v5

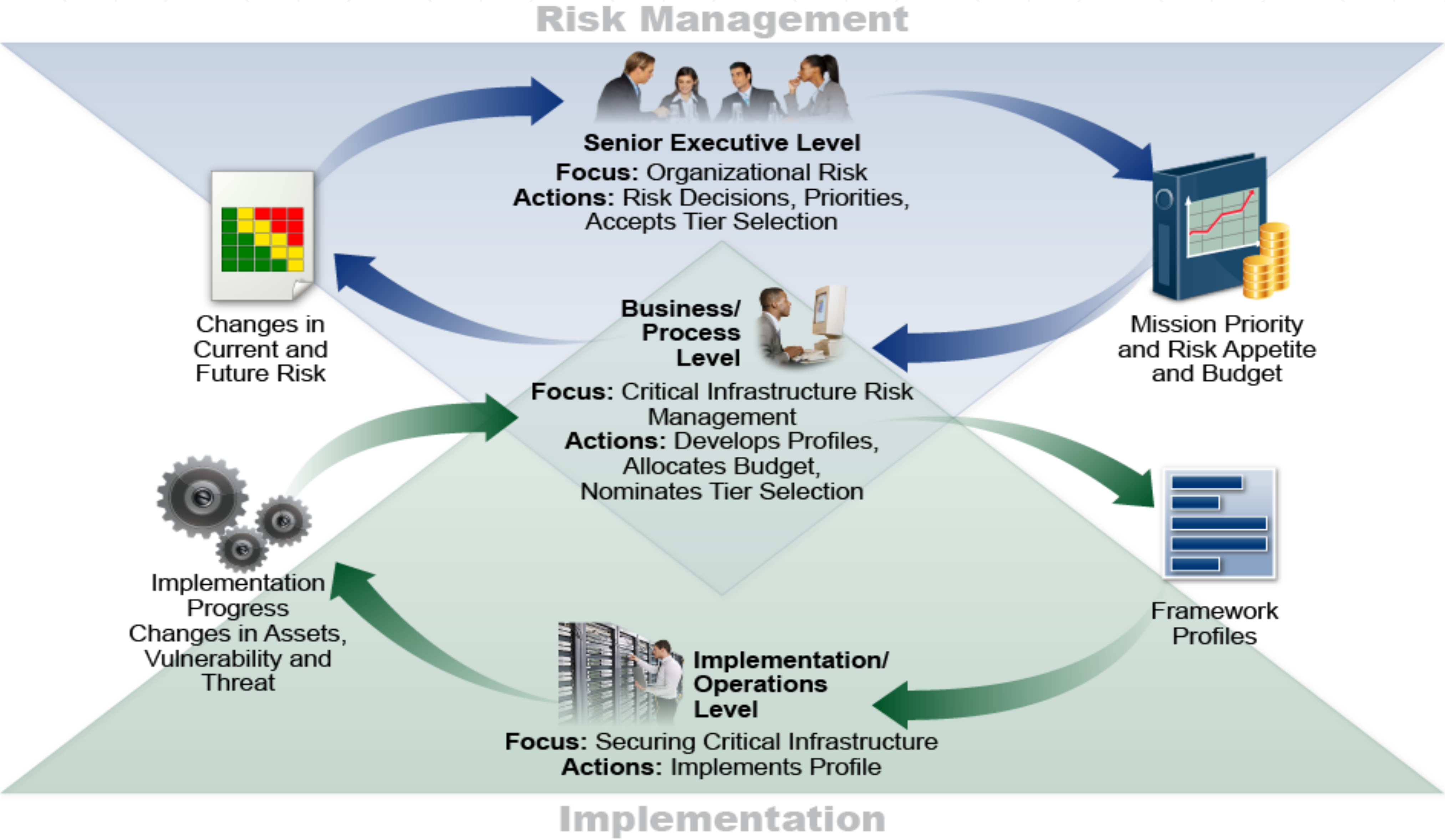
AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports ®

PCI COMPLIANT
PCi
PCI COMPLIANT

Compliance does not always mean secure

Other times security is not commensurate with the risk

The Framework establishes a common language within organizations and among external partners



Risk Management

Senior Executive Level

Focus: Organizational Risk
Actions: Risk Decisions, Priorities, Accepts Tier Selection

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

Business/ Process Level

Focus: Critical Infrastructure Risk Management
Actions: Develops Profiles, Allocates Budget, Nominates Tier Selection

Implementation Progress Changes in Assets, Vulnerability and Threat

Framework Profiles

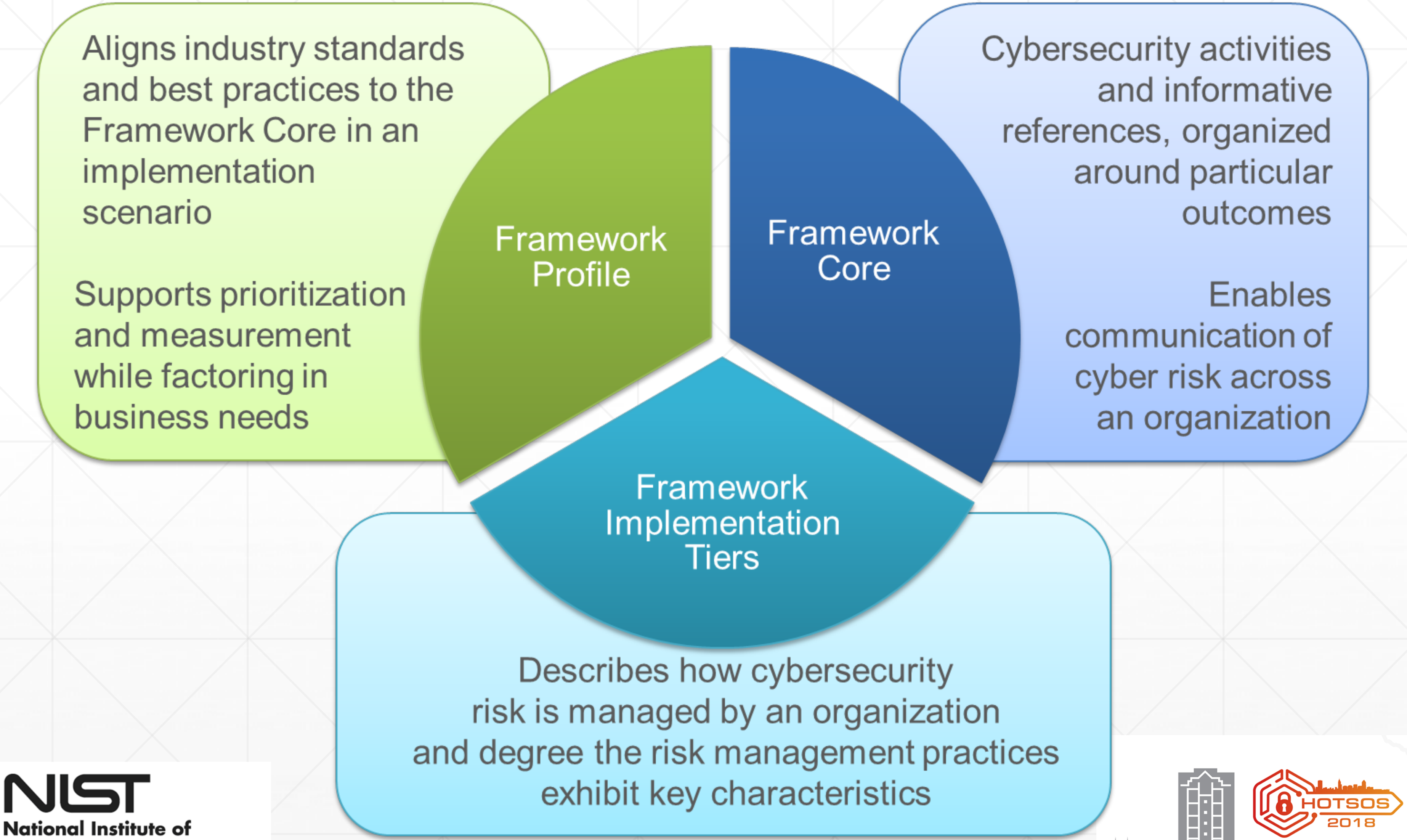
Implementation/ Operations Level

Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

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

The Framework established three primary components used to develop a holistic cybersecurity program



Framework Profile

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

The Framework Core establishes a catalog of cybersecurity outcomes

	Function
What processes and 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

- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

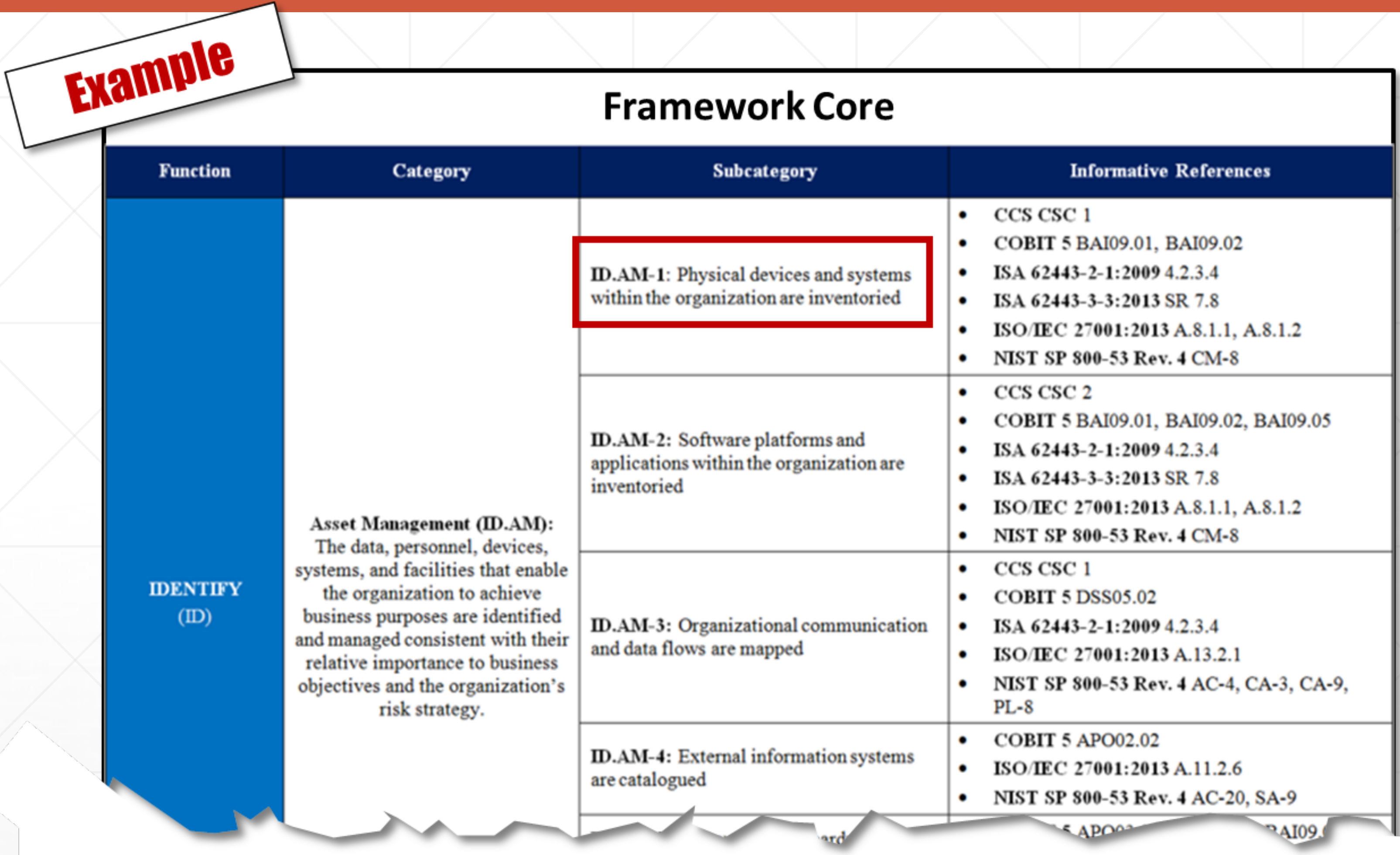
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

HOTSOS 2018

The Framework Categories provide groupings of cybersecurity outcomes

	Function	Category
What processes and assets need protection?	Identify	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
What safeguards are available?	Protect	Access Control
		Awareness and Training
		Data Security
		Information Protection Processes & Procedures
		Maintenance
		Protective Technology
What techniques can identify incidents?	Detect	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
What techniques can contain impacts of incidents?	Respond	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
What techniques can restore capabilities?	Recover	Recovery Planning
		Improvements
		Communications

Framework subcategories describe expected outcomes

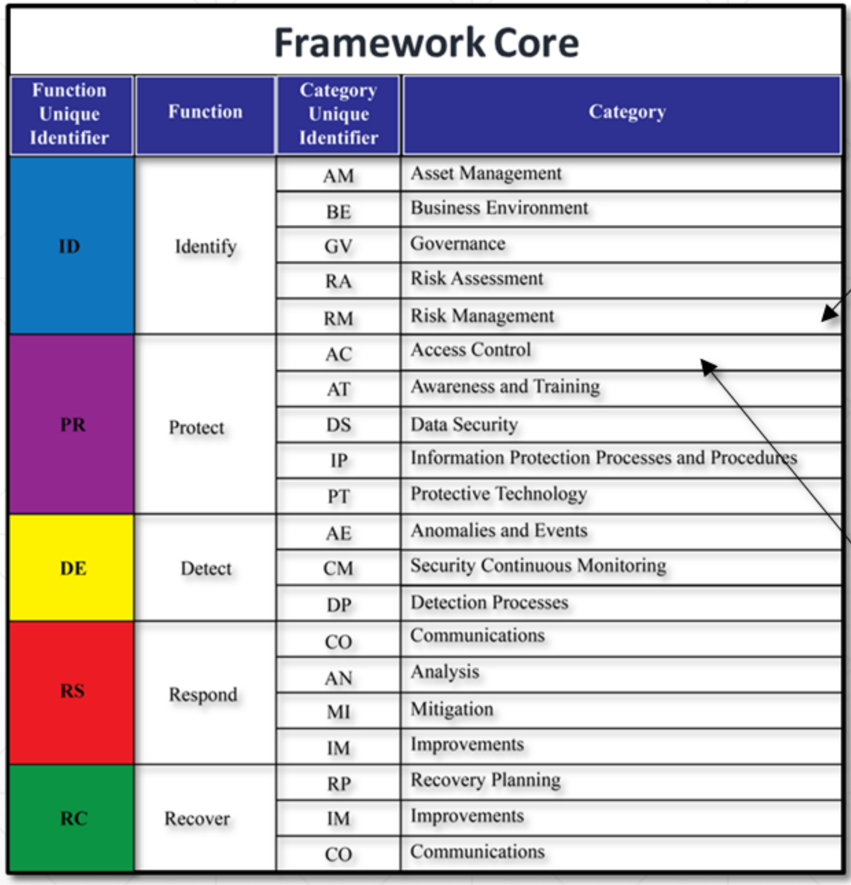


Example

Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**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	• 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	• 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	• 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	• COBIT 5 APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9

There are several Proposed Category updates in the draft Framework Version 1.1



Framework Core

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Supply Chain Risk Management

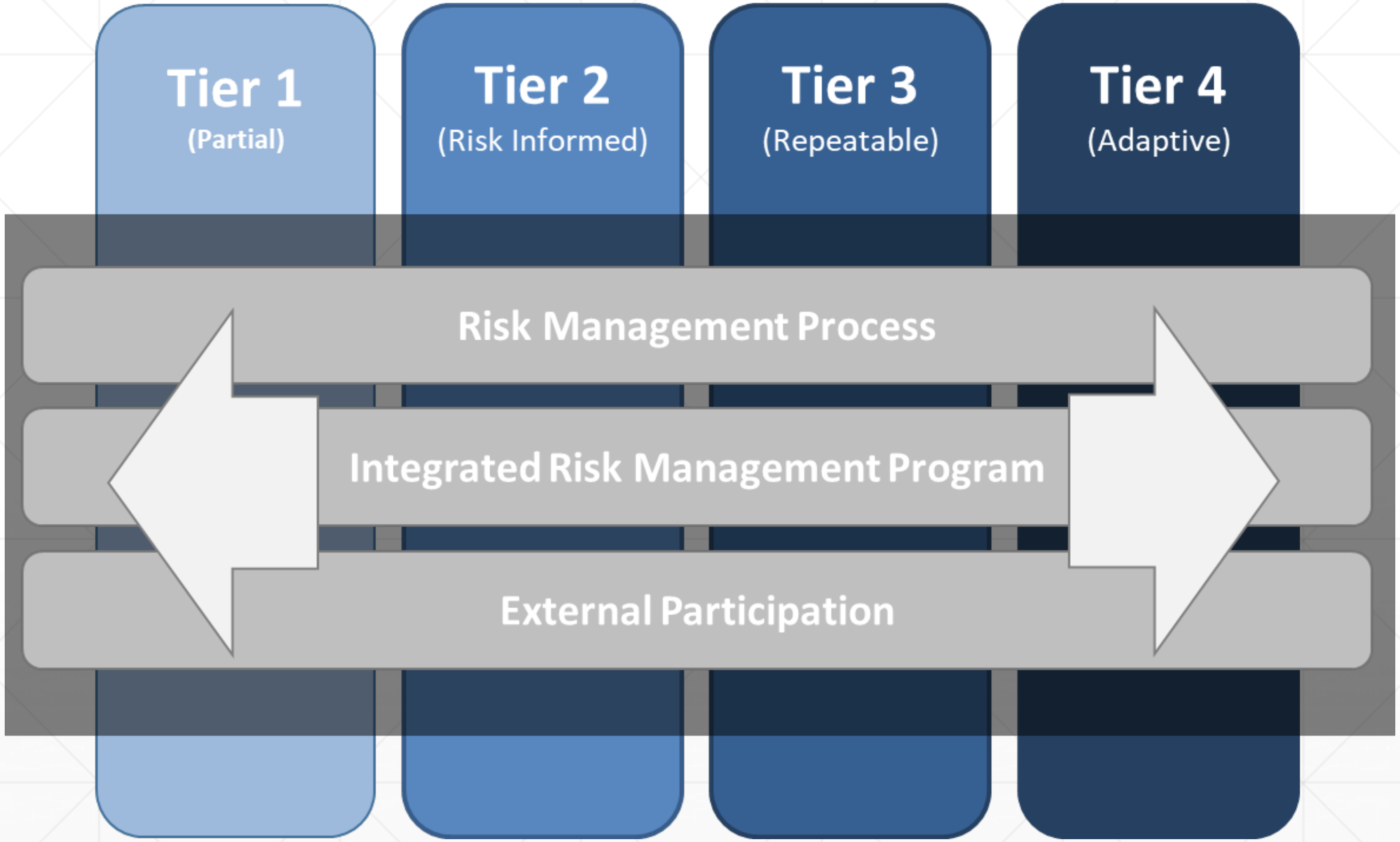
Identity Management & Access Control

- Functions: 5 → 5
- Categories: 22 → 23
- Subcategories: 98 → 108

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

HOTSOS 2018

Organizations select an Implementation Tier based on their risk threshold

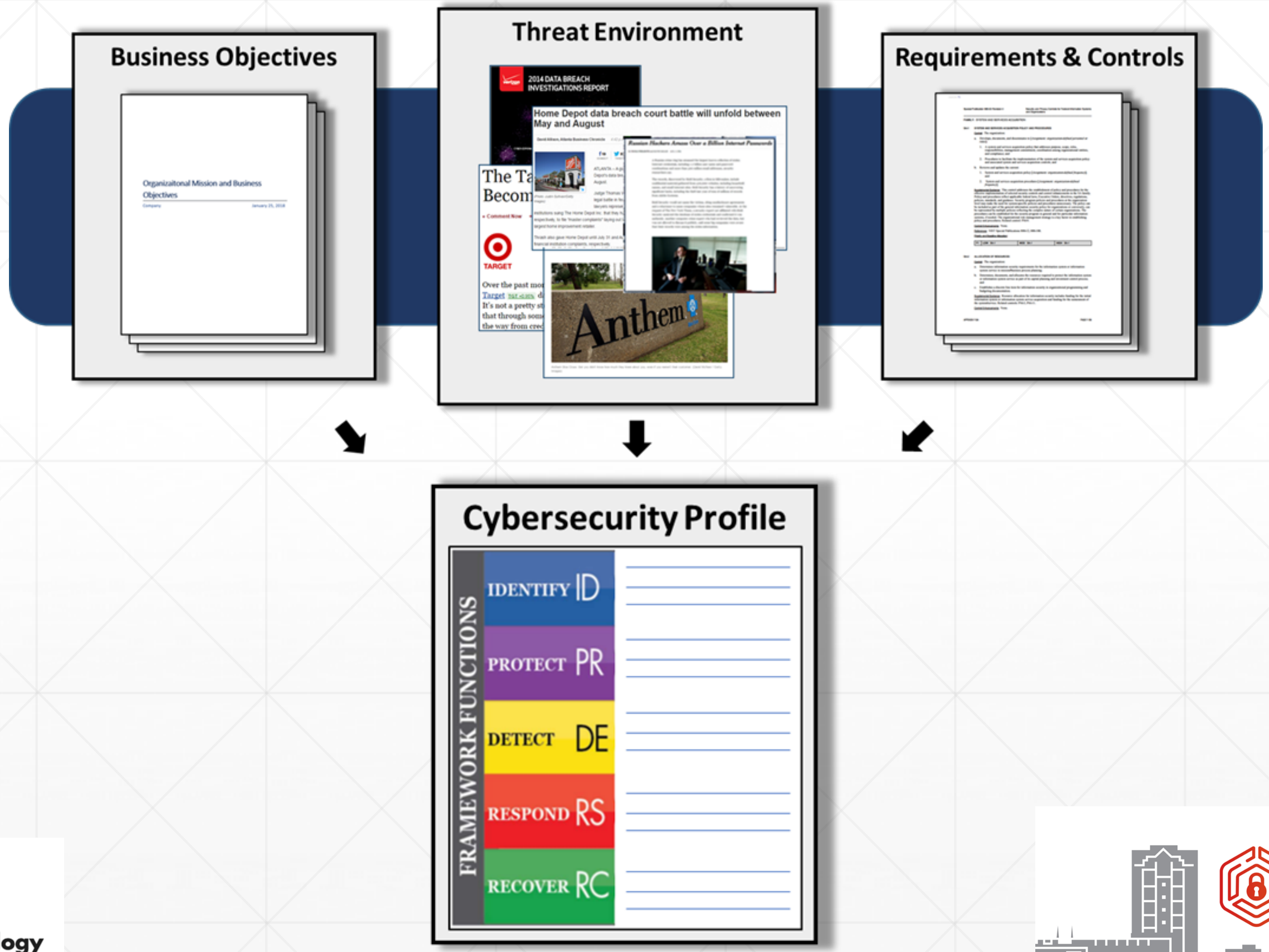


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

HOTSOS 2018

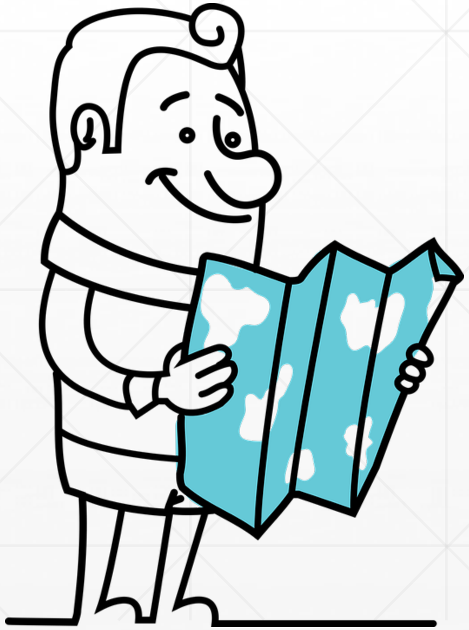
Organizations have applied the Implementation Tiers in different ways and at different levels

Profiles help organizations align & prioritize cybersecurity activities

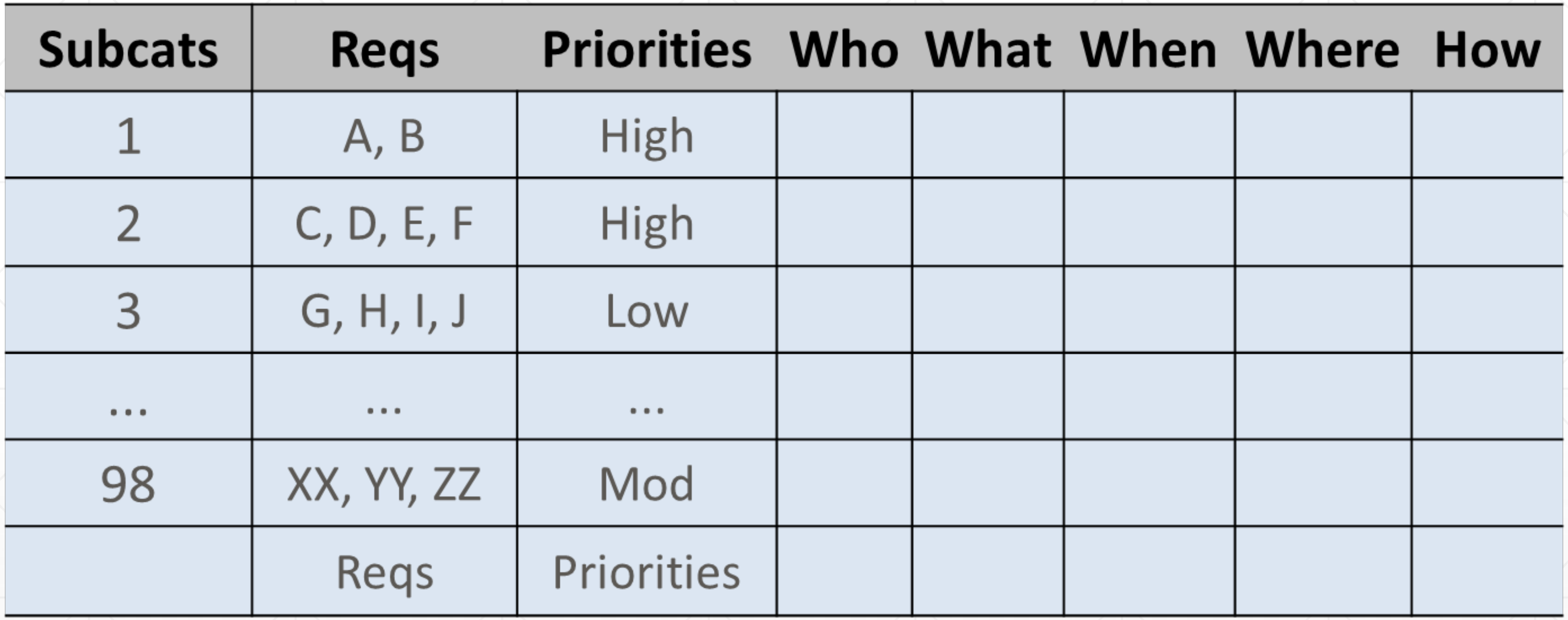

Business Objectives
Organizaitonal Mission and Business Objectives
Threat Environment
2014 DATA BREACH INVESTIGATIONS REPORT
Home Depot data breach court battle will unfold between May and August
Russian Hackers Amass Over a Billion Internet Passwords
The Ta
Becom
TARGET
Anthem
Requirements & Controls
Cybersecurity Profile
FRAMEWORK FUNCTIONS
IDENTIFY ID
PROTECT PR
DETECT DE
RESPOND RS
RECOVER RC

Current and Target state Profiles help organizations capture their cybersecurity program

- Current State Profile
  - Present state of the organization's unique cybersecurity program
- Target State Profile
  - Captures the to-be state for the organization's cybersecurity program



Cybersecurity Framework target state profiles can help 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					

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

Organizations identify business and mission objectives to initiate the process

Step 1: Prioritize and Scope

Organizational Structure

Mission Goals

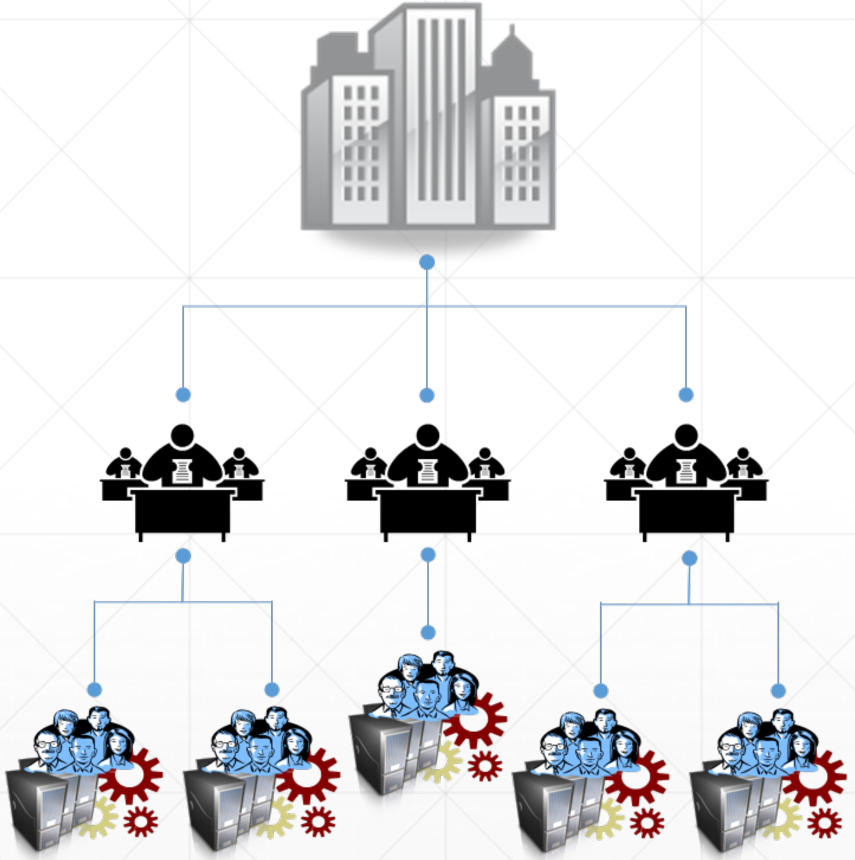
Priorities

Business Drivers

Regulatory Requirements

Existing Policies

Budget



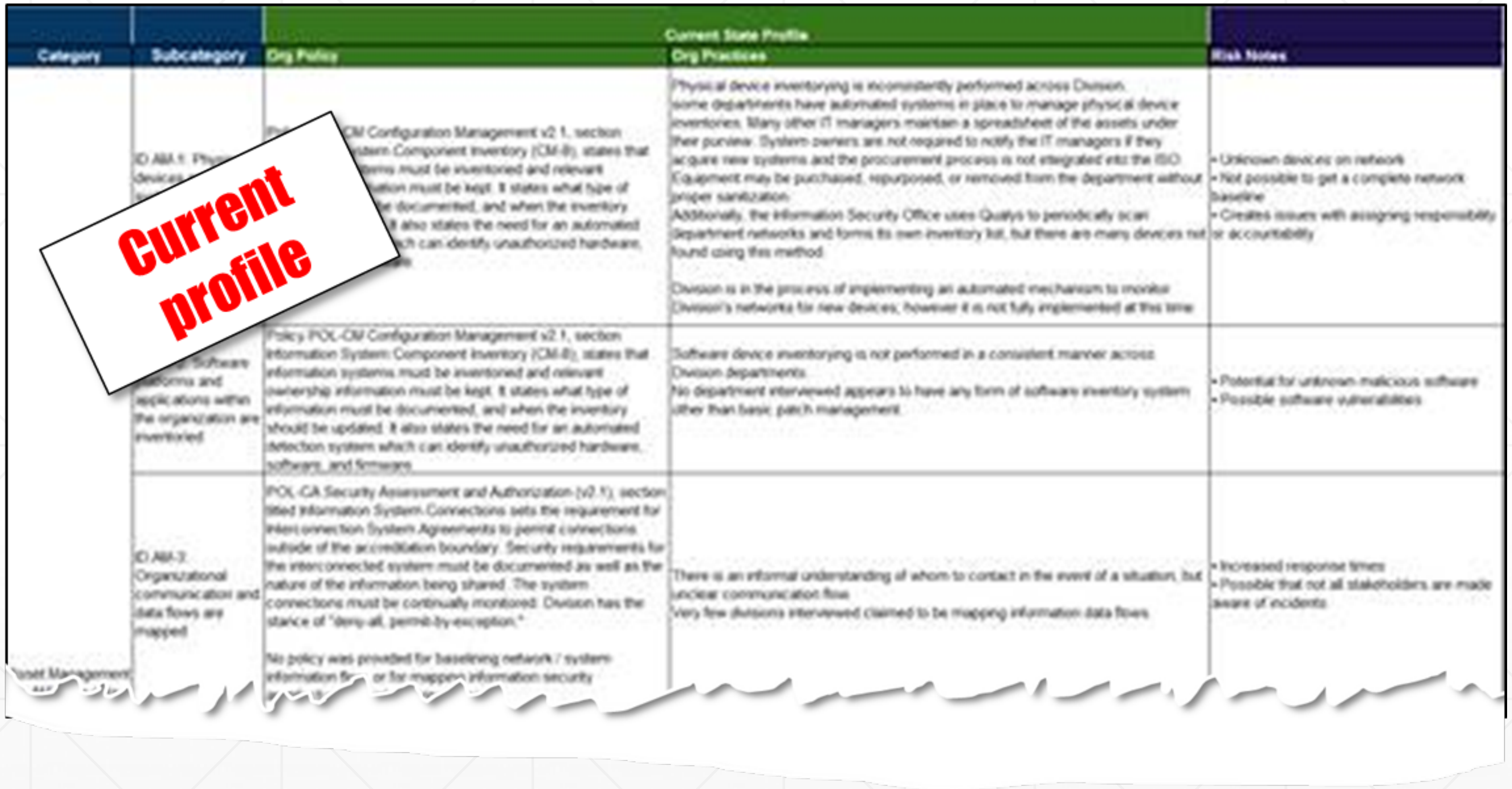
The orient step aligns the business goals, assets, systems, and regulatory requirements for the program

Step 2: Orient

Risk Thresholds

A Current Profile captures the organizations policies, procedures, and practices

Step 3: Current Profile

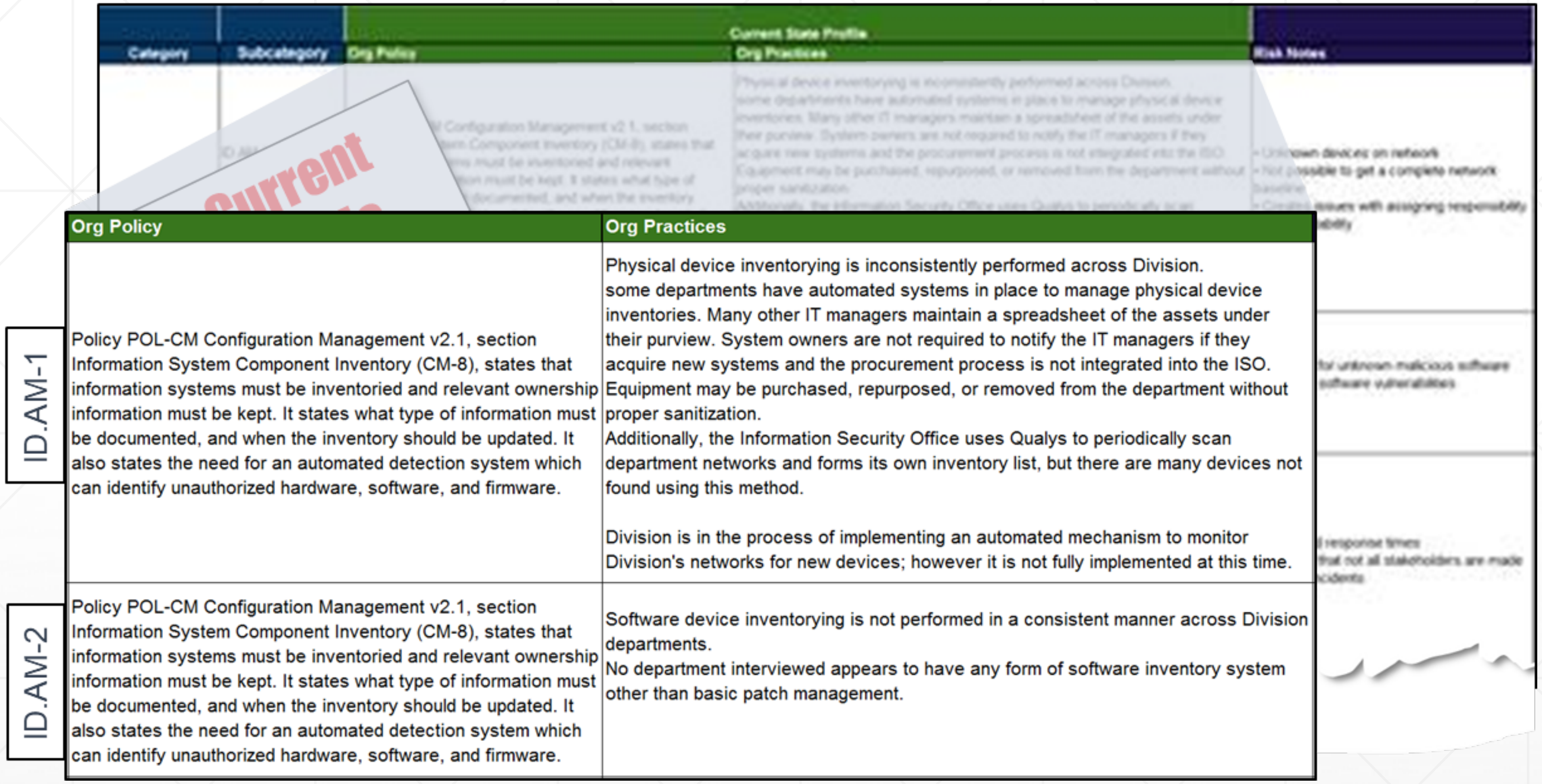


		Current State Profile		
Category	Subcategory	Org Policy	Org Practices	Risk Notes
Asset Management	ID.AM-1: Phys[illegible] devices [illegible]	Pol[illegible] CM Configuration Management v2.1, section [illegible] System Component Inventory (CM-8), states that [illegible] systems must be inventoried and relevant [illegible] information must be kept. It states what type of [illegible] be documented, and when the inventory [illegible] It also states the need for an automated [illegible] which can identify unauthorized hardware, [illegible]	Physical device inventorying is inconsistently performed across Division. some departments have automated systems in place to manage physical device inventories. Many other IT managers maintain a spreadsheet of the assets under their purview. System owners are not required to notify the IT managers if they acquire new systems and the procurement process is not integrated into the ISO. Equipment may be purchased, repurposed, or removed from the department without proper sanitization. Additionally, the Information Security Office uses Qualys to periodically scan department networks and forms its own inventory list, but there are many devices not found using this method. Division is in the process of implementing an automated mechanism to monitor Division's networks for new devices; however it is not fully implemented at this time	• Unknown devices on network • Not possible to get a complete network baseline • Creates issues with assigning responsibility or accountability
	[illegible] Software platforms and applications within the organization are inventoried	Policy POL-CM Configuration Management v2.1, section Information System Component Inventory (CM-8), states that information systems must be inventoried and relevant ownership information must be kept. It states what type of information must be documented, and when the inventory should be updated. It also states the need for an automated detection system which can identify unauthorized hardware, software, and firmware.	Software device inventorying is not performed in a consistent manner across Division departments. No department interviewed appears to have any form of software inventory system other than basic patch management.	• Potential for unknown malicious software • Possible software vulnerabilities
	ID.AM-3: Organizational communication and data flows are mapped	POL-CA Security Assessment and Authorization (v2.1), section titled Information System Connections sets the requirement for Interconnection System Agreements to permit connections outside of the accreditation boundary. Security requirements for the interconnected system must be documented as well as the nature of the information being shared. The system connections must be continually monitored. Division has the stance of "deny-all, permit-by-exception." No policy was provided for baselining network / system information fl[illegible] or for mapping information security	There is an informal understanding of whom to contact in the event of a situation, but unclear communication flow. Very few divisions interviewed claimed to be mapping information data flows.	• Increased response times • Possible that not all stakeholders are made aware of incidents

Current profile

A Current Profile captures the organizations policies, procedures, and practices

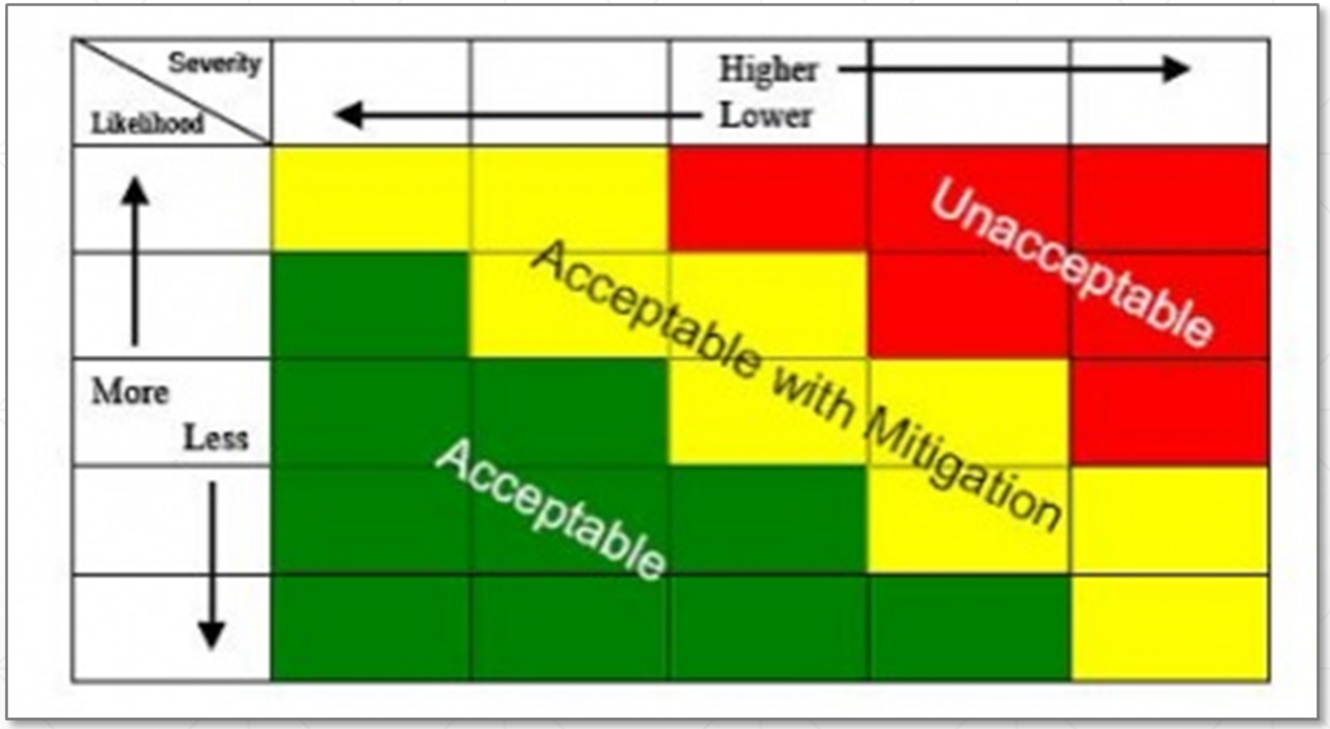
Step 3:
Current Profile


Current State Profile
Category
Subcategory
Org Policy
Org Practices
Risk Notes
ID.AM
Current
- Unknown devices on network
- Not possible to get a complete network baseline
- Creates issues with assigning responsibility
for unknown malicious software
software vulnerabilities
response times
that not all stakeholders are made
incidents

	Org Policy	Org Practices
ID.AM-1	Policy POL-CM Configuration Management v2.1, section Information System Component Inventory (CM-8), states that information systems must be inventoried and relevant ownership information must be kept. It states what type of information must be documented, and when the inventory should be updated. It also states the need for an automated detection system which can identify unauthorized hardware, software, and firmware.	Physical device inventorying is inconsistently performed across Division. some departments have automated systems in place to manage physical device inventories. Many other IT managers maintain a spreadsheet of the assets under their purview. System owners are not required to notify the IT managers if they acquire new systems and the procurement process is not integrated into the ISO. Equipment may be purchased, repurposed, or removed from the department without proper sanitization. Additionally, the Information Security Office uses Qualys to periodically scan department networks and forms its own inventory list, but there are many devices not found using this method. Division is in the process of implementing an automated mechanism to monitor Division's networks for new devices; however it is not fully implemented at this time.
ID.AM-2	Policy POL-CM Configuration Management v2.1, section Information System Component Inventory (CM-8), states that information systems must be inventoried and relevant ownership information must be kept. It states what type of information must be documented, and when the inventory should be updated. It also states the need for an automated detection system which can identify unauthorized hardware, software, and firmware.	Software device inventorying is not performed in a consistent manner across Division departments. No department interviewed appears to have any form of software inventory system other than basic patch management.

A security risk assessment identifies those risks the organization must address

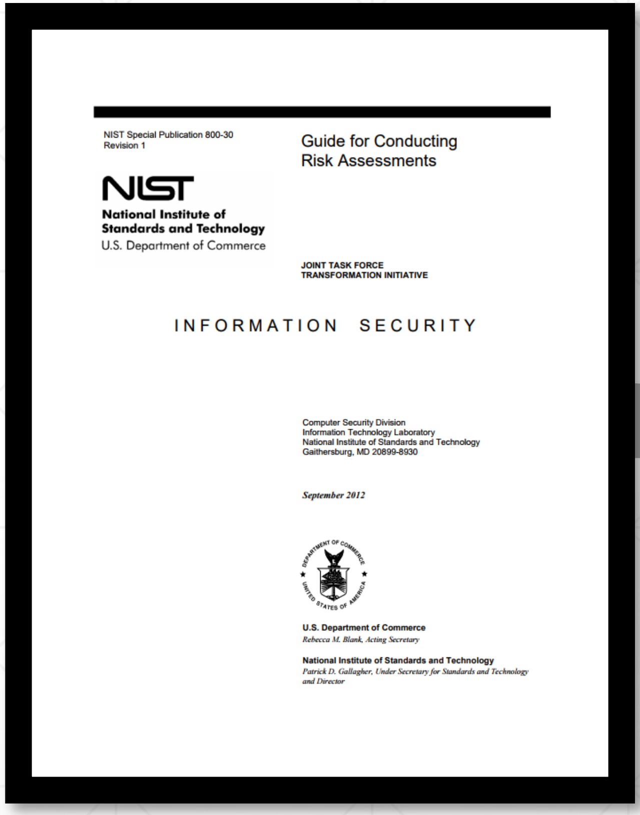
Step 4: Conduct a Risk Assessment



Severity / Likelihood	←		Higher Lower	→	
↑	🟨	🟨	🟥	🟥	🟥
	🟩	🟨	🟨	🟥	🟥
More Less	🟩	🟩	🟨	🟨	🟥
	🟩	🟩	🟩	🟨	🟨
↓	🟩	🟩	🟩	🟩	🟨

Unacceptable
Acceptable with Mitigation
Acceptable

NIST 800-30, Guide for Conducting Risk Assessments, can help define risk to Acme's infrastructure



NIST Special Publication 800-30
Revision 1

Guide for Conducting
Risk Assessments

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

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2012

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

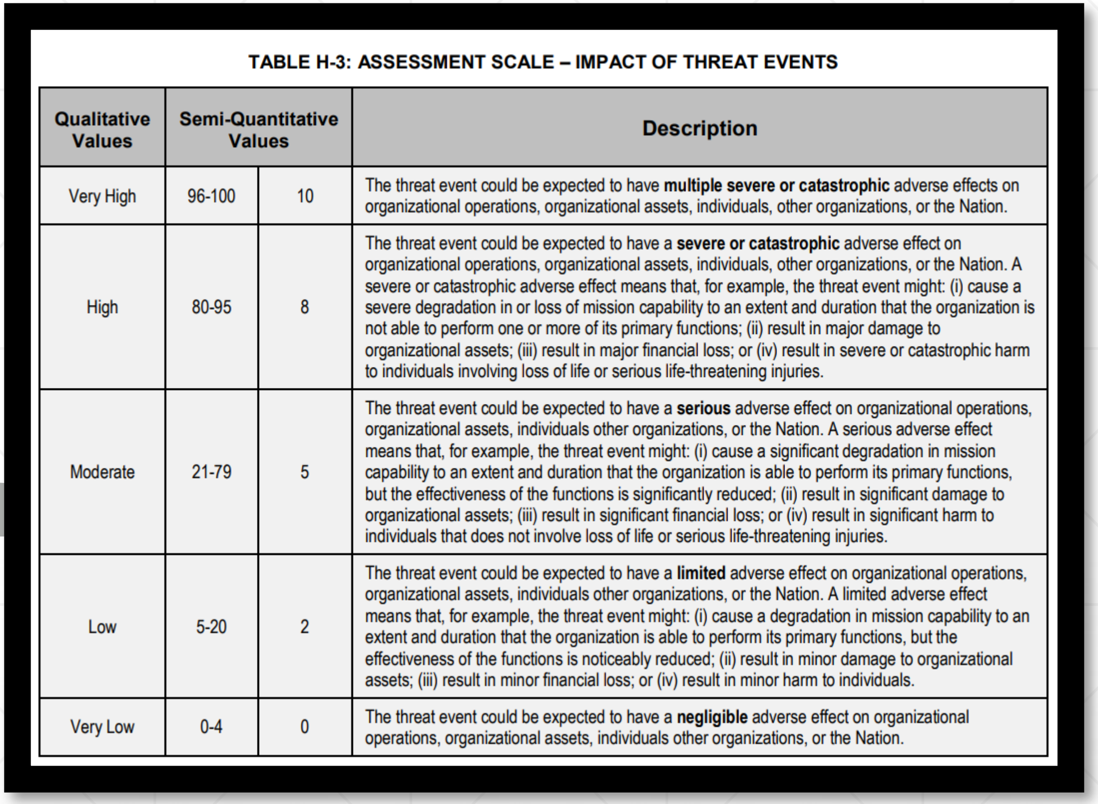


TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

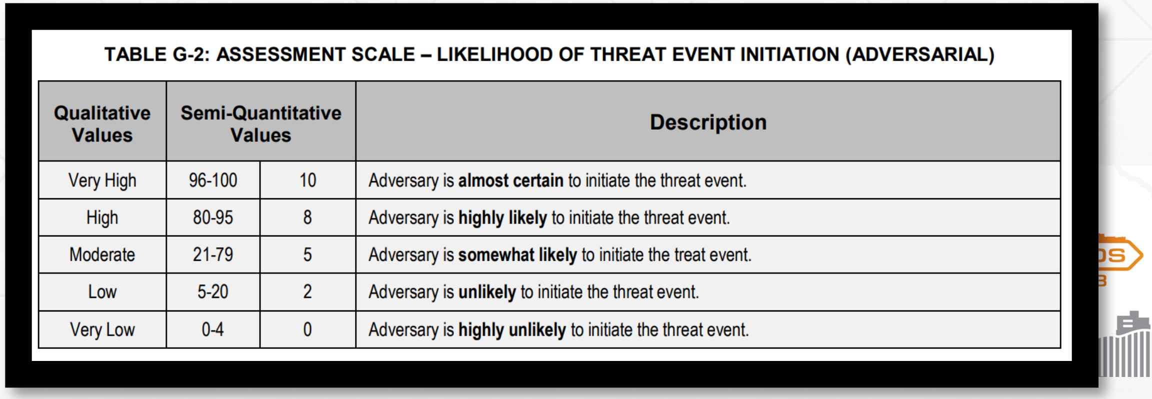


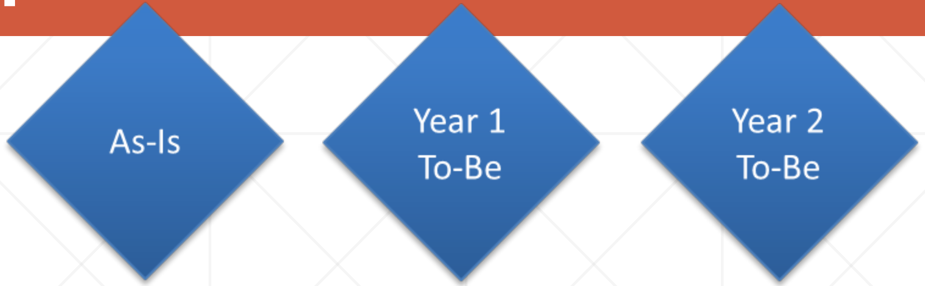
TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

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

Incorporating regulatory requirements with risks establishes a robust cybersecurity program

Step 5:
Create a Target Profile



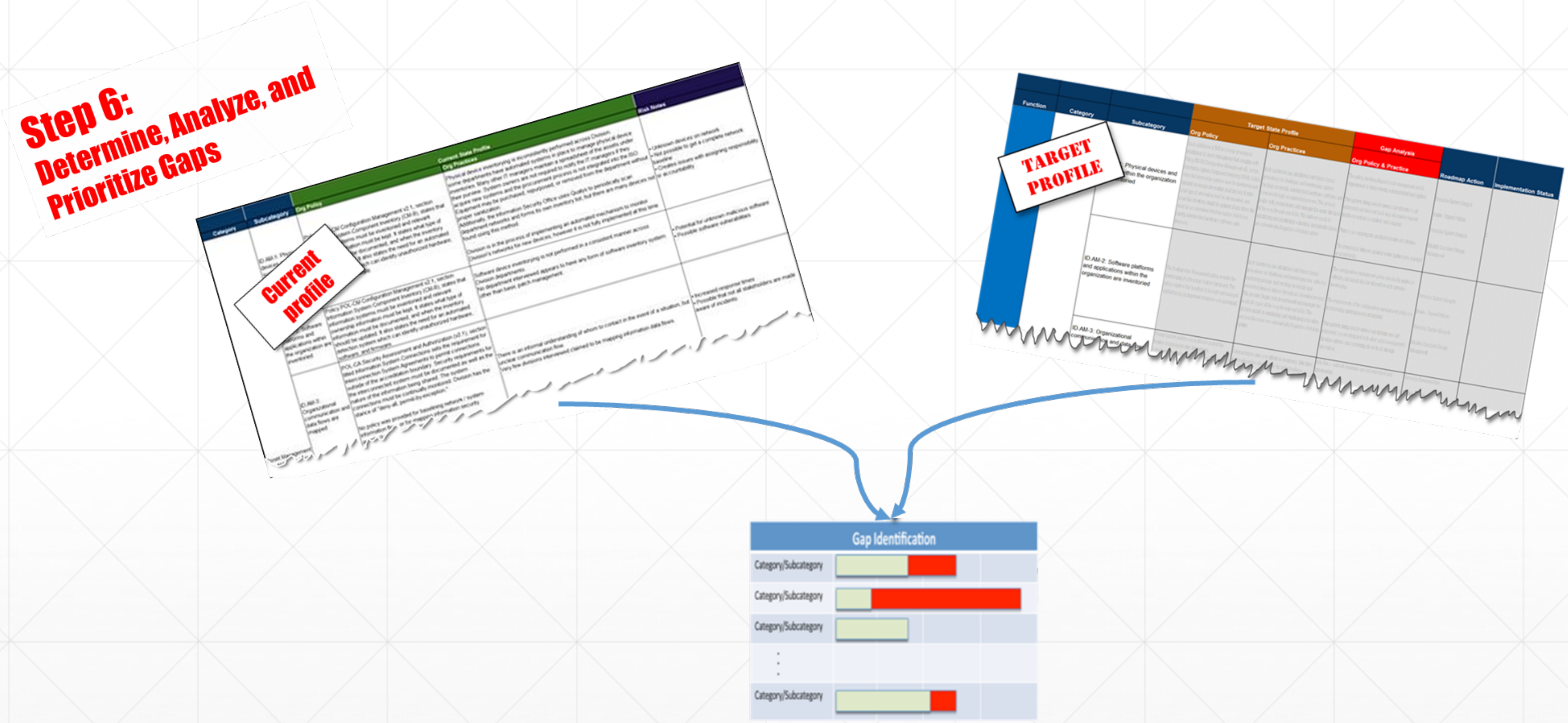
Sub-category	Priority	Gaps	Budget	Year 1 Activities	Year 2 Activities
1	moderate	small	$$$		X
2	high	large	$$	X	
3	moderate	medium	$	X	
…	…	…	…		
98	moderate	none	$$		reassess

Framework supports operating decisions and improvement

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

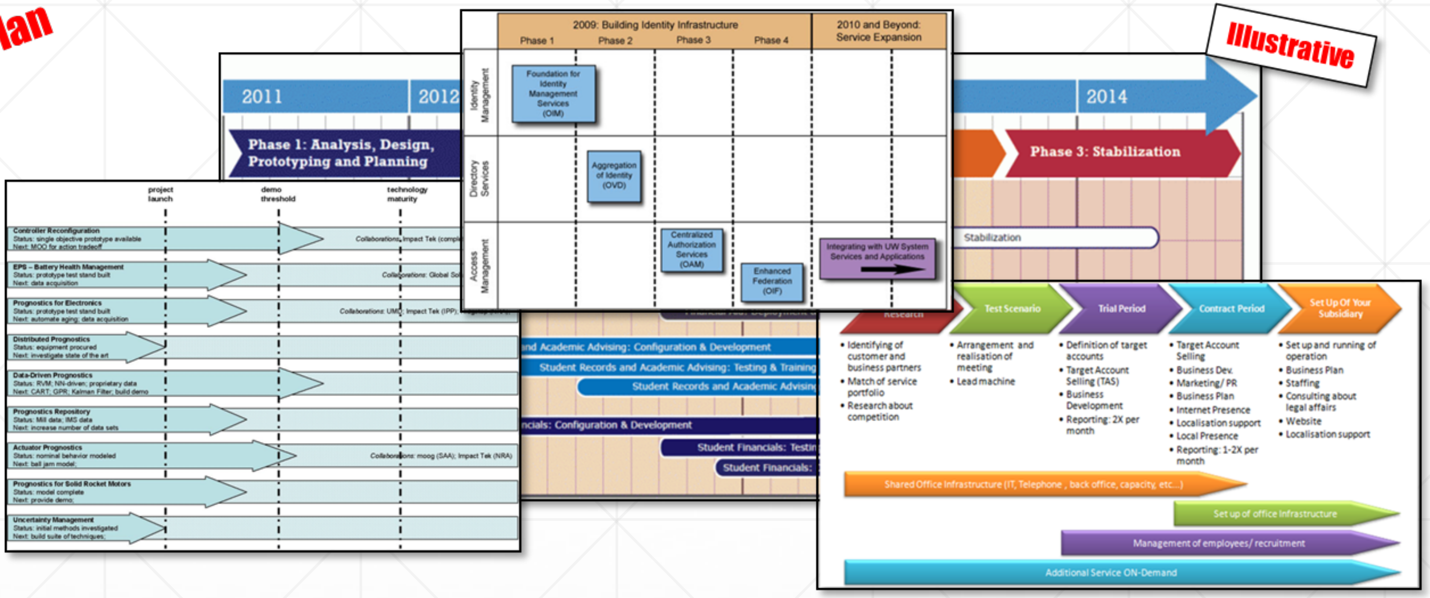
HOTSOS 2018

Next organization assess their current and target cybersecurity programs to identify gaps



The final step is to implement and monitor an action plan to close identified gaps

Step 7: Implement Action Plan



2011
2012
2014
Phase 1: Analysis, Design, Prototyping and Planning
Phase 3: Stabilization
Stabilization
project launch
demo threshold
technology maturity
Controller Reconfiguration
Status: single objective prototype available
Next: MOO for action tradeoff
Collaborations: Impact Tek (compl
EPS – Battery Health Management
Status: prototype test stand built
Next: data acquisition
Collaborations: Global So
Prognostics for Electronics
Status: prototype test stand built
Next: automate aging; data acquisition
Collaborations: UMD; Impact Tek (IPP);
Distributed Prognostics
Status: equipment procured
Next: investigate state of the art
Data-Driven Prognostics
Status: RVM; NN-driven; proprietary data
Next: CART; GPR; Kalman Filter; build demo
Prognostics Repository
Status: Mill data; IMS data
Next: increase number of data sets
Actuator Prognostics
Status: nominal behavior modeled
Next: ball jam model;
Collaborations: moog (SAA); Impact Tek (NRA)
Prognostics for Solid Rocket Motors
Status: model complete
Next: provide demo;
Uncertainty Management
Status: initial methods investigated
Next: build suite of techniques;
2009: Building Identity Infrastructure
Phase 1
Phase 2
Phase 3
Phase 4
2010 and Beyond: Service Expansion
Identity Management
Directory Services
Access Management
Foundation for Identity Management Services (OIM)
Aggregation of Identity (OVD)
Centralized Authorization Services (OAM)
Enhanced Federation (OIF)
Integrating with UW System Services and Applications
and Academic Advising: Configuration & Development
Student Records and Academic Advising: Testing & Training
Student Records and Academic Advising
ncials: Configuration & Development
Student Financials: Testin
Student Financials:
Research
Test Scenario
Trial Period
Contract Period
Set Up Of Your Subsidiary
• Identifying of customer and business partners
• Match of service portfolio
• Research about competition
• Arrangement and realisation of meeting
• Lead machine
• Definition of target accounts
• Target Account Selling (TAS)
• Business Development
• Reporting: 2X per month
• Target Account Selling
• Business Dev.
• Marketing/ PR
• Business Plan
• Internet Presence
• Localisation support
• Local Presence
• Reporting: 1-2X per month
• Set up and running of operation
• Business Plan
• Staffing
• Consulting about legal affairs
• Website
• Localisation support
Shared Office Infrastructure (IT, Telephone , back office, capacity, etc…)
Set up of office Infrastructure
Management of employees/ recruitment
Additional Service ON-Demand

Illustrative

Stakeholders

Milestones

Status

Completion Date

Priority

Specific Action

Resources

Owner

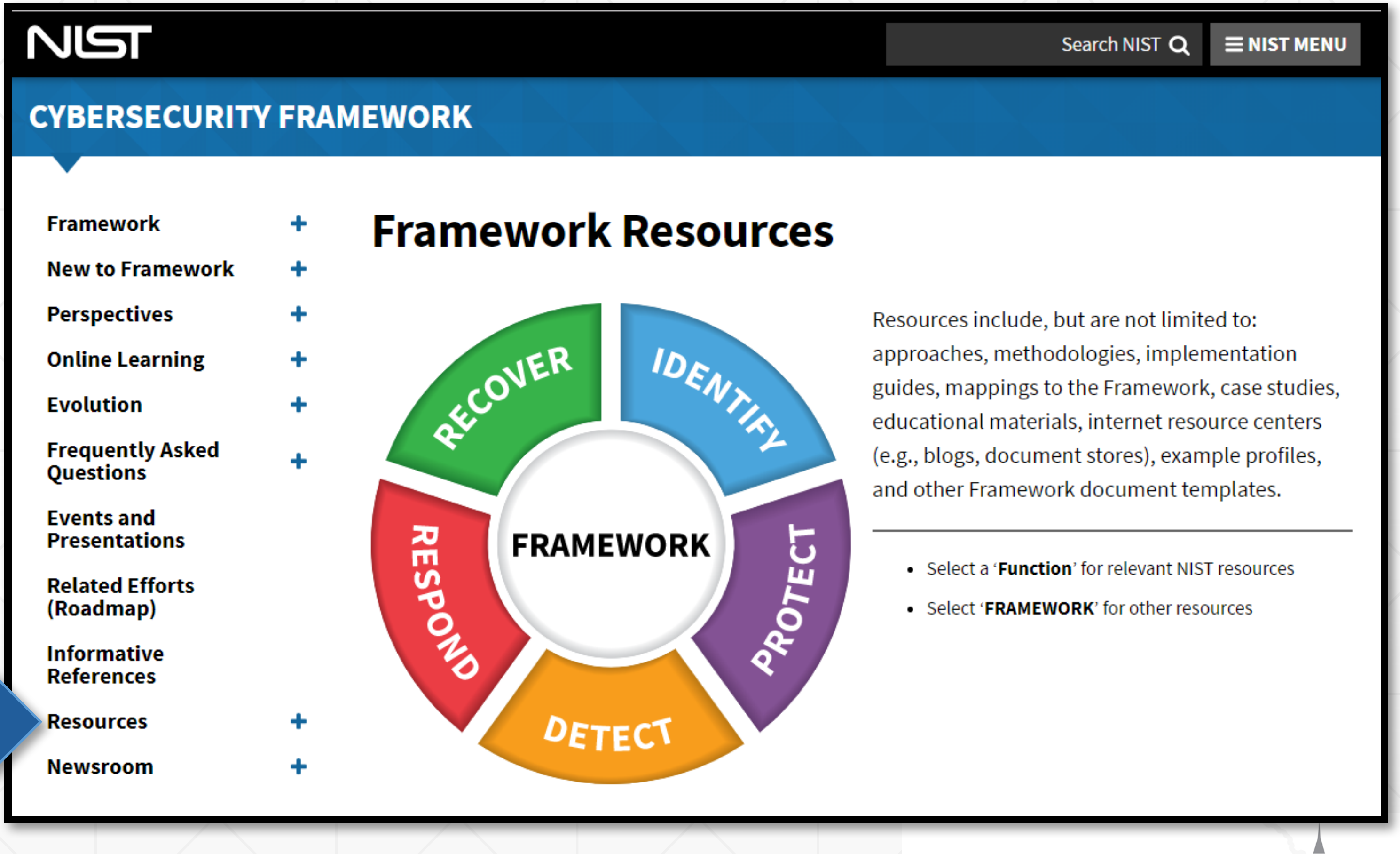
Action Identifier

Dependencies

Rationale

The NIST Cybersecurity Framework website includes resources to help industry use the Framework

https://www.nist.gov/cyberframework



CYBERSECURITY FRAMEWORK

Framework Resources

Resources include, but are not limited to: approaches, methodologies, implementation guides, mappings to the Framework, case studies, educational materials, internet resource centers (e.g., blogs, document stores), example profiles, and other Framework document templates.

- Select a ‘**Function**’ for relevant NIST resources
- Select ‘**FRAMEWORK**’ for other resources

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

A few Examples of Framework Industry Resources

cini Cyber Security National Lab

CIS Sapienza
Cyber Intelligence and Information Security

Italy’s National Framework for Cybersecurity

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

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

FSSCC

Financial Services Sector Specific Cybersecurity “Profile”

U.S. State & Local governments are also using the Framework

DIR

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

ITD

GREATER HOUSTON PARTNERSHIP

Making Houston Greater.

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

NASCIO

Representing Chief Information Officers of the states

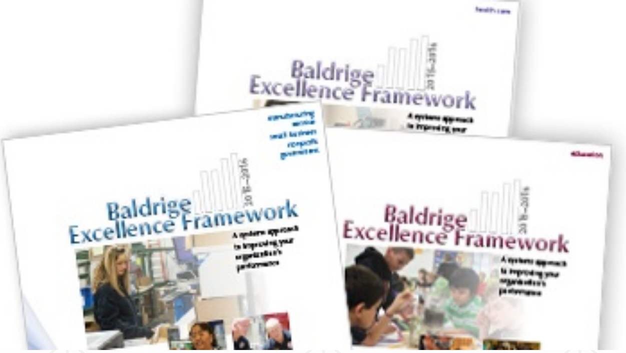
NIST recently published additional guidance for using the Framework

Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Self-Assessment Criteria

Baldrige Cybersecurity Excellence Builder

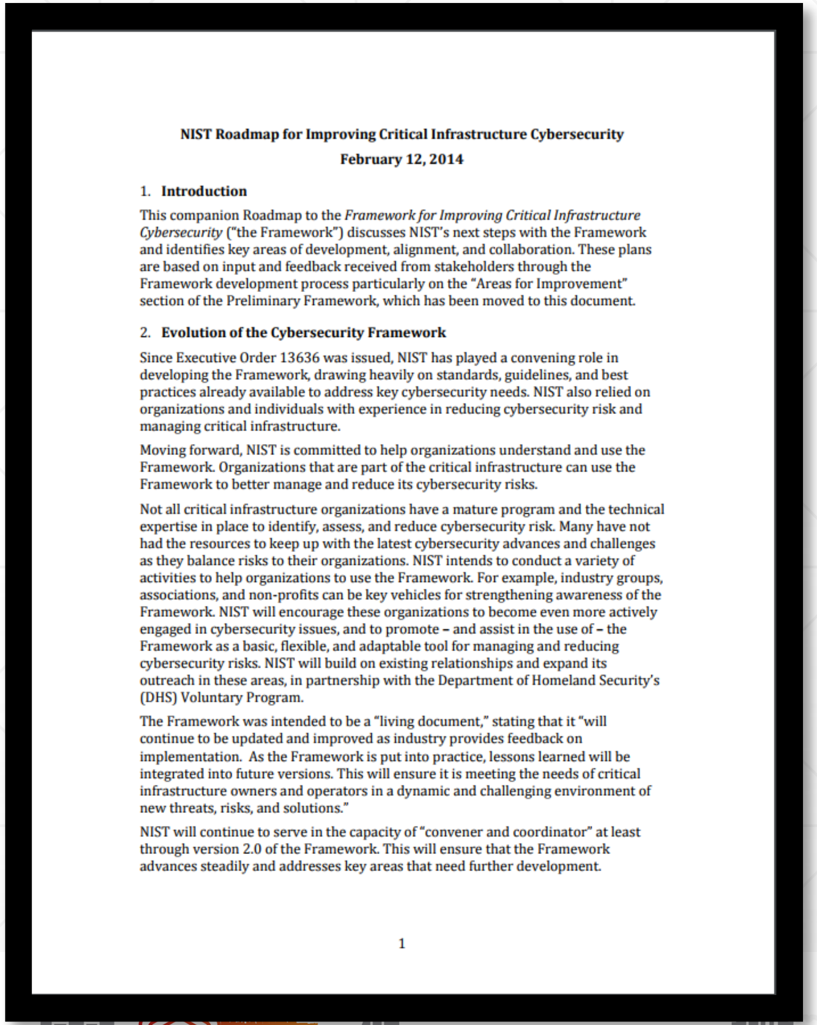

Baldrige Excellence Framework
Baldrige Excellence Framework
Baldrige Excellence Framework

Maritime Profile

U.S. Coast Guard Bulk Liquid Transport Profile

The Roadmap is a companion document to the Cybersecurity Framework

- The Roadmap:
  - identifies key areas of development, alignment, and collaboration
  - provides a description of activities related to the Framework
- Roadmap items are generally:
  - Topics that are meaningful to critical infrastructure cybersecurity risk management
  - Focus areas of both private sector and the federal government
  - Related to Framework, but managed as separate efforts



NIST Roadmap for Improving Critical Infrastructure Cybersecurity

February 12, 2014

1. Introduction

This companion Roadmap to the *Framework for Improving Critical Infrastructure Cybersecurity* ("the Framework") discusses NIST's next steps with the Framework and identifies key areas of development, alignment, and collaboration. These plans are based on input and feedback received from stakeholders through the Framework development process particularly on the "Areas for Improvement" section of the Preliminary Framework, which has been moved to this document.

2. Evolution of the Cybersecurity Framework

Since Executive Order 13636 was issued, NIST has played a convening role in developing the Framework, drawing heavily on standards, guidelines, and best practices already available to address key cybersecurity needs. NIST also relied on organizations and individuals with experience in reducing cybersecurity risk and managing critical infrastructure.

Moving forward, NIST is committed to help organizations understand and use the Framework. Organizations that are part of the critical infrastructure can use the Framework to better manage and reduce its cybersecurity risks.

Not all critical infrastructure organizations have a mature program and the technical expertise in place to identify, assess, and reduce cybersecurity risk. Many have not had the resources to keep up with the latest cybersecurity advances and challenges as they balance risks to their organizations. NIST intends to conduct a variety of activities to help organizations to use the Framework. For example, industry groups, associations, and non-profits can be key vehicles for strengthening awareness of the Framework. NIST will encourage these organizations to become even more actively engaged in cybersecurity issues, and to promote – and assist in the use of – the Framework as a basic, flexible, and adaptable tool for managing and reducing cybersecurity risks. NIST will build on existing relationships and expand its outreach in these areas, in partnership with the Department of Homeland Security's (DHS) Voluntary Program.

The Framework was intended to be a "living document," stating that it "will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions."

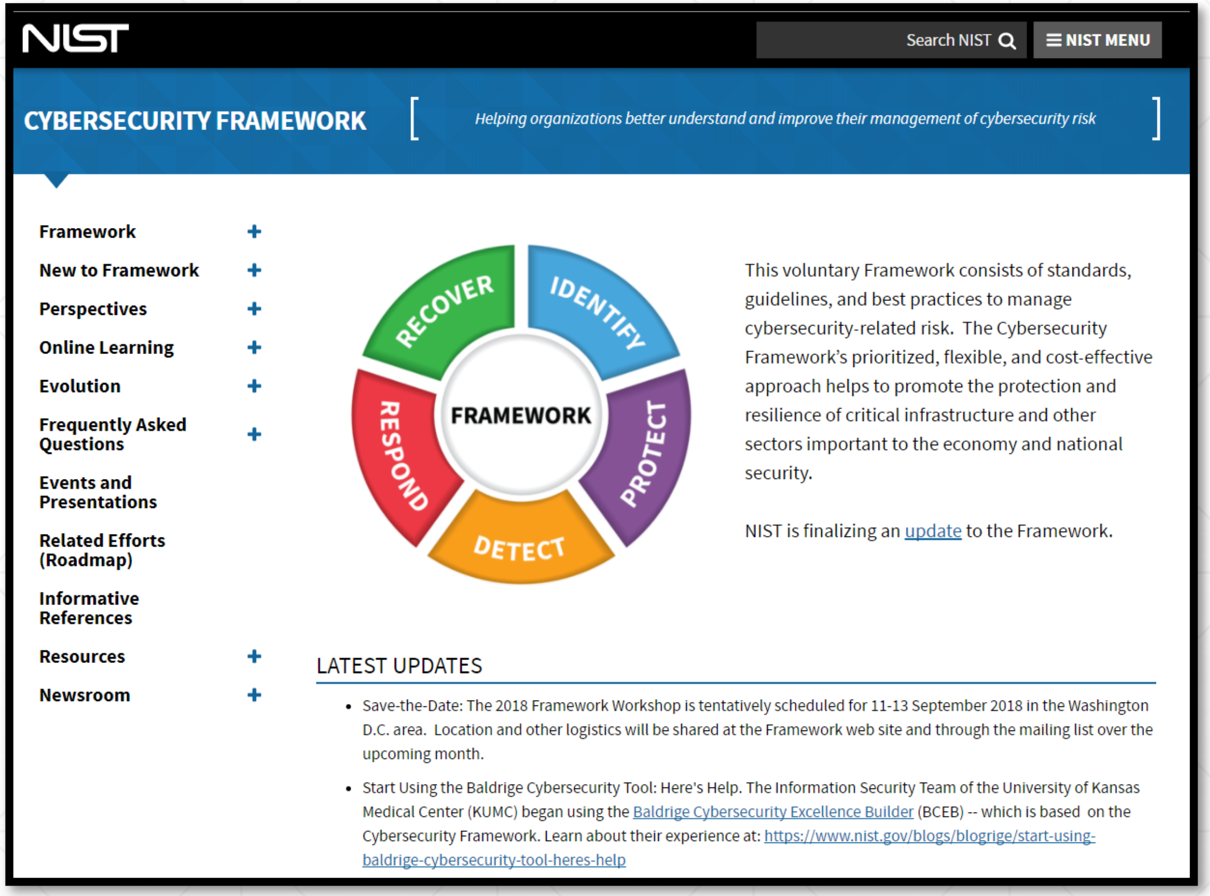
NIST will continue to serve in the capacity of "convener and coordinator" at least through version 2.0 of the Framework. This will ensure that the Framework advances steadily and addresses key areas that need further development.

You can help promote and share your experience using the Framework

- Stakeholders should consider activities to:
  - Customize 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.
  - Submit a paper during the NIST call for abstracts
  - Share your Framework resources with NIST at cyberframework@nist.gov.
  - Participate in Framework workshops

More information and resources are available on the Cybersecurity Framework website

- Relevant news and information:
  - https://www.nist.gov/cyberframework
- Additional cybersecurity resources:
  - https://csrc.nist.gov/
- Questions, comments, ideas:
  - cyberframework@nist.gov



CYBERSECURITY FRAMEWORK

[Helping organizations better understand and improve their management of cybersecurity risk]

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

NIST is finalizing an update to the Framework.

LATEST UPDATES

- Save-the-Date: The 2018 Framework Workshop is tentatively scheduled for 11-13 September 2018 in the Washington D.C. area. Location and other logistics will be shared at the Framework web site and through the mailing list over the upcoming month.
- Start Using the Baldrige Cybersecurity Tool: Here's Help. The Information Security Team of the University of Kansas Medical Center (KUMC) began using the Baldrige Cybersecurity Excellence Builder (BCEB) -- which is based on the Cybersecurity Framework. Learn about their experience at: https://www.nist.gov/blogs/blogrige/start-using-baldrige-cybersecurity-tool-heres-help