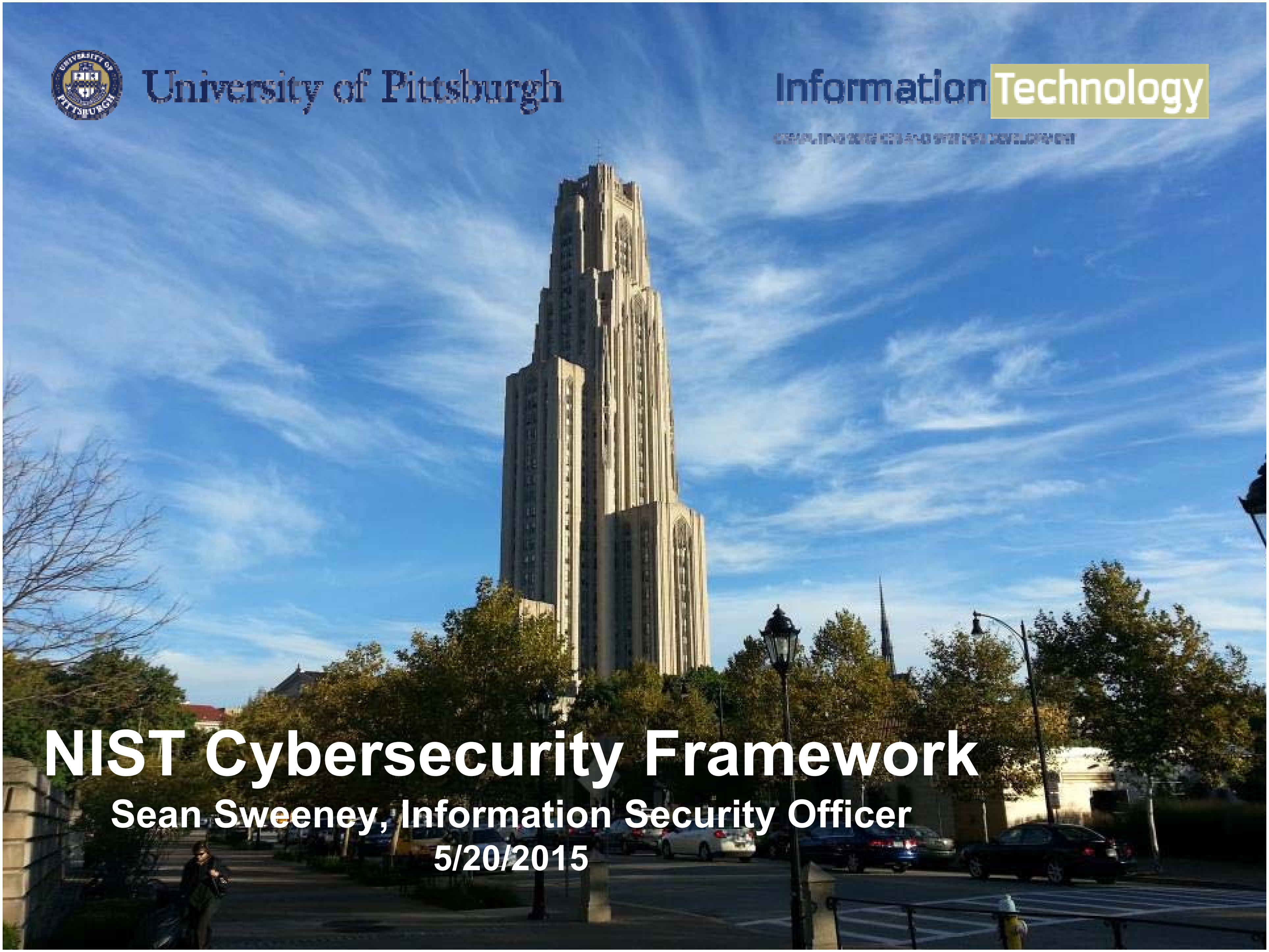
University of Pittsburgh

Information Technology

COMPUTING SERVICES AND SYSTEMS DEVELOPMENT



NIST Cybersecurity Framework

Sean Sweeney, Information Security Officer

5/20/2015

Overview

- The University of Pittsburgh
- NIST Cybersecurity Framework
- Pitt NIST Cybersecurity Framework Program
- Wrap Up
- Questions

The University of Pittsburgh

Snapshot: Community

Bradford
Titusville
Pittsburgh
Johnstown
Greensburg

Responsibility Centers = 49

Snapshot: Information Security Office

- 10 full-time security professionals*
  - – Responsible for:
    - Enterprise Network Firewalls
    - Security Monitoring and Alerting
    - Incident Response
    - Policy, Risk, and Compliance
    - Awareness
    - Security Tools (Managed & Self-service)

*Supported by 230 Central IT Professionals

Snapshot: Target-rich Environment

- Size and speed of network
- Collaborative nature of research—open access
- Diverse information-rich environment
- Fluid user population
- Decentralized IT
- BYOD

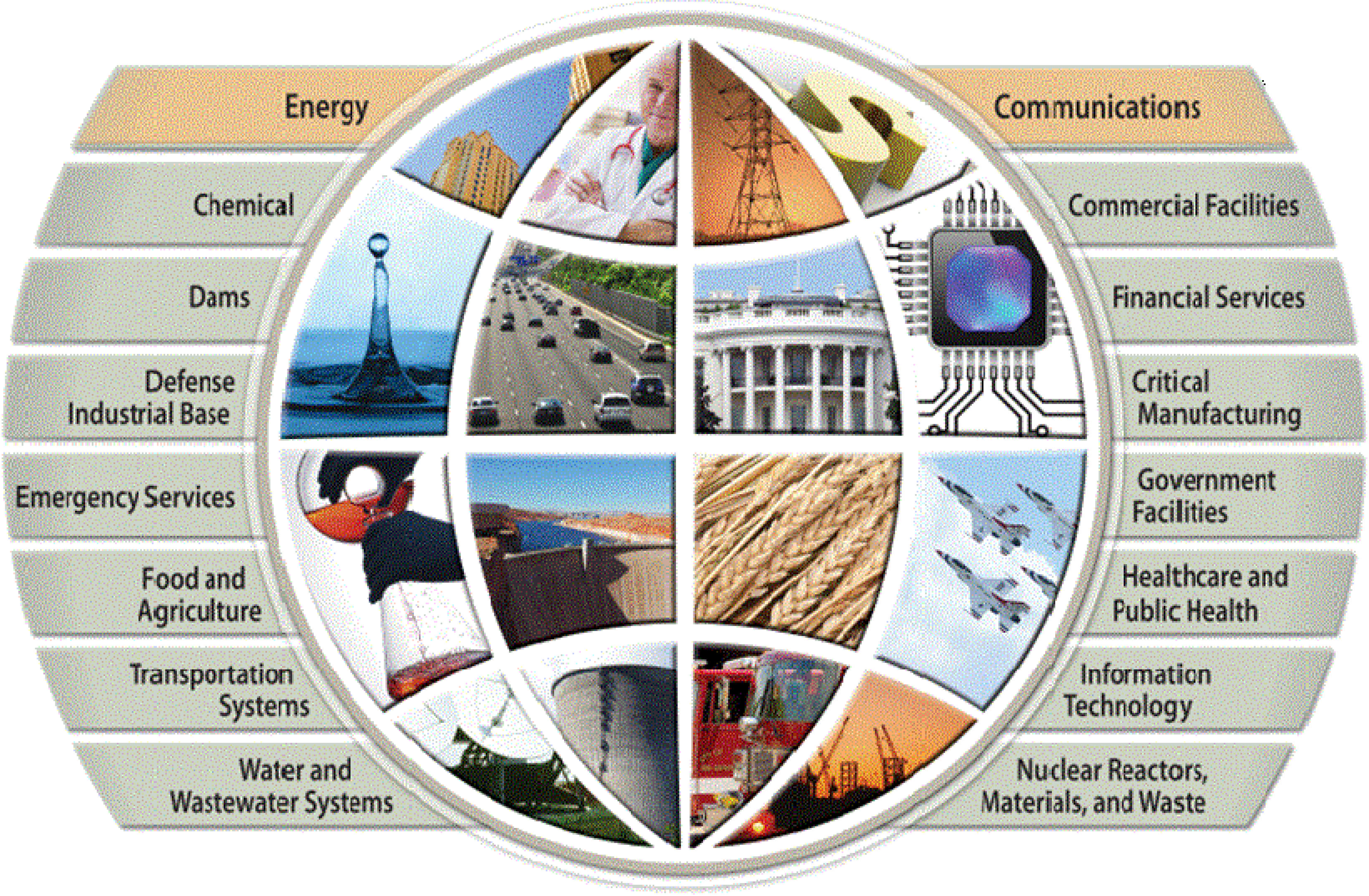
NIST Cybersecurity Framework

Origin of the NIST CSF

- Executive Order 13636, Improving Critical Infrastructure Cybersecurity, Feb. 2013
  - Directed NIST to work with stakeholders to develop voluntary framework – based on existing standards, guidelines, and practices – for reducing cyber risks to critical infrastructure

NIST
National Institute of
Standards and Technology

Presidential Policy Directive 21

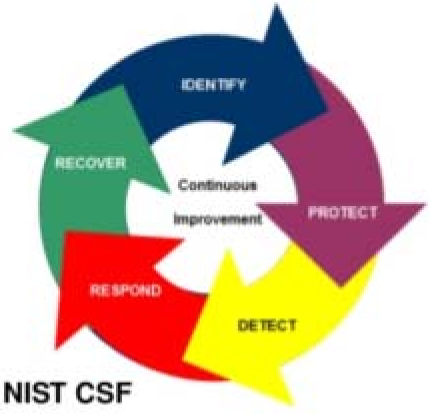


NIST CSF Overview

- Provides standard measurement that organizations can use to measure risk and improve security
- Includes senior management understanding of cyber risk
- Currently voluntary, but likely the de-facto standard in event of a breach
- Common language, not “government speak”
- Maps to COBIT, ISO, 800-53, etc.

NIST CSF Design

- Core
  - – Five Functions (Identify, Protect, Detect, Respond, Recover)
    - 22 categories, 98 subcategories
- Implementation tiers
  - – Partial, Risk Informed, Repeatable, Adaptive
  - – One size does not fit all
- Profiles
  - – Current & Target



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

Identify

- Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
  - ID.AM-1: Physical devices and systems within the organization are inventoried
  - ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources

Protect

- Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
  - PR.AC-1: Identities and credentials are managed for authorized devices and users
  - PR.DS-1: Data-at-rest is protected

Detect

- Develop and implement the appropriate activities to identify the occurrence of cybersecurity event.
  - DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
  - DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

Respond

- Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
  - RS.RP-1: Response plan is executed during or after an event
  - RS.MI-1: Incidents are contained

Recover

- Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
  - RC.RP-1: Recovery plan is executed during or after an event
  - RC.CO-1: Public relations are managed

Tier 1 Partial

- Risk Management Process
  - Ad hoc
- Integrated Risk Management Program
  - Limited awareness of risk. Managed case by case basis.
- External Participation
  - No processes in place to collaborate.

Tier 2 Risk Informed

- Risk Management Process
  - Established by management, but not policy
- Integrated Risk Management Program
  - Awareness of risk. Managed well. No organization wide approach.
- External Participation
  - No formal processes for interaction and sharing.

Tier 3 Repeatable

- Risk Management Process
  - Expressed by policy. Practices updated regularly.
- Integrated Risk Management Program
  - Organization wide approach to manage cyber risk.
- External Participation
  - Receives information from partners for collaboration

Tier 4 Adaptive

- Risk Management Process
  - Continuous improvement incorporating advanced technologies and practices.
- Integrated Risk Management Program
  - Cyber risk management is part of culture
- External Participation
  - Actively shares information with partners

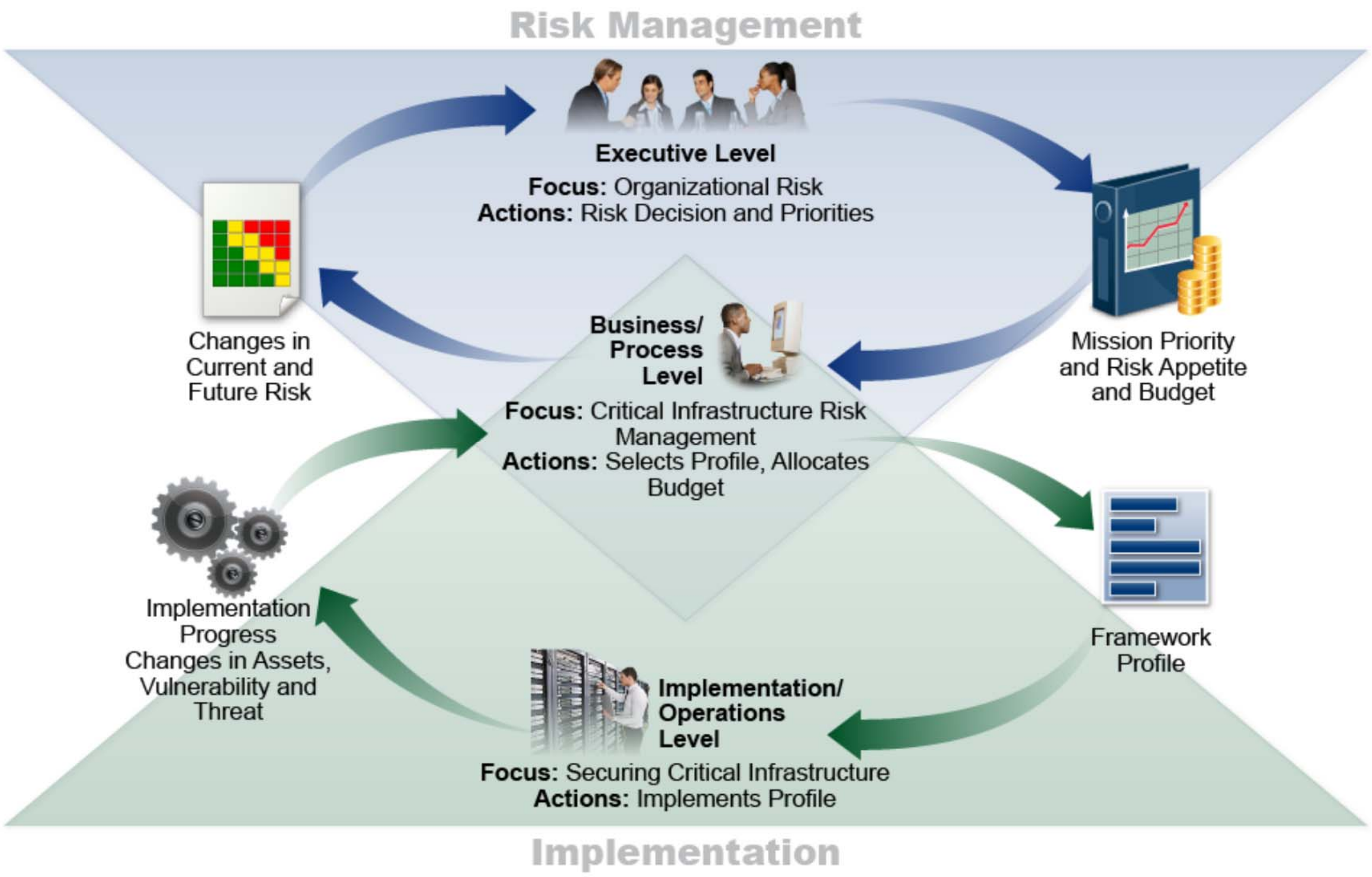
Note About Tiers

- Tiers do not represent maturity levels.
- Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.
- Successful implementation of the Framework is based upon achievement of the outcomes described in the organization’s Target Profile(s) and not upon Tier determination.

Profiles

- Alignment of the functions, categories, and subcategories with the business requirements, risk tolerance, and resources of the organization.
- Current and Target
  - Current outcomes vs those needed to achieve goals.
- Comparison of Profiles
  - Gap mitigation prioritized and roadmap created
  - Allows organization to prioritize resources
- “Living” document

NIST CSF Decision Flows



Risk Management

Executive Level

Focus: Organizational Risk
Actions: Risk Decision and Priorities

Mission Priority and Risk Appetite and Budget

Changes in Current and Future Risk

Business/ Process Level

Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget

Framework Profile

Implementation Progress Changes in Assets, Vulnerability and Threat

Implementation/ Operations Level

Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

Pitt NIST CSF Program

Steps

1. Prioritize and Scope
2. Orient, Create Current Profile
3. Conduct Risk Assessment
4. Create Target Profile
5. Determine, Analyze, and Prioritize Gaps
6. Implement Plan of Action

Year 1 (July 1, 2014 – June 30, 2015)

- Focused on enterprise network and systems managed by central IT.
- Included central IT stakeholders in preparing profiles
- Presented profiles and roadmap to executive management
- Internal Audit review

Year 2 (July 1, 2015 – June 30, 2016)

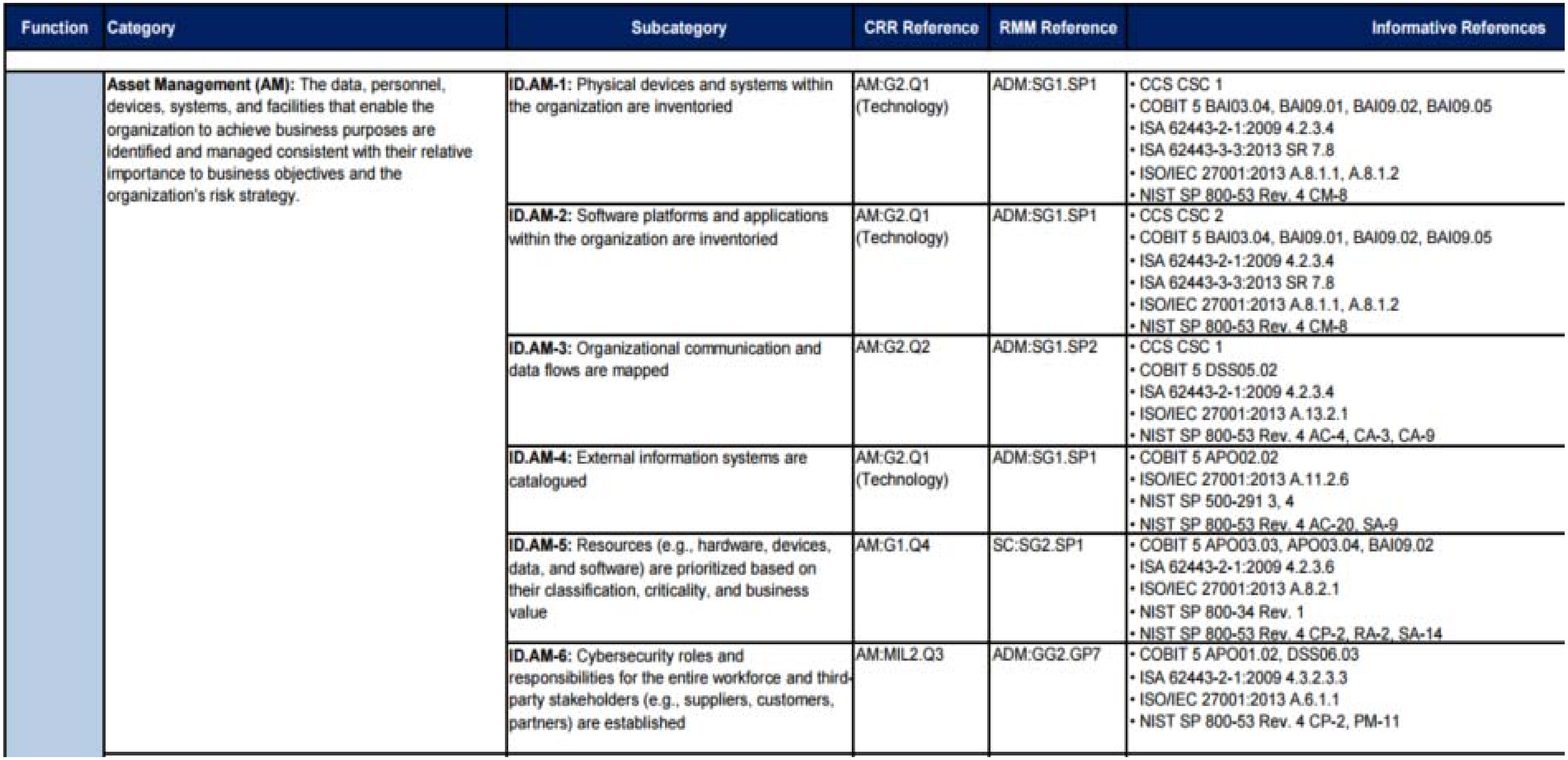
- Expand scope of the system and assets by using framework on two key non-central units.
- Adapt framework for departmental/school use.
- Train key personnel to perform current state assessment.
- Information Security to create target profile, gap analysis, and remediation plan with input from departments/schools.

Wrap Up

Future of NIST CSF

- Roadmap published with CSF
  - Identified key areas of development, alignment, and collaboration.
- Critical Infrastructure Cyber Community Voluntary Program
  - Focuses on Use, Outreach, and Feedback
  - Onsite or self-guided Cyber Resilience Review
- Many critical sectors still determining how to apply framework

Cross walking the NIST CSF



Function	Category	Subcategory	CRR Reference	RMM Reference	Informative References
	Asset Management (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	AM:G2.Q1 (Technology)	ADM:SG1.SP1	• CCS CSC 1 • COBIT 5 BAI03.04, 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-2: Software platforms and applications within the organization are inventoried	AM:G2.Q1 (Technology)	ADM:SG1.SP1	• CCS CSC 2 • COBIT 5 BAI03.04, 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	AM:G2.Q2	ADM:SG1.SP2	• 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
		ID.AM-4: External information systems are catalogued	AM:G2.Q1 (Technology)	ADM:SG1.SP1	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 500-291 3, 4 • 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	AM:G1.Q4	SC:SG2.SP1	• 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 800-34 Rev. 1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	AM:MIL2.Q3	ADM:GG2.GP7	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PM-11

Thoughts on NIST CSF

- Allows communication of cyber risk up and across
- Not overly prescriptive, but not vague
- Not purely an IT controls exercise
- Able to apply to unique enterprise without modification
- Allows for prioritization of risk and associated resources
- Future unclear

Questions?