Grant Thornton

How did we get here and what's next?

May 9, 2019

Glenn Keaveny
Director
National Advisory Services
Public Sector | Risk Advisory Services
T: 703-562-5946
glenn.keaveny@us.gt.com

Grant Thornton

Learning Objectives

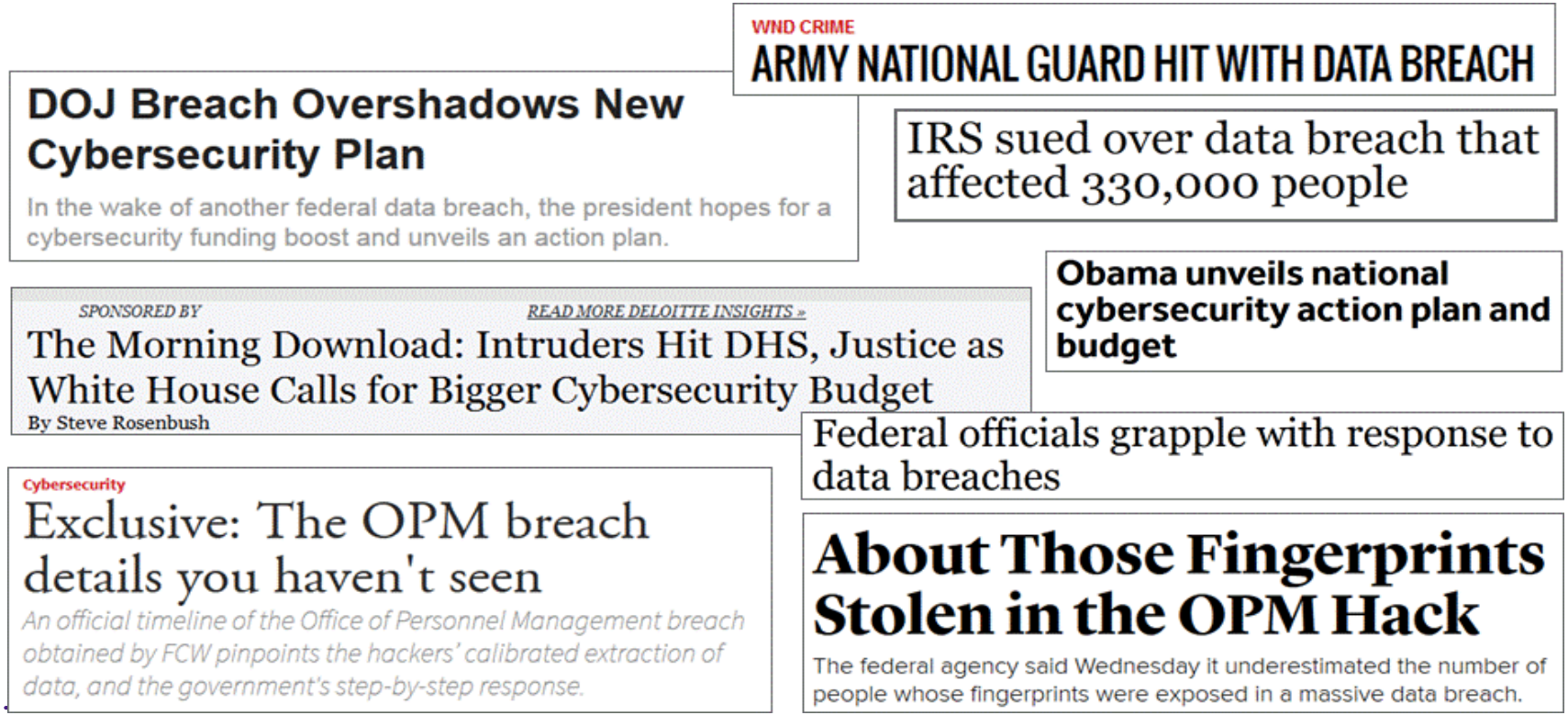
- NIST History
- Tools and Techniques to Operate Under Current Standards and Conditions
- What Does the Future Look Like?
- What to do Now to be Ready for Tomorrow

Agenda

- NIST History (Why NIST?)
- NIST Mission
- Frameworks
- Tools and Techniques
  - First Things First (Implementation and Remediation)
  - Not My Problem (Inheritance)
  - Reciprocity
- The NIST Horizon
- What to do Now
- Questions

Why NIST?

Why NIST?

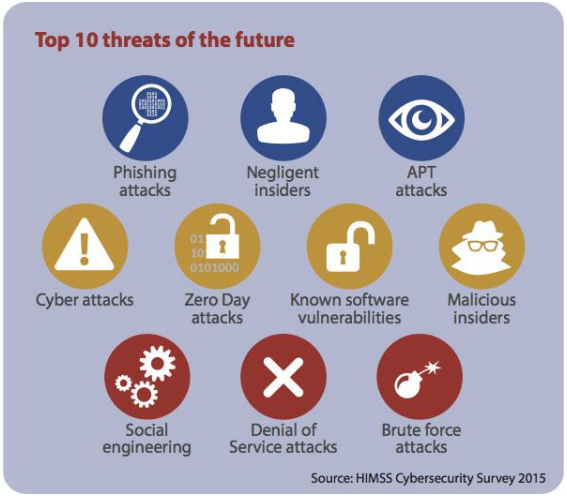


Grant Thornton

Why NIST?

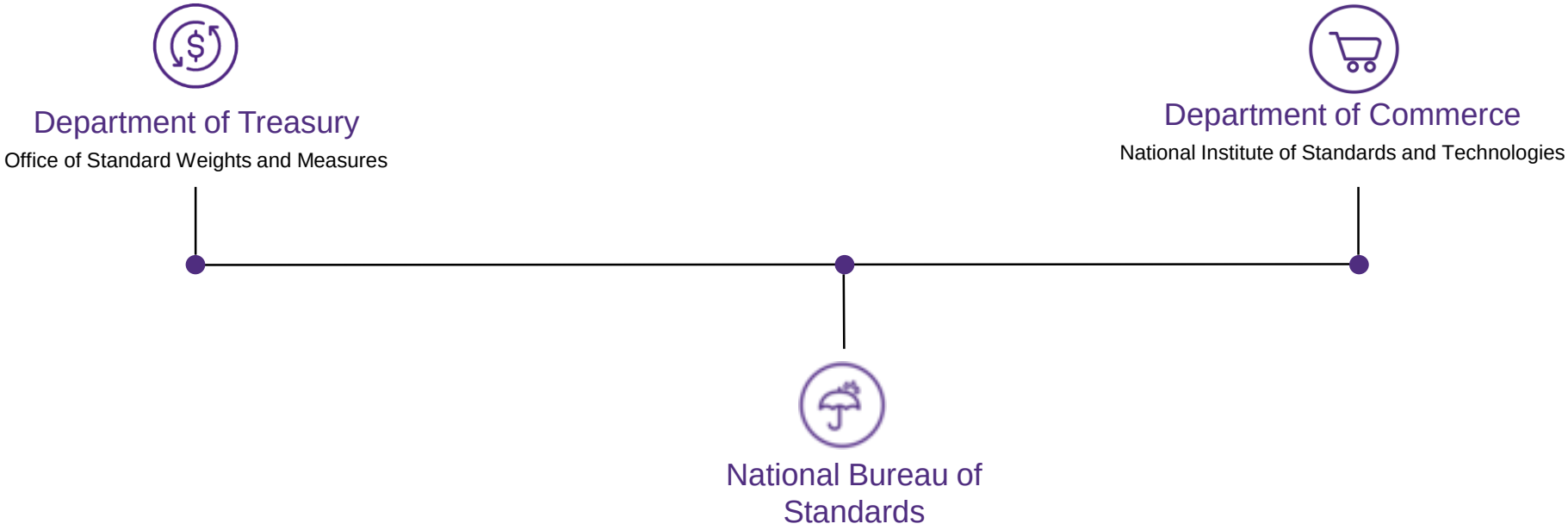
- IBM-Ponemon Study
  - The average cost incurred for each lost or stolen record containing sensitive and confidential information increased from **$154** to **$158.** Similar numbers show that in 2014 that number was **$145**

    - Loss of reputation difficult to quantify
    - Leaks: Unprecedented leaks of comprehensive datasets, with over 4 billion compromised records exposed.
    - Methods: Cybercriminals continue to favor older attack methods to gain access to valuable data and resources, including command injection, malware and ransomware.



Grant Thornton

NIST History



NIST History

- 1821 - “Weights and measures may be ranked among the necessities of life to every individual human society” – John Quincy Adams

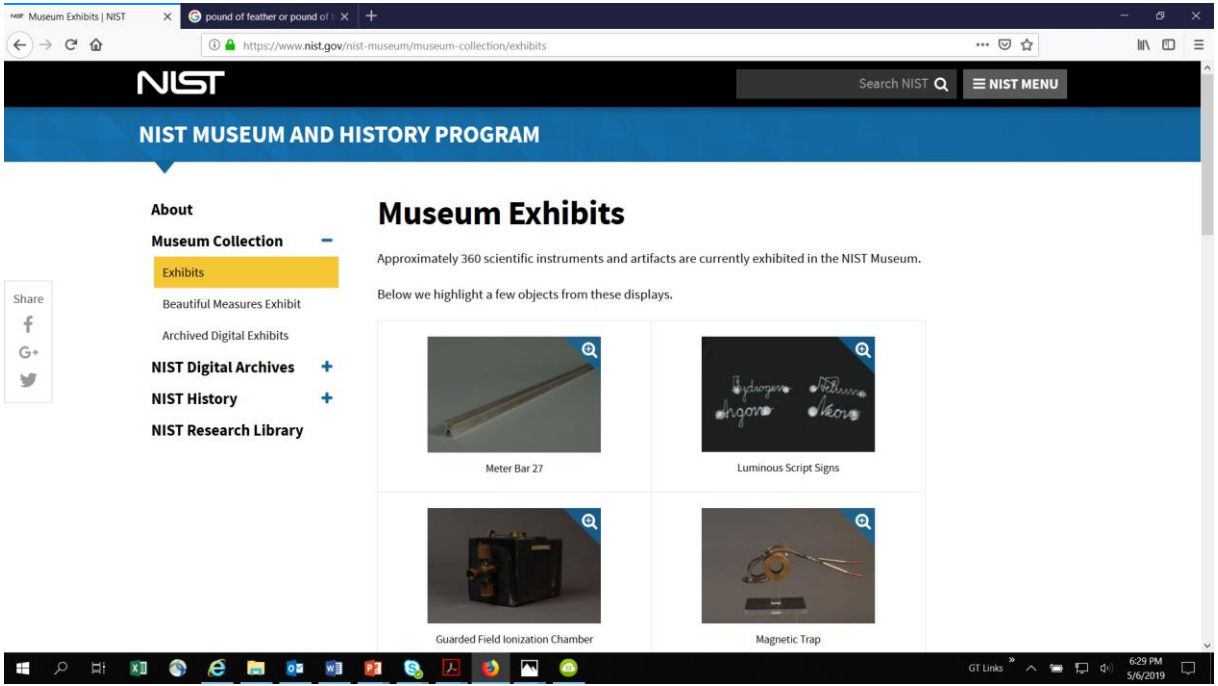
- 1830-1901 – The Office of Standard Weights and Measures

- 1838 – The United States establishes a uniform standard of weights and measures

- 1901 - National Bureau of Standards is established to provide standard weights and measures and serve as the national physical laboratory
  - Meteorological Services
  - Expands Weights and Measures (Materials, Light, Electricity)

- 1988 – National Institute of Standards and Technology (NIST)
  - Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

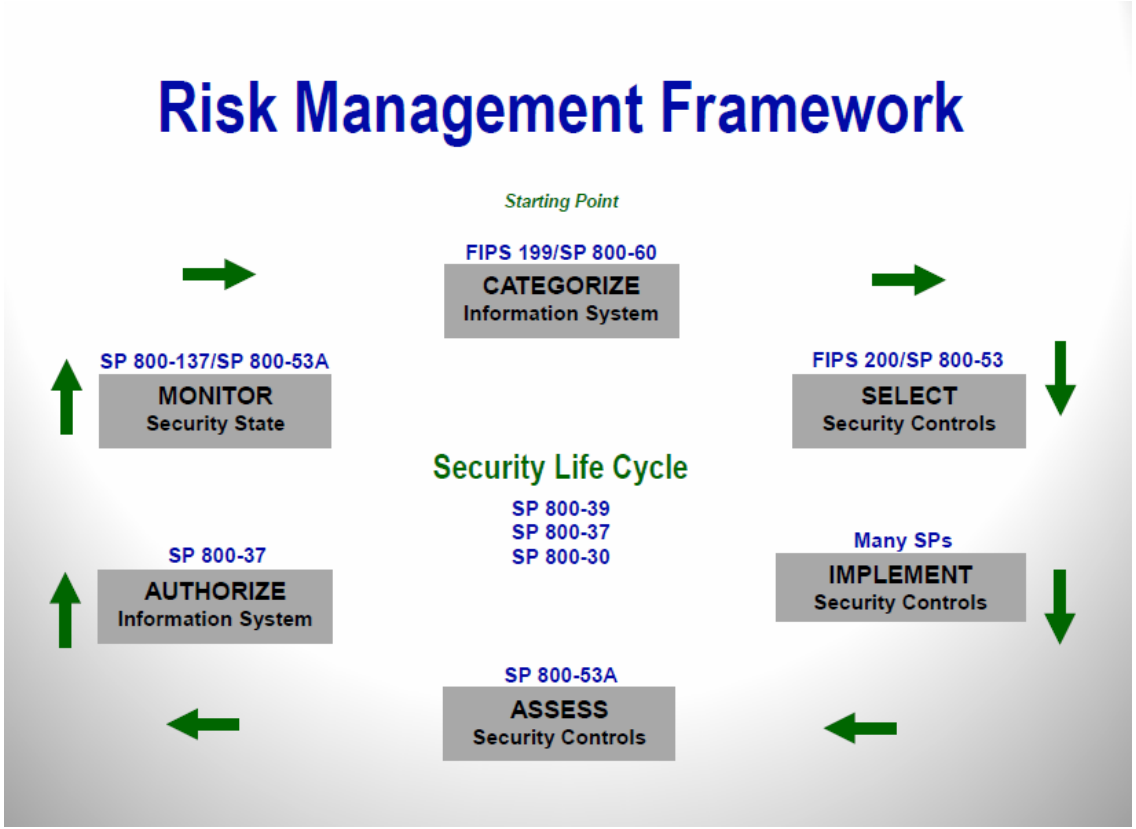
NIST History



Frameworks

- NIST has 1,102 Cybersecurity Publications
  - NIST SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems a: A Security Life Cycle Approach (RMF)
    - NIST SP 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Information
    - NIST SP 800-171, Revision 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  - Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (CSF)
  - Federal Risk and Authorization Management Program (FedRAMP)

RMF



RMF

- The risk-based approach to risk management considers:
  - organization-wide risk
  - integration of activities into the system development life cycle (SDLC)
    - Will be discussed next slide
  - considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.

Applicable NIST Publications:

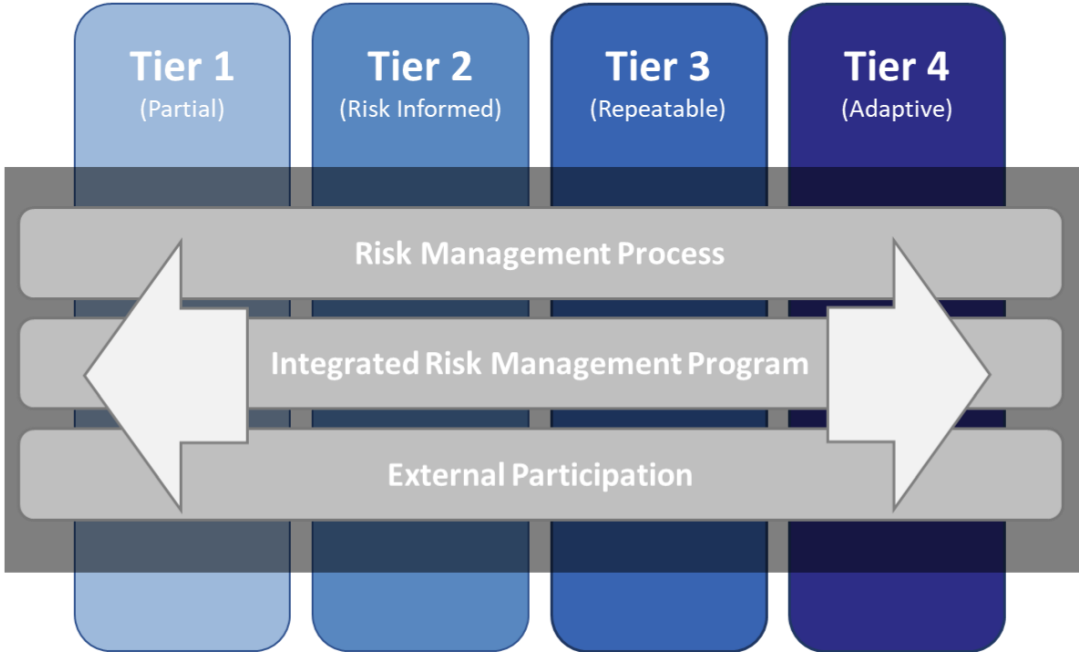
- NIST SP 800-39 – Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-37 Rev 1 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-30 Rev 1 – Guide for Conducting Risk Assessments
- NIST SP 800-160 - System Security Engineering

Grant Thornton

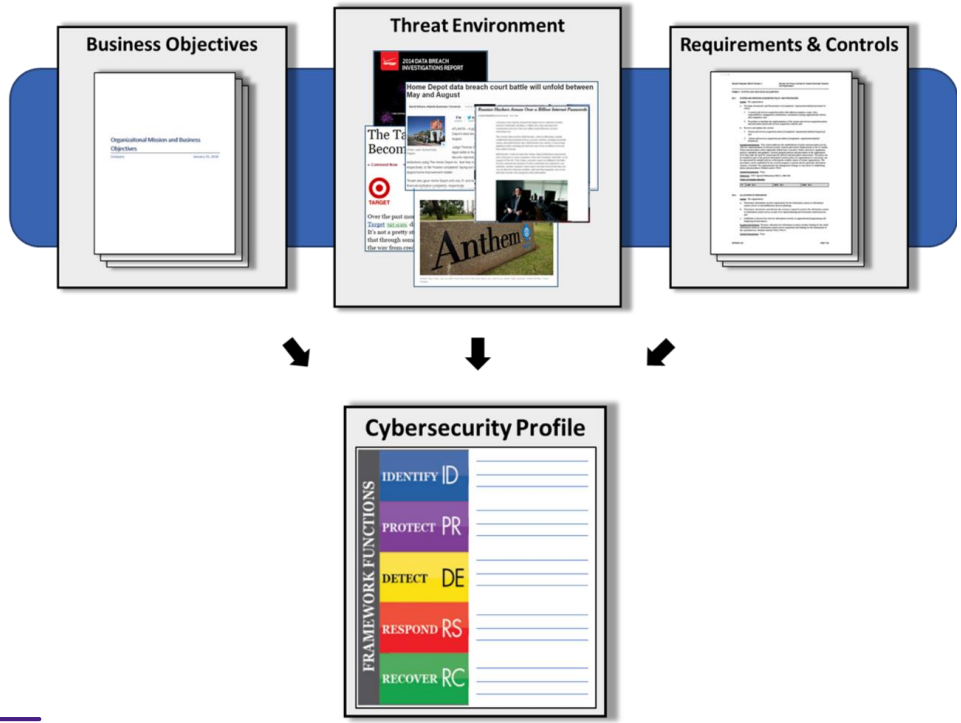
CSF

- **NIST Cybersecurity Framework – Overview**
- Executive Order 13631 (Feb. 2013) – Directed a "Framework for Improving Critical Infrastructure Cybersecurity"
  - NIST to lead creation of Framework working with stakeholders from industry, government, and academia
  - Prioritized, risk-based, include performance measures, etc.
  - Identify and leverage established cybersecurity standards, guidelines, and practices
- *Final* NIST CSF v1.1
- Components of NIST CSF
  - Framework Tiers
  - Framework Profiles – *Current* vs. *Target*
  - Framework Core

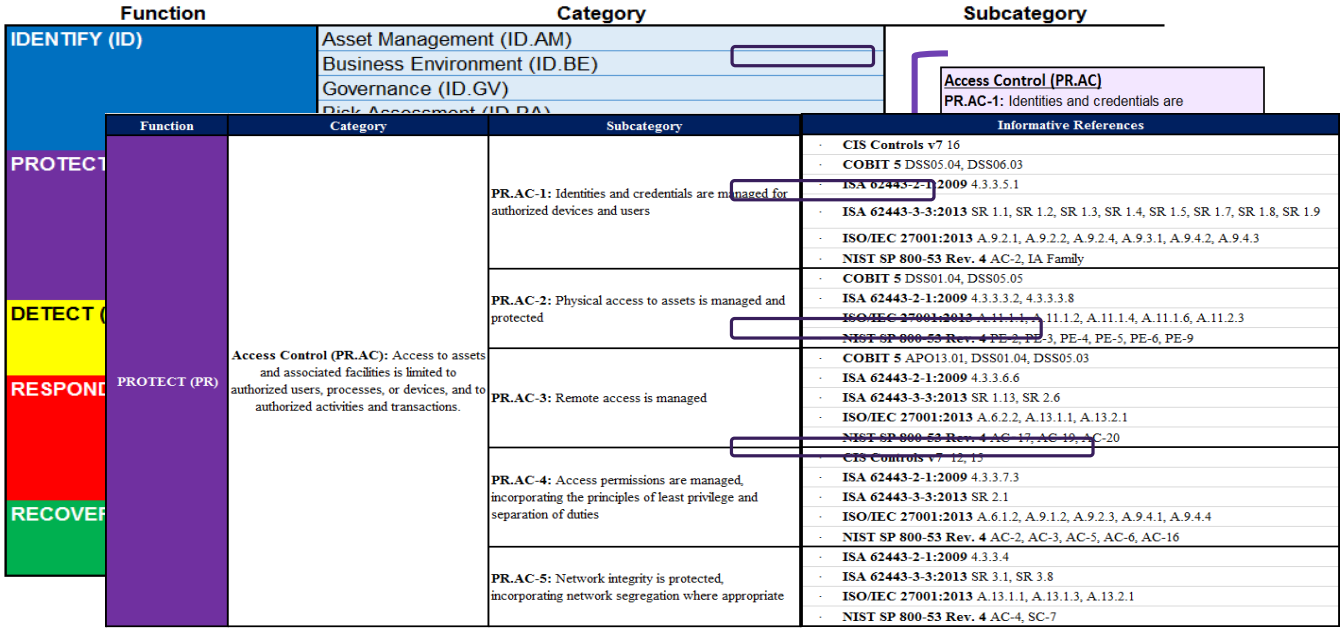
CSF Tiers



CSF Profiles



CSF Core

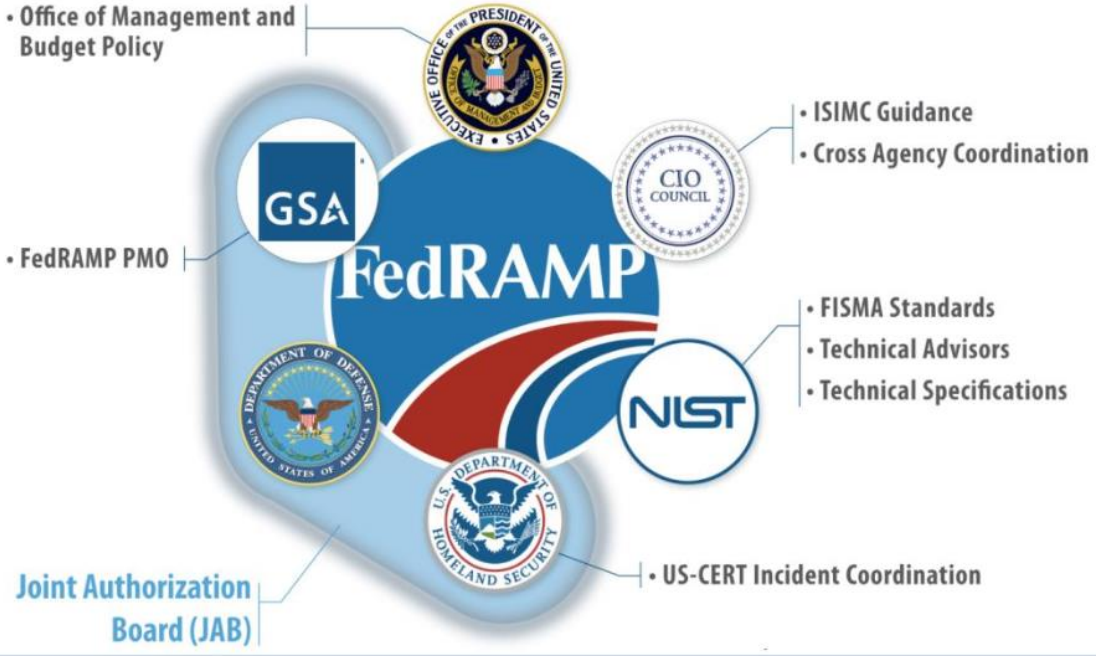


FedRAMP

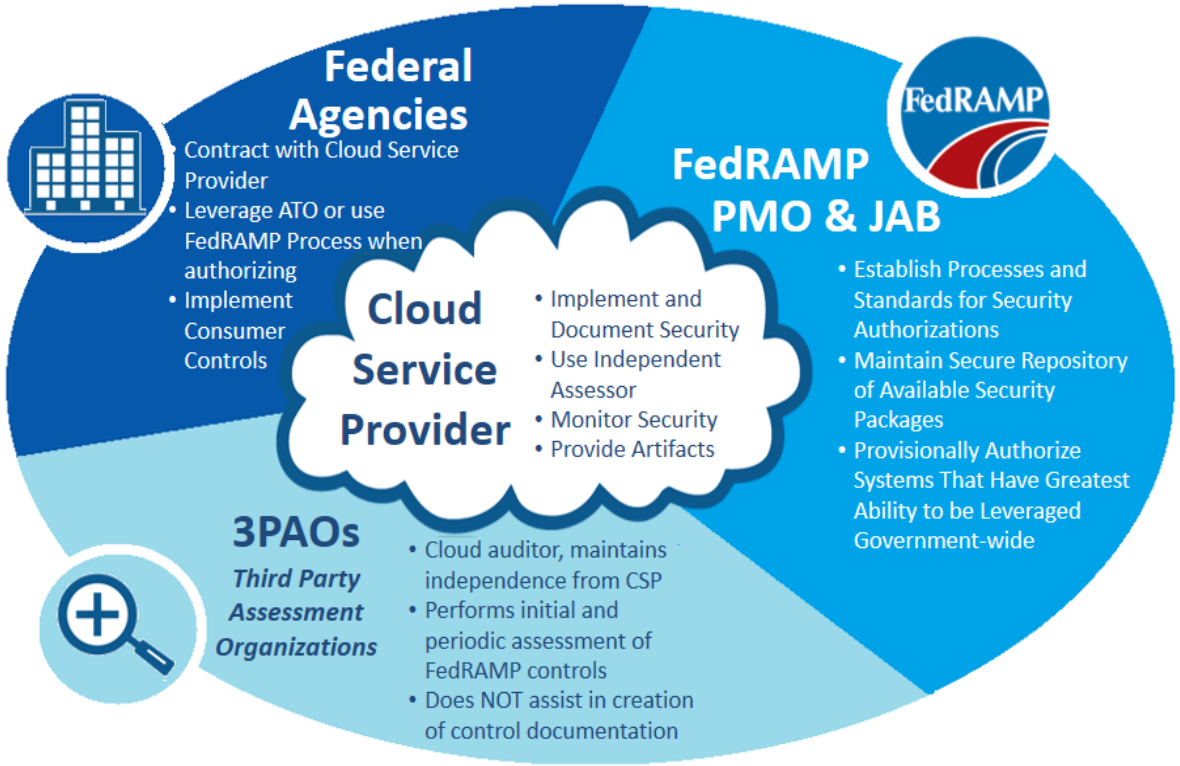
The Federal Risk and Authorization Management Program (FedRAMP)

- Developed in collaboration with NIST, GSA, DOD, NSA, OMB, CIO Council, DHS, and private industry
- Mandated by OMB Memo on December 8, 2011
- Requires assessment of a subset of NIST Special Publication 800-53 controls
- Standardizes security assessment, authorization, and continuous monitoring for cloud service providers (CSPs)
- Risk-based model that can be leveraged government-wide
- Provides processes, artifacts, and a secure repository that enables agencies to leverage authorization

FedRAMP



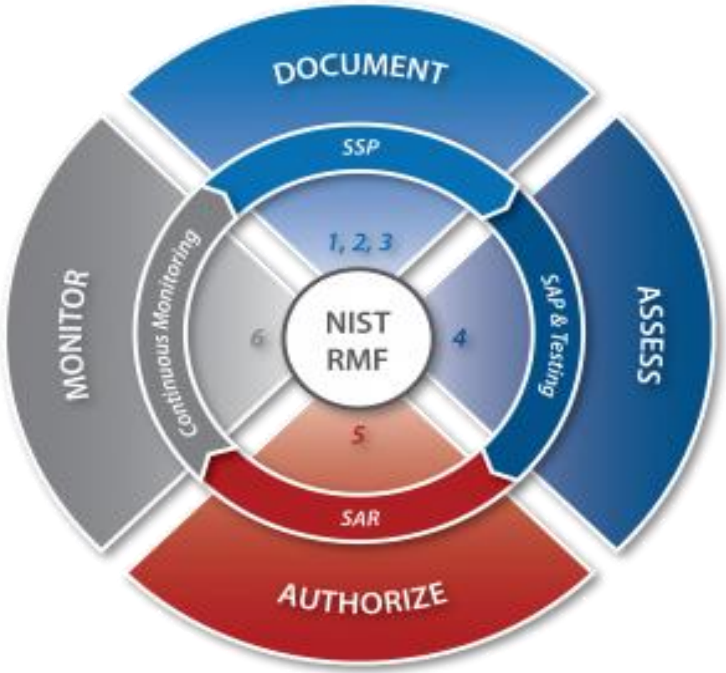
FedRAMP



Grant Thornton

FedRAMP

1. **Document**: CSPs categorize the type of data; Select and implement security control baseline
2. **Assess**: Independent Assessor (IA) evaluates security controls
3. **Authorize**: IA delivers Security Assessment Report (SAR); IA and CSP create Plane of Action and Milestones (POA&Ms)
4. **Monitor**: CSP enters the continuous monitoring phase



Grant Thornton

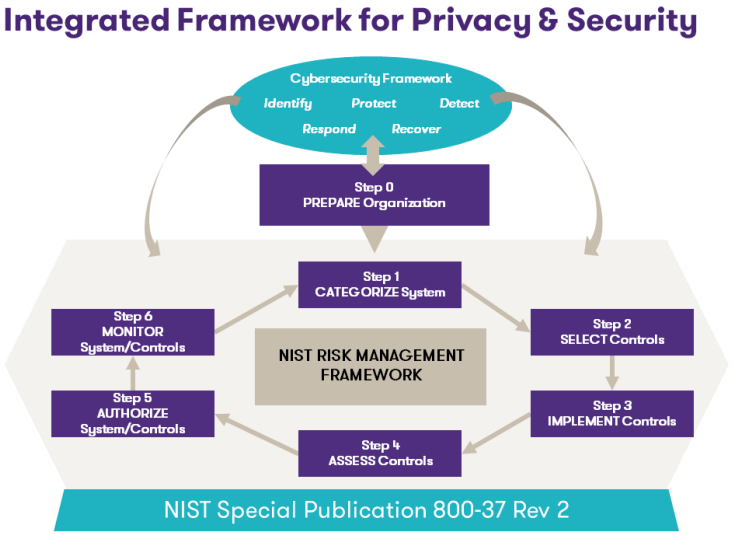
Tools and Techniques

- First Things First!
  - Implementation – Demo
  - Remediation – Demo
- Not My Problem!
  - Inheritance – Demo
- Reciprocity

The NIST Horizon

NIST SP 800-37 Rev 2: Risk Management Framework for Information systems and Organizations: A System Lifecycle Approach for Security and Privacy

- Identify missions, business functions, and processes that will be supported by the system
- Define organizational risk management strategy
- Identify stakeholders
- Conduct initial risk assessment and determine the value of organizational assets
- Define stakeholder protection needs and security requirements
- Determine system boundaries
- Identify how the system integrates into the enterprise and security architecture of the organization
- Identify and assign specific roles associated with RMF execution

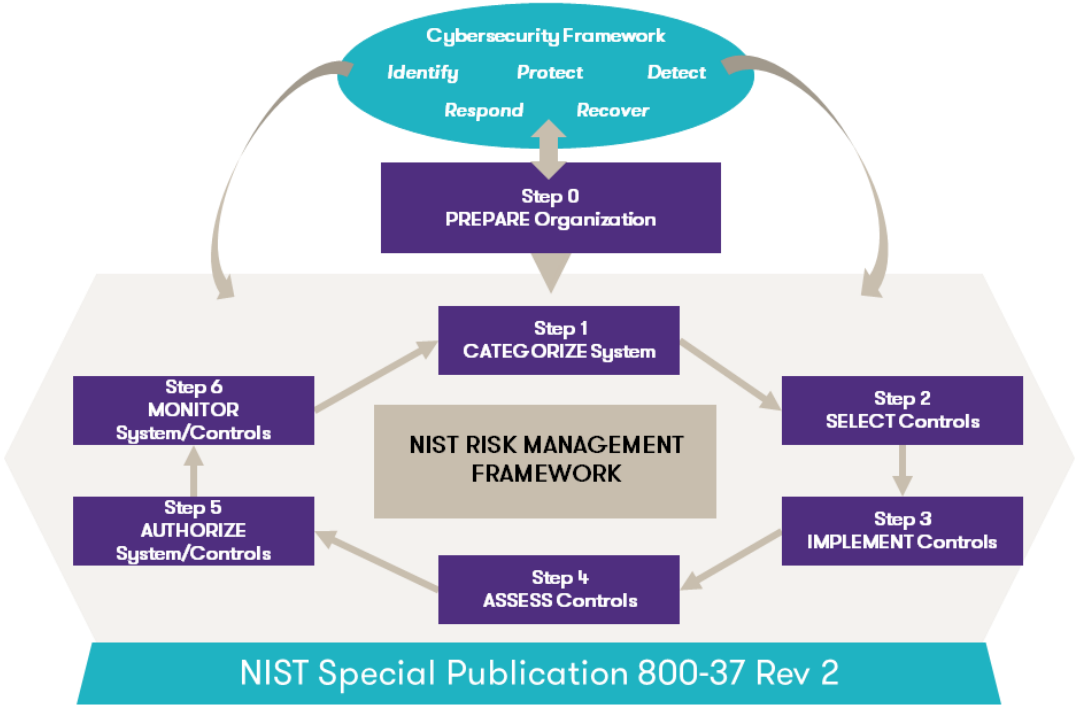


Holistic approach tightens linkage and alignment to business mission

Grant Thornton

The NIST Horizon

Integrated Framework for Privacy & Security



Grant Thornton

NIST SP 800-53 Rev. 5

- Security and Privacy Controls for Information Systems and Organizations
- Expanded focus on supply chain, cloud, mobile, cyber-physical, industrial/process control systems, and IoT devices
- Outcome-based controls structure
- Full integration of privacy controls into the security control catalog
- Integration with the Cybersecurity Framework
- New controls based on threat intelligence and empirical attack data

NIST SP 800 53 Rev 5 Outcome-based control focus

Revision 4 control structure	Revision 5 control structure
SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY Control: The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY Control: Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) Control: The information system implements multifactor authentication for network access to privileged accounts.	IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) Control: Implement multifactor authentication for network access to privileged accounts.

NIST SP 800 53 Rev 5 – Privacy control Integration

TABLE E-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	WITHDRAWN	PRIVACY-RELATED	IMPLEMENTED BY	ASSURANCE	CONTROL BASELINES		
						LOW	MOD	HIGH
AT-1	Awareness and Training Policy and Procedures		P	O	A	X	X	X
AT-2	Awareness Training		P	O	A	X	X	X
AT-2(1)	PRACTICAL EXERCISES		P	O	A			
AT-2(2)	INSIDER THREAT			O	A		X	X
AT-2(3)	SOCIAL ENGINEERING AND MINING			O	A		X	X
AT-3	Role-Based Training		P	O	A	X	X	X
AT-3(1)	ENVIRONMENTAL CONTROLS			O	A			
AT-3(2)	PHYSICAL SECURITY CONTROLS			O	A			
AT-3(3)	PRACTICAL EXERCISES		P	O	A			
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR			O	A			

Grant Thornton

NIST SP 800 53 Rev 5 – Privacy Control Integration

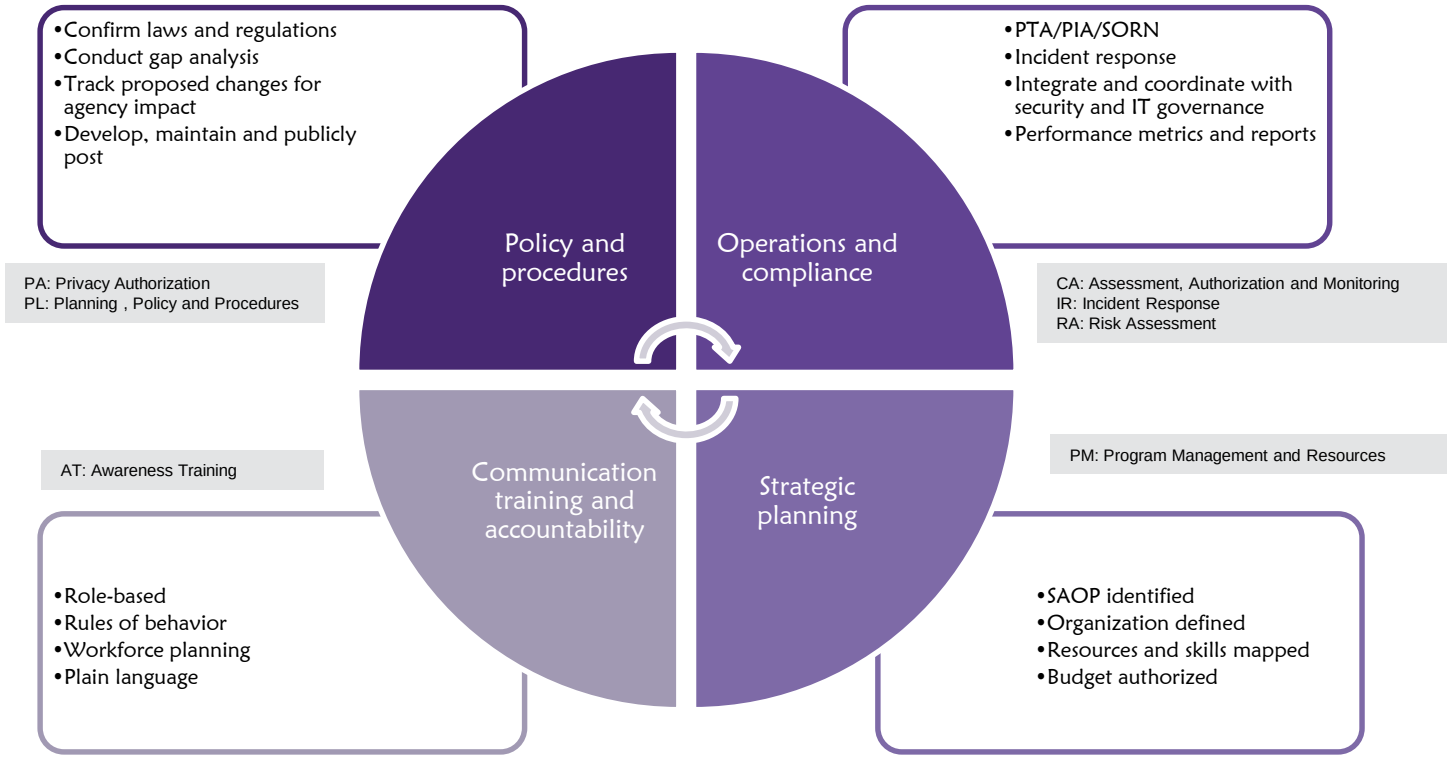
IP-1	Individual Participation Policies and Procedures	P	R
IP-2	Consent	P	S
IP-2(1)	Consent | ATTRIBUTE MANAGEMENT	P	D
IP-2(2)	Consent | JUST-IN-TIME NOTICE OF CONSENT	P	D
IP-3	Redress	P	S
IP-3(1)	Redress | NOTICE OF CORRECTION OR AMENDMENT	P	S
IP-3(2)	Redress | APPEAL	P	S
IP-4	Privacy Notice	P	S
IP-4(1)	Privacy Notice | JUST-IN-TIME NOTICE OF PRIVACY AUTHORIZATION	P	D

Ownership
Privacy Program (P) or Joint (J)

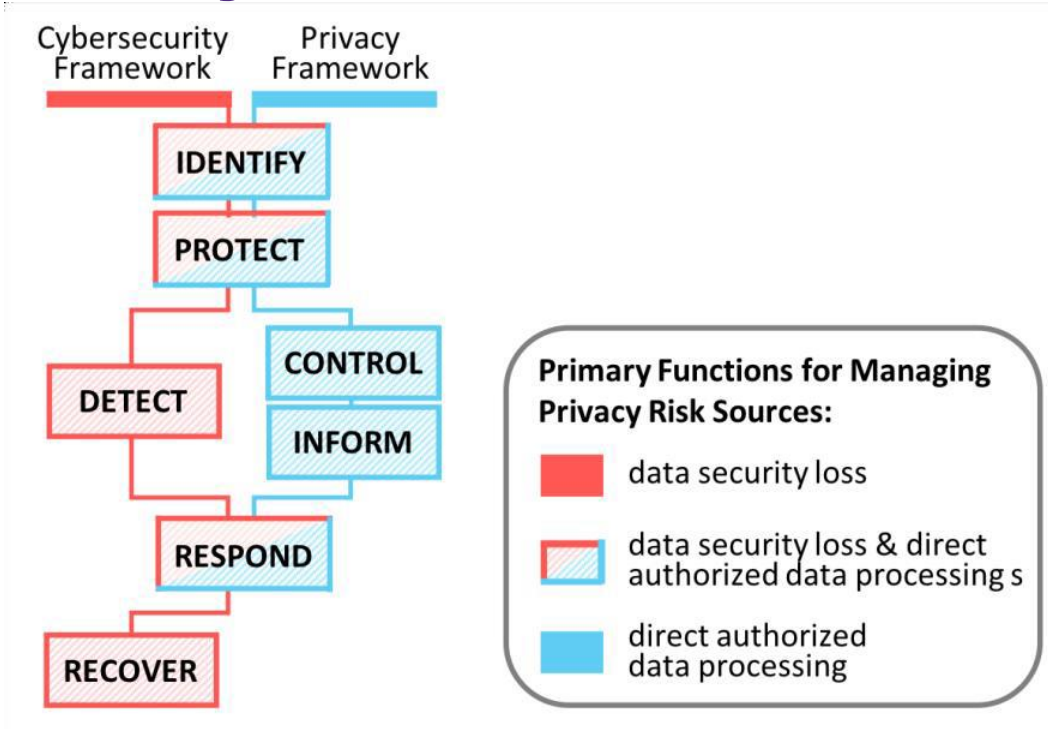
Selection Criteria
Required (R): based on legal, regulatory or policy regs
Situationally Required (S): laws and regs that only apply in specific circumstances
Discretionary (D): optional based on privacy risk

Grant Thornton

Privacy Authorization Covers Framework for Comprehensive Privacy Management



NIST Privacy Framework



What to do Now

- Address Privacy and Supply Chain Risks
  - Create or update policy, procedures, etc.
  - Conduct training on NIST guidelines
  - Collaborate to identify and select privacy controls
- Update System Security Plans and other related documentation
- Review and integrate RMF rev 2, Step 0 tasks
  - New systems: Initiation
  - Legacy systems: Operations/maintenance
- Continue to integrate the frameworks across the enterprise

Grant Thornton

Glenn Keaveny
Director
D: 703-562-5946
E Glenn.Keaveny@us.gt.com

References

- https://www.nist.gov/cyberframework
- https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
- https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- https://www.fedramp.gov/
- https://www.nist.gov/privacy-framework
- https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final
- https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Grant Thornton