AICPA

Cybersecurity & Privacy Enhancements

John Lainhart, Director, Grant Thornton

The National Institute of Standards and Technology (NIST) is in the process of updating their 3 major guidelines dealing with cybersecurity, risk and privacy – NIST Special Publication (SP) 800-53, NIST Risk Management Framework (RMF) and NIST Cybersecurity Framework (CSF).

These changes are needed to address the May 11, 2017 "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." With this Executive Order (EO), all federal agencies are required to take an enterprise approach to cybersecurity risk management, including assessment and mitigation. With respect to the federal government, the EO states that the President will hold heads of executive departments and agencies 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 whole, and to national security, the EO states that it is the policy of the United States to manage cybersecurity risk as an executive branch enterprise. The EO mandates that each agency head shall use the NIST CSF to manage the agency's cybersecurity risk.

Furthermore, a 2017 Defense Science Board report, Task Force on Cyber Defense, provided an alarming assessment of the current vulnerabilities in the U.S. critical infrastructure and the systems that support the mission essential operations and assets in the public and private sectors.

> *"…The Task Force notes that the cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries. It is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed…"*

Thus, there is an urgent need to update the NIST documents to provide guidance to further strengthen the underlying systems, component products, and services that we depend on in every sector of the critical infrastructure—ensuring those systems, components, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States.

These updates are of particular importance because they address significant changes incorporating risk management principles that are critical in determining the importance of the data to an agency and providing guidance to the agency in how to address high value data assets which require additional protections. This guidance is necessary to assist agencies in meeting the Presidential Executive Order and helps agencies in making decisions based on the mission impact of the data being protected, thereby allowing agencies to tailor their security requirements based on the risks to the agency in meeting their mission requirements. The NIST RMF is being updated to reflect this by requiring the identification of the agencies' missions, business functions, and mission/business processes that will be supported by the system; defining an organizational risk management strategy. The NIST CSF will be updated to incorporate these changes to NIST 800-53 (Revision 5) and the NIST RMF.

NIST SP 800-53 (Revision 5) was the first document updated (published in draft in August 2017 with changes currently being made to finalize it). This publication provides a catalog of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks. The NIST RMF (revision 2) was just updated and published as a draft on May 9, 2018 (with comments due by June 22, 2018). It requires the identification of the agencies' missions, business functions, and mission/business processes that will be supported by the system, and defines an organizational risk management strategy. The NIST CSF (version 1.1) was published on April 16, 2018 incorporating the changes being made to NIST 800-53 (Revision 5) and the NIST RMF (revision 2). In addition to the federal government, the NIST CSF is being implemented by state and local entities and commercial businesses in the U.S. and organizations on a global basis so these changes will be of significant impact globally.

NIST Special Publication (SP) 800-53

The Draft NIST SP 800-53 (Revision 5) contains major changes including:

- "Making the security and privacy controls more outcome-based by changing the structure of the controls;
- Fully integrating the privacy controls into the security control catalog creating a consolidated and unified set of controls for systems and organizations, while providing summary and mapping tables for privacy-related controls;
- Separating the control selection process from the actual controls, thus allowing the controls to be used by different communities of interest including systems engineers, software developers, enterprise architects; and mission/business owners;
- Promoting integration with different risk management and cybersecurity approaches and lexicons, including the Cybersecurity Framework;
- Clarifying the relationship between security and privacy to improve the selection of controls necessary to address the full scope of security and privacy risks; and
- Incorporating new, state-of-the-practice controls based on threat intelligence and empirical attack data, including controls to strengthen cybersecurity and privacy governance and accountability."

Security and privacy controls described in this publication have a well-defined organization and structure. For ease of use in the security and privacy control selection and specification process, controls are organized into twenty families. Each family contains security and privacy controls related to the specific topic of the family. A two-character identifier uniquely identifies each control family. Security and privacy controls may involve aspects of policy, oversight, supervision, manual processes, and automated mechanisms that are implemented by systems or actions by individuals. The table below lists the security and privacy control families and their associated family identifiers.

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

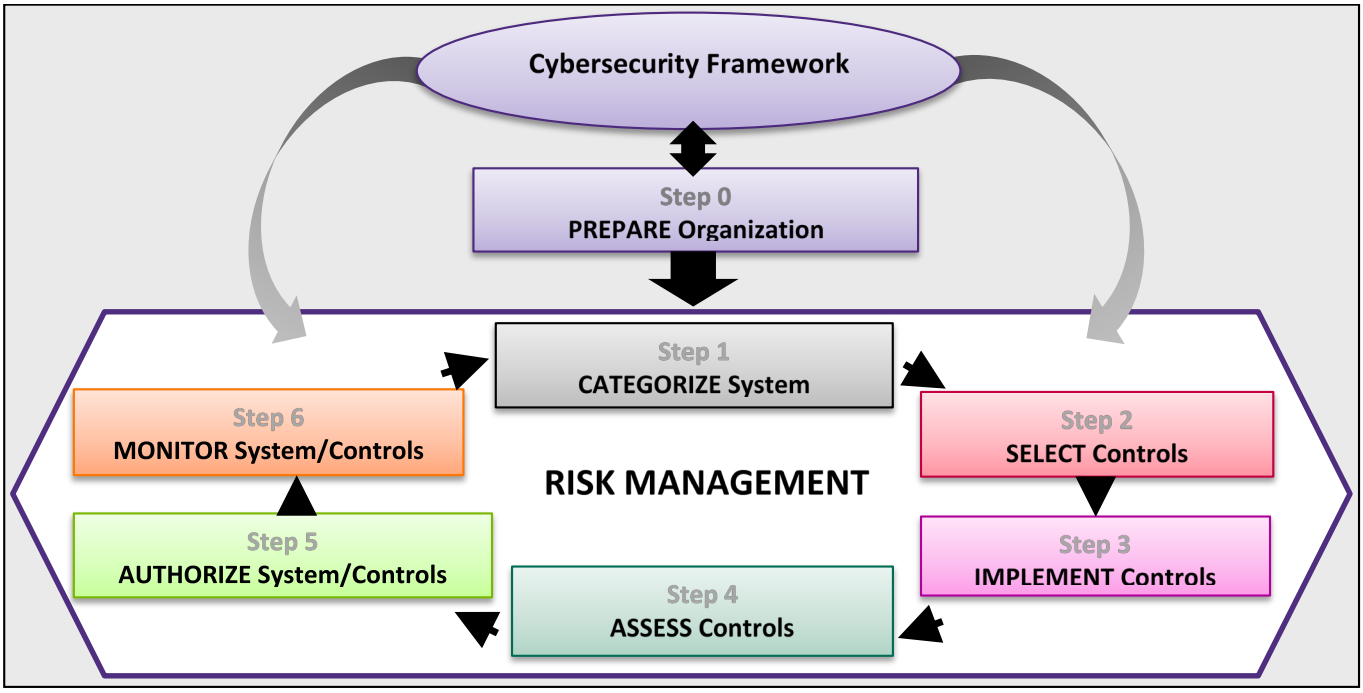
The security and privacy controls in the catalog are independent of the specific process employed to select those controls. Such selection processes can be part of an organization-wide risk management process, a life cycle-based systems engineering process, or a risk management or cybersecurity framework. The control selection criteria can be guided and informed by many factors including, for example, stakeholder protection needs and concerns, mission and business needs, standards and best practices, and requirements to comply with laws, Executive Orders, directives, policies, regulations, standards. The comprehensive nature of the controls coupled with a flexible, risk-based control selection process, can help organizations achieve adequate security for their systems and privacy protections for individuals. Finally, in separating the process of control selection from the security and privacy controls, a significant amount of tailoring guidance and other informative material previously contained in Special Publication 800-53 was eliminated from the publication. That content will be moved to other publications such as Special Publication 800-37 (Risk Management Framework) during the upcoming cycle for that document, which is also in process.

NIST Risk Management Framework (RMF)

The Draft NIST Risk Management Framework (Revision 2) has been updated to reflect changes in NIST SP 800-53, most significant of which is the addition of step 0, the Organizational Preparation Step.This is the step required to prepare the organization to execute the Risk Management Framework. It “includes identifying missions, business functions, and mission/business processes that will be supported by the system; defining an organizational risk management strategy; identifying the stakeholders having a security interest in the system; conducting an initial risk assessment and determining the value of organizational assets to be protected; defining stakeholder protection needs and security requirements; determining the system boundary to establish the scope of protection; showing how the system is integrated into the enterprise and information security architectures; allocating security requirements to the system and to the organization; and assigning individuals to key risk management roles.” Management will be able to use Step 0 to help them tailor security and privacy control baselines and develop overlays to support the specific

protection needs and requirements of stakeholders and their organizations to achieve trustworthy systems. Specifically, controls and control enhancements for low-impact, moderate-impact, and high-impact systems will be able to be identified to facilitate compliance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. These baselines represent an initial starting point in selecting controls for protecting federal systems. The baselines are hierarchical with respect to the controls allocated to those baselines. For example, for low-impact systems, the baseline controls may be sufficient; however, for high-impact systems, a number of control enhancements may be necessary to adequately protect those systems. Thus, step 0 is critical in preparing executives to make these critical decisions with respect to the specific protections needed to achieve trustworthy systems, as depicted in the diagram below.

NIST Cybersecurity Framework (CSF)

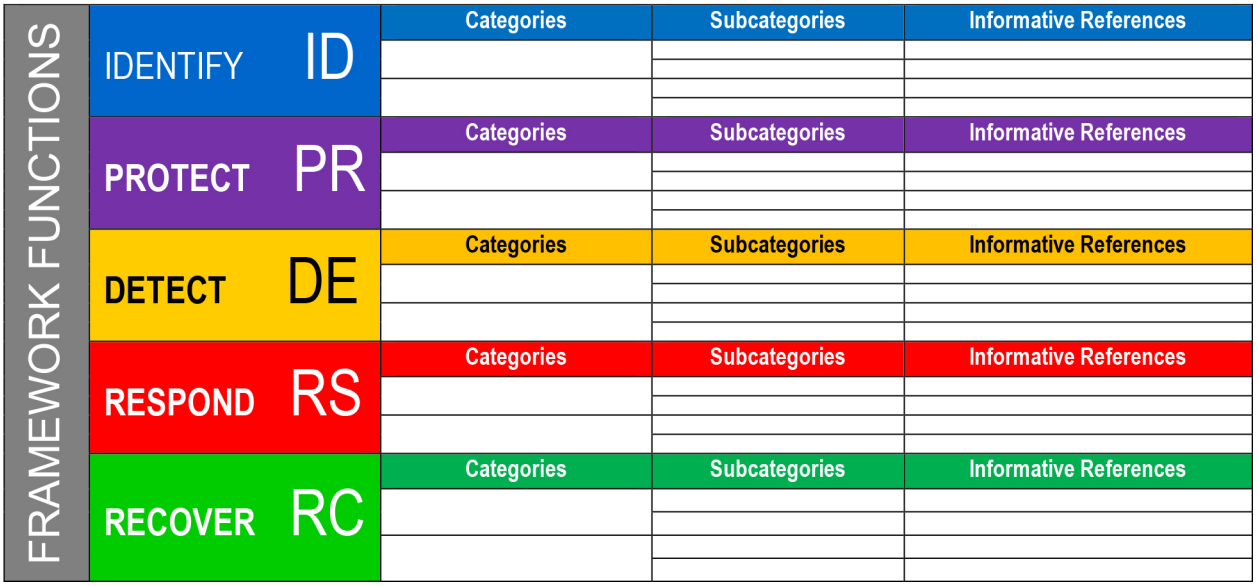


The NIST Cybersecurity Framework (version 1.1) includes this new Organization Preparation Step in the Risk Management Framework as well as several other changes, including:

- A new section on cybersecurity measurement
- Greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes
- Refinements to better account for authentication, authorization, and identity proofing
- Better explanation of the relationship between Implementation Tiers and Profile

The Framework Core provides a set of cybersecurity activities, desired outcomes, and appropriate references common across critical infrastructure sectors. It contains industry standards, guidelines and best practices identified by industry as helpful in managing cybersecurity risk.

The Core, as depicted in the figure below, comprises four elements: Functions, Categories, Subcategories, and Informative References.



Author Bio

John Lainhart
Director - Cybersecurity Executive at Grant Thornton LLP

John is a member of Grant Thornton Public Sector's Cyber Risk Advisory practice as a senior strategist and is responsible for developing cybersecurity offerings to broaden the Public Sector's overall advisory offerings. John also serves on the Board of Directors of George Washington University's Center for Cyber and Homeland Security, serves on the CyberUSA Advisory Board and serves as Advisor to the ISACA Board of Directors.

Prior to joining Grant Thornton, was the IBM Global Business Services (GBS) US Public Sector Cybersecurity & Privacy Service Area Leader. John also served on the Board of Directors of the Center for Cyber and Homeland Security at the George Washington University. He represented IBM on the National Governors Association State Cybersecurity Advisory Council and ended an appointment as co-chair of the National Association of Counties Cyber Security Task Force, where he was a member that task force. As IBM representative to the AICPA's Assurance Services Executive Committee, he was instrumental in the development of the AICPA's TrustServices and SSAE No. 16.

John remains very active in ISACA, having served as ISACA Board Chair, 1984-1985, and currently serving as the first Chair of the Future of Enterprise Governance of Information & Technology Advisory Council. He also served as Co-chair of the COBIT 5 Task Force and Principal Volunteer Advisor for IT Governance, COBIT, ValIT and RiskIT related initiatives. Mr. Lainhart is recognized as the "father" of the Certified Information Systems Auditor (CISA) program. He co-authored two books on information systems auditing -- System Development Auditor and Computerized Information Systems (CIS) Audit Manual and a NIST Special Publication on systems development life cycle auditing.

In addition to all this, Mr. Lainhart has a long, distinguished, and pioneering history of public service culminating in his service as the first Inspector General of the U.S. House of Representatives.

AICPA