We’re really happy with the NIST Cybersecurity Framework. Using NIST 800-171 assessments eases the grant proposal and submittal process—allowing us to focus on our passion for research.”

- Jonathan C. Silverstein, MD, MS, FACS, FACMI, Chief Research Informatics Officer, Department of Biomedical Informatics, University of Pittsburgh School of Medicine

**BENEFITS RECEIVED**

- As part of the University’s implementation of the NIST Cybersecurity Framework, an organization-wide security assessment resulted in a prioritized data security mitigation and remediation plan—which became a launch point for an ongoing dialogue on a more holistic approach to security issues in general.
- Consistent data management standards across a decentralized environment: Utilizing the Cybersecurity Framework, as well as NIST 800-171, provides all schools and departments—across the University—with the tools needed to meet shared security goals.
- Compliance with multiple standards: Adopting NIST 800-171 as the superseding standard—a decision made during a Framework implementation pilot—eliminates the need for further data management changes ahead of the Department of Education’s 2019 student financial aid audits; it also meets other standards required elsewhere in the University.

**SITUATION**

- The University receives hundreds of millions of dollars in government funding each year—from student financial aid, to a wide variety of competitive grants for faculty research in science and engineering—resulting in varying compliance requirements from multiple federal agencies.
- As a result, there are a variety of standards, incorporating a mixture of approaches, for information security used across the University; coordination has been difficult.
- Departments, faculty, and researchers store multiple classifications of sensitive data. They include controlled unclassified information (CUI), personally-identifiable information (PII), personal health information (PHI), student education records, intellectual property, and other data that have legal, regulatory, or contractual requirements for protection.
- This combination of regulatory requirements and good business practices increases the need for a standardized way to meet security requirements in an agile, decentralized IT environment.
- The University’s initial use of the Cybersecurity Framework provided the organization with better knowledge and perspective about its management of cybersecurity risks and identified multiple opportunities for better coordination of its cybersecurity approaches, investments, and priority needs.

**DRIVERS**

- The need to meet cybersecurity needs associated with managing federal grant recipients while alleviating complexity.
- The U.S. Department of Education’s yearly auditing to NIST 800-171 compliance for student financial aid was projected to start in 2019.
- A sense of duty to ensure the University holds all student, research, and healthcare records within reasonable protections, policies, and procedures.
Success Story: Cybersecurity Framework

• Because the University recognizes the value of, and aims to take advantage of the Cybersecurity Framework in some areas, as well as to meet NIST 800-171 compliance in others, adopting both as standard practice across the University will ensure that its information is more secure, while also demonstrating compliance.

PROCESS

Pitt Information Technology initiated a three-step hybrid approach, which builds an environment for those needing NIST 800-171 compliance and fits within the Cybersecurity Framework, as the basis for all risk assessment across the University.

Step 1: Two-Part Risk Assessment

All departments within the University complete an exploratory questionnaire to identify where each stores data and determine if they have sensitive data.

Departments indicating higher risk data in the initial survey, such as PCI, PII, HIPAA, etc., complete an advanced questionnaire which:

• identifies how each department protects its sensitive data through analysis of current security measures (technical, policy, procedural);
• allows gap analysis comparing existing security measures to NIST 800-171 requirements;
• determines residual risks;
• requires no further action from those without sensitive data.

Step 2: Mitigation Plan

• Identify existing mitigations currently in place, in relation to previously identified gaps.
• Prioritize gaps using standard risk management methodology to develop a mitigation and remediation plan—outlining a priority listing, timeline, costs, and resources.
• Begin work on and track mitigation actions.

Step 3: Periodic NIST 800-171 Assessments

RESULTS AND IMPACTS

• There is increased awareness and a broader view of security risks and compliance issues across the University, resulting in units proactively seeking security support from the Information Technology department on issues broader than federal grant management requirements.
• Many previously reluctant units are now looking to centralize security and other infrastructure items through the Information Technology department, allowing each unit’s internal IT staff to focus on unique business needs.

LESSONS LEARNED

• Departments that did not embrace the initial pilot Information Technology risk assessment process due to its complexity would welcome a process organized along the lines of the Cybersecurity Framework and NIST 800-171.
• Adopting specific guidelines like NIST 800-171 could actually make requirements for compliance easier to communicate and more widely accepted.

WHAT’S NEXT

• Standardize risk assessment as part of the procedure for all future data use requests.
• As more units source security responsibilities to central Information Technology, central IT will gain visibility for better monitoring, identifying, and responding to potential incidents—and units will be more likely to use servers hosted at the Network Operations Center or remote desktop management provided by Information Technology.
• The University will continue to rely on the Cybersecurity Framework as well as 800-171.

CONTACT INFORMATION & RESOURCES

• University of Pittsburgh Office of the CIO: technology.pitt.edu/about-us/office-of-the-cio
• University of Pittsburgh IT Security website: technology.pitt.edu/security
• Cybersecurity Framework website: www.nist.gov/cyberframework

University of Pittsburgh