



NIST Special Publication 800-171 for Higher Education

A guide to helping colleges and
universities address compliance

“The protection of Controlled Unclassified Information while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations.”

— NIST Special Publication 800-171



Higher education institutions are being asked to comply with new federal rules with heightened requirements to safeguard data known as Controlled Unclassified Information (CUI). By December 31, 2017, select grants and contracts with the federal government may be subject to additional requirements, and timely compliance will be essential to avoid potential fines or the loss of contracts that could impact the institution’s research and preeminence missions.

Institutions that process, store or transmit CUI data — such as student financial aid information or research conducted under federally funded contracts — may be impacted. This can include, but is not limited to:

- Agriculture Data
- Controlled Technical Information
- Engineering Data & Drawings
- Export Control Data
- Financial Information (Student Loans)
- Genetic Data
- Health Records
- Patent Information
- Privacy Data
- Research Data
- Student Records

Prioritizing compliance

The Defense Federal Acquisition Regulation Supplement (DFARS) 252.204.7012 establishes the National Institute of Standards and Technology’s Special Publication 800-171 (NIST SP 800-171) as the minimum security standards for protecting both CUI and Covered Defense Information (CDI) associated with defense related contracts. The Federal Acquisition Regulation (FAR) clause is also expected to apply NIST SP 800-171 standards to protect CUI associated with civilian contracts. Institutions will therefore face additional contractual requirements, likely associated with federal grants and research contracts as the National Institute of Standards and Technology’s Special Publication 800-171 (NIST SP 800-171) covers 14 groups of security control families.

If organizations fail to comply with these new regulations, they risk the loss of access to mission-critical data, and consequently government funding that contributes to research and day-to-day operations. Furthermore, there’s a risk of remaining non-compliant if institutions adopt the wrong technology or compliance activities. This could result in exposure to data breaches or regulatory audit findings causing brand and financial damage.

Indeed it remains unclear what the future regulatory environment will look like including general expectations, standards, and penalties. This may force higher education institutions to spend increasingly more resources and time on NIST compliance activities.

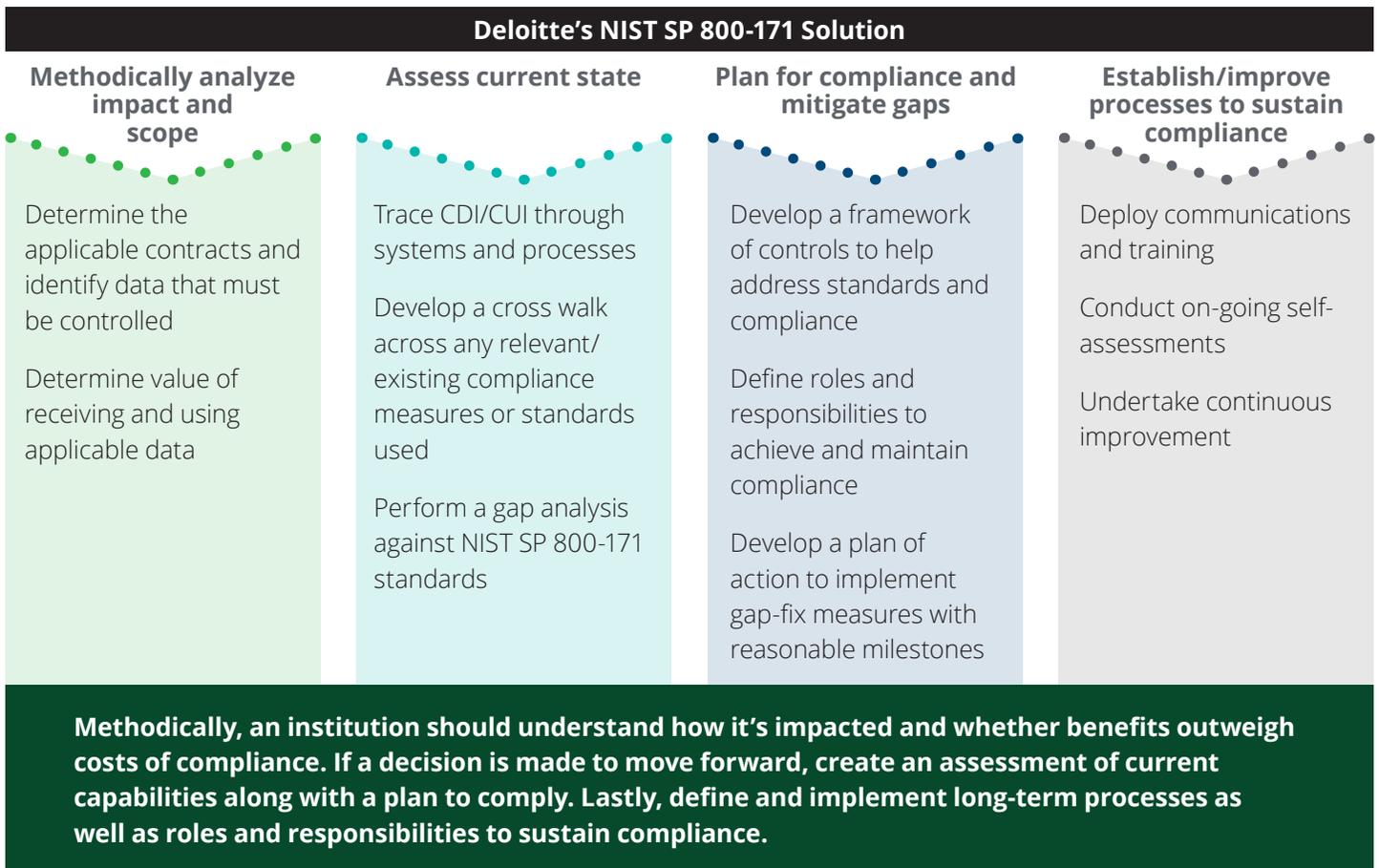
NIST SP 800-171 Security Control Families

NIST SP 800-171 groups 110 basic and derived control requirements across the following 14 families.

- Access control
- Audit and accountability
- Awareness and training
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Physical and environmental protection
- Program management
- Risk assessment
- System and communication protection
- System and information integrity

How can Deloitte help?

While each institution will be impacted differently by the new regulations, there are critical activities that should be undertaken to manage these compliance requirements. Deloitte, the leading provider of cyber governance, can help institutions both meet their December 31, 2017 compliance requirement, as well as maintain and monitor ongoing compliance by following a methodical approach.



The Deloitte difference

Deloitte is a market leader in designing and deploying cybersecurity, compliance and transformational solutions. We also bring a deep understanding of higher education, based on over 90 years of serving colleges and universities, and combine that with the extensive experience in our Federal practice obtained from implementing relevant cyber security standards.

As a result, we offer an unparalleled ability to effectively interpret NIST SP 800-171 requirements and design and deploy federally compliant systems and processes that address the specific needs of our higher education clients.

Our tools, accelerators, and methodologies can help your institution:

- engage appropriate stakeholders
- scope compliance efforts
- assess current security and controls
- develop plans for compliance
- mitigate gaps
- implement organization changes
- deploy effective communication and training
- implement sustainable and efficient processes for ongoing compliance

Deloitte.

This publication contains general information only and Deloitte Risk and Financial Advisory is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte Risk and Financial Advisory shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte Risk and Financial Advisory" means Deloitte & Touche LLP, which provides audit and risk advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2017 Deloitte Development LLC. All rights reserved

Looking ahead

The changing regulatory landscape will require institutions to remain vigilant as they build out their NIST programs. It's important for institutions to be strategic in the adoption of compliance activities by understanding their particular set of requirements and expectations. Deloitte can help higher education institutions understand this dynamic regulatory landscape, and promptly help them achieve compliance by implementing the required compliance activities that can become sustainable and integrated with day-to-day operations. More importantly, by being strategic with their decisions, institutions can reduce overall compliance costs by choosing the requisite programs from the start.

The breadth of our capabilities across contract compliance, risk management, IT consulting and organizational transformation allows us to define an approach that can efficiently and effectively align people, process, and technology. We can help higher education institutions meet their NIST SP 800-171 compliance obligations which will be required to maintain project funding and avoid other compliance issues that may result.

Contact us:

Betty Fleurimond
Managing Director,
Higher Education
Deloitte Services LP
+1 202 492 1453
bfleurimond@deloitte.com

Michael Wyatt
Principal
Deloitte and Touche LLP
+1 512 771 8062
miwyatt@deloitte.com

Richard Rudnicki
Specialist Leader
Deloitte & Touche LLP
+1 313 401 5263
rrudnicki@deloitte.com

Justin Williams
Senior Manager
Deloitte & Touche LLP
+1 346 224 5001
jmwilliams@deloitte.com