USE CASE

CRITICAL**START**® NIST 800-171 r2 Risk Assessment

KEY BENEFITS

- ✓ Evaluate protection gaps
- ✓ Demonstrate compliance
- ✓ Qualify for federal bids
- ✓ Increase data security
- ✓ Get insights for assessing compliance with other frameworks

Guidelines to protect Controlled Unclassified Information (CUI)

The National Institute of Standards and Technology (**NIST**) **SP 800-171 Revision 2** provides a list of 111 recommended security requirements to nonfederal organizations needing to maintain the confidentiality of Controlled Unclassified Information (**CUI**) in their information systems while working with the federal government.

Ideal use cases

The NIST SP 800-171 Rev. 2 helps assess compliance levels of security measures safeguarding the CUI. It is recommended for US federal contractors and partners needing to safeguard sensitive data in cloud apps and IT systems.

This is applicable for organizations that need to protect the confidentiality of CUI when:

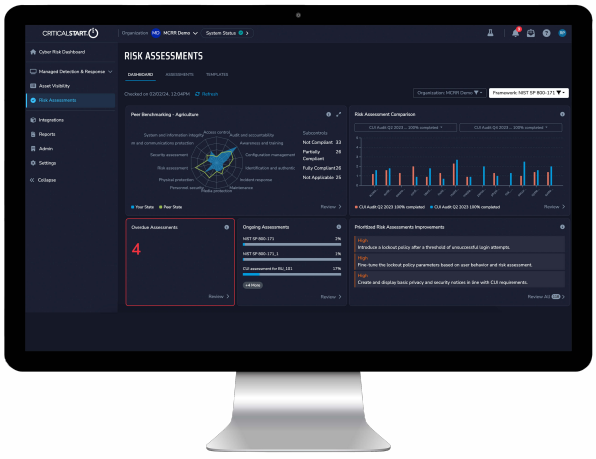
- The information is resident in nonfederal systems and organizations
- The nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency
- There are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI Registry

Completing the NIST SP 800-171 Rev. 2 provides insights for assessing compliance, allowing organizations to map controls and requirements between additional cybersecurity standards and frameworks to reveal overlapping or related areas. Correlating to other guidelines simplifies benchmarking against peers compliant with related standards, including the International Organization for Standardization and the Cybersecurity Maturity Model Certification (**ISO**, **CMMC**), etc. and streamlines compliance reporting by fulfilling multiple standards simultaneously.

How it works

No external certification is needed for NIST SP 800-171 Rev. 2 compliance. Critical Start's Cyber Risk Dashboard displays security maturity levels ranked against NIST SP 800-171 requirements. The Dashboard also contains risk-ranked recommendations so that organizations can identify, prioritize, and mitigate the gaps that would jeopardize CUI and limit federal opportunities.

Contractors interested in incrementally improving and maturing their cybersecurity defenses in line with expected policies and industry best practices receive customized recommendations for adding security controls to fix or improve their security protections.



© 2024 CRITICALSTART. All rights reserved.

CRITICALSTART®