NIST IT Risk Assessments

NIST Cybersecurity Framework

Make Cybersecurity risks a part of your overall risk management strategy through a 6-function model:

- Identify
- Protect
- Detect
- Respond
- Recover

NIST SP 800-171 IT Risk Assessment

Often called "Rule 171", this guidance controls Federal Unclassified Information and evaluates 12 areas of focus:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

The National Institute of Standards and Technology (NIST) is a non-regulatory agency that is part of the Department of Commerce whose mission is to promote innovation and industrial competitiveness. One area of focus for NIST is Cybersecurity and they have developed two key assessments that organizations use to determine their risk level.

NIST Cybersecurity Framework:
The NIST Cybersecurity Framework was developed in response to the changing cybersecurity threat landscape related to critical infrastructure. The NIST Cybersecurity Framework aims to have organizations consider cybersecurity risks as a part of the organization's overall risk management strategy.

NIST SP 800-171:
Today, more than at any time in history, the federal government is relying on external service providers to help carry out a wide range of federal missions and business activities related to unclassified information. As such, these contractors and subcontractors must demonstrate the ability to keep this unclassified information safe and secure through a specific IT Risk Assessment outlined in "Rule 171". This assessment evaluates all facets of an organization, including people, processes, and technology.

Compass IT Compliance
2 Asylum Road, North Providence, RI 02904
www.compassitc.com | 888-254-2482 | Info@compassitc.com