blackpoint

NIST 800-171 + Blackpoint Control Checklist

Work towards NIST 800-171 compliance with Blackpoint's Active Cybersecurity

What is NIST Special Publication 800-171?

Titled, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," it is a set of guidelines developed by the National Institute of Standards and Technology (NIST) to safeguard Controlled Unclassified Information (CUI) in non-federal information systems and organizations.

What's this guide for?

This publication is part of the U.S. government's effort to protect sensitive federal information when processed, stored, and used by non-federal entities, including contractors, state and local governments, and universities.

With this checklist, you can see how Blackpoint helps your organization meet various NIST 800-171 compliance requirements.

Topline Takeaways

Blackpoint Cyber helps meet requirements within the following NIST 800-171 families:

- **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** ✓

Control Checklist

Blackpoint helps meet the following controls:

FAMILY	REQUIREMENT
Access Control	**3.1.1** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.
	3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
	3.1.8 Limit unsuccessful logon attempts.
	3.1.11 Terminate (automatically) a user session after a defined condition.
	3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.
	3.1.20 Verify and control/limit connections to and use of external systems.
Audit and Accountability	**3.3.1** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
	3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.
	3.3.3 Review and update logged events.
	3.3.4 Alert in the event of an audit logging process failure.
	3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
	3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.
	3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
Configuration Management	**3.4.2** Establish and enforce security configuration settings for information technology products employed in organizational systems.
	3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
	3.4.9 Control and monitor user-installed software.

Control Checklist *(continued)*

blackpoint

FAMILY	REQUIREMENT
Identification and Authentication	3.5.1 Identify system users, processes acting on behalf of users, and devices.
	3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
Incident Response	3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
	3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
	3.6.3 Test the organizational incident response capability.
Personnel Security	3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers
Risk Assessment	3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
Security Assessment	3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
	3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
System and Communications Protection	3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
	3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.
System and Information Integrity	3.14.1 Identify, report, and correct system flaws in a timely manner.
	3.14.2 Provide protection from malicious code at designated locations within organizational systems.
	3.14.3 Monitor system security alerts and advisories and take action in response.
	3.14.4 Update malicious code protection mechanisms when new releases are available.
	3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
	3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
	3.14.7 Identify unauthorized use of organizational systems.

To learn more about NIST 800-171, visit the Center for Internet Security's website.