safous

NIST CYBERSECURITY CHECKLIST

Meet NIST SP 800-171 Rev.3 Compliance Requirements With Safous

NIST SP 800-171 Rev.3 outlines the security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems. While originally designed for U.S. Department of Defense contractors, these controls are becoming increasingly relevant to global supply chain security and Zero Trust initiatives.

Safous helps organizations meet NIST 800-171 Rev.3 requirements by providing secure, governed remote access to operational and IT environments – without exposing sensitive networks or credentials.

Safous and NIST SP 800-171 Rev.3 Compliance

NIST Requirement	How Safous Helps	ODP/Evidence
03.01.01 – Account Management	Supports account lifecycle enforcement via IdP-integrated, role-based access policies and time-bound approvals for privileged sessions.	ODP: account inactivity window, deprovision SLA Evidence: IdP integration screenshots, deprovision test record, access policy export
03.01.02 – Access Enforcement	Enforces approved authorizations via policy (RBAC/ABAC) and just-in-time approvals at the Safous gateway.	ODP: policy decision points, exception workflow Evidence: policy definitions, change-control tickets
03.01.04 – Separation of Duties	Implements role separation between requestors, approvers, and auditors while keeping admin privileges distinct from approvers.	ODP: roles requiring separation Evidence: role matrix, admin & auditor account listings
03.01.05 – Least Privilege	Grants time-bound, task-scoped privileges; scheduled reviews remove excess rights.	ODP: privilege review frequency, high-risk functions list Evidence: JIT policy, quarterly privilege review records
03.01.11 – Session Termination	Auto-terminates sessions on organization-defined triggers (idle time, clock time, workflow end).	ODP: idle timeout minutes, after-hours cutoff Evidence: gateway config + test log
03.01.12 – Remote Access	Routes remote access through a managed access control point with approval workflows and recording for privileged sessions.	ODP: permitted remote methods, pre-approval criteria Evidence: architecture diagram, AppGateway ruleset
03.03.01 – Event Logging	Selects and reviews organization-defined event types; configures Safous to log privileged session events accordingly.	ODP: event categories and review cadence Evidence: event catalog, log settings
03.03.02 – Audit Record Content	Ensures session recording and command logs capture event type, time, source, outcome, and associated identities.	ODP: additional fields Evidence: sample log with required fields

NIST Requirement	How Safous Helps	ODP/Evidence
03.03.03 – Audit Record Generation	Generates audit records for the selected event types and required content, and retains records per policy.	ODP: retention period Evidence: retention policy, log storage proof
03.03.08 – Protection of Audit Information	Stores audit data in tamper- resistant repositories and restricts access to authorized roles.	ODP: authorized roles, integrity controls Evidence: storage controls, access lists
03.05.03 – Multi-Factor Authentication	Requires MFA for access to privileged and non-privileged accounts, enforced at the gateway.	ODP: allowed factors, exception handling Evidence: MFA policy, gateway sign-in logs
03.05.05 – Identifier Management	Integrates with enterprise IdPs so each session maps to a verified identity; prohibits identifier reuse for a defined period.	ODP: reuse prohibition period, identity proofing steps Evidence: IdP config, policy excerpt
03.05.12 – Authenticator Management	Uses credential vaulting/SSO to minimize secret exposure; defines processes for issuance, revocation, and lost or stolen authenticators.	ODP: reset verification steps, revocation SLA Evidence: runbook, ticket samples
03.13.08 – Transmission & Storage Confidentiality	Encrypts communications to protect CUI in transit and at rest. FIPS-validated crypto is recommended for protecting CUI, & may be required per contract.	ODP: approved cryptographic types and versions Evidence: cipher suites list; module validation or vendor statement
03.13.10 – Cryptographic Key Establishment & Management	Document key generation, distribution, storage, rotation, and destruction for TLS and vaults used by Safous integrations; align with org key management policy.	ODP: key rotation interval Evidence: KMS/HSM config, key lifecycle records

How Safous Helps Businesses Meet NIST SP 800-171 Requirements

Safous offers:

- ✓ **Identity-based access** with MFA and least-privilege, JIT session controls
- ✓ **Full session recording** and logs for compliance audits and forensics
- ✓ **Credential vaulting** to eliminate shared passwords and standing privileges
- ✓ **Secure remote connections** without VPN clients or host-based agents
- ✓ **Centralized access governance** across IT, OT, and cloud systems
- ✓ **Flexible licensing,** named or concurrent, to meet your specific needs

Meet NIST SP 800-171 Rev.3 Requirements With Safous

Safous provides secure remote access for every environment under a fully-integrated Zero Trust platform, so you can strengthen your compliance with NIST 800-171 Rev.3 controls – without adding complexity to your infrastructure.

Contact us today to see how Safous can help your organization meet NIST compliance with unified access governance for IT, OT, and hybrid systems.

EXPLORE SAFOUS →

safous