safous

NIST CSF 2.0 COMPLIANCE CHECKLIST

Support NIST Cybersecurity Framework (CSF) 2.0 Outcomes With Safous

The NIST Cybersecurity Framework (CSF) 2.0 is a framework for protecting organizational assets across IT, OT, manufacturing, and supply chain environments. Unlike prescriptive standards, CSF 2.0 provides outcomes that organizations can tailor to their mission and risk tolerance, serving as a common language for cybersecurity risk management and stakeholder communication.

Manufacturing and OT environments rely on remote access from system integrators, vendors, and field engineers. Unfortunately, traditional VPN-based access increases credential exposure and lateral movement risk, creating security gaps that threaten critical infrastructure.

Safous Privileged Remote Access helps organizations address these challenges by supporting alignment with NIST CSF 2.0. It enables security teams to enforce least-privilege access through approval workflows, log privileged actions for compliance, and isolate application-level access from network exposure – reducing attack surface and remote access threats without adding complexity.

Safous Privileged Remote Access provides technical and governance controls that support customer alignment with NIST CSF 2.0. Businesses remain responsible for implementing and maintaining their cybersecurity risk management programs in accordance with NIST CSF 2.0 and their organizational context.

Safous and NIST CSF 2.0 Compliance

NIST Category	CSF 2.0 Reference	How Safous Helps	ODP/Evidence
Govern (GV)	**GV.OC – Organizational Context**	Ensures remote access policies reflect organizational structure and dependencies via IdP integration and centralized access logging.	**ODP:** critical systems list, stakeholder dependencies, contractual access requirements **Evidence:** IdP integration configuration, access policy matrix, session audit logs with user identity and system accessed
	GV.RM – Risk Management Strategy	Enables risk-informed access decisions via centralized approval workflows and policy enforcement.	**ODP:** risk tolerance levels, high-risk access functions, approval authority delegation **Evidence:** approval workflow policy, monthly access metrics reports, risk dashboard integration
	GV.RR – Roles, Responsibilities, and Authorities	Enforces role-based separation of duties through distinct admin, approver, and auditor roles; attributes actions to a named role for demonstrable accountability throughout the access lifecycle.	**ODP:** roles requiring separation, delegation of authority **Evidence:** role matrix, admin account listing with role assignments, access policy export, audit-ready logs showing role-based approvals

NIST Category	CSF 2.0 Reference	How Safous Helps	ODP/Evidence
Govern (GV)	**GV.SC – Cybersecurity Supply Chain Risk Management**	Provides centralized third-party and vendor access governance with time-limited, task-scoped policies and full session recording; enables rapid session termination and credential revocation.	**ODP:** vendor access policies, time limits per vendor role, approval requirements, termination procedures **Evidence:** vendor and third-party access policy documentation, approval workflow records, session logs with filtering
Protect (PR)	**PR.AA – Identity Management, Authentication, and Access Control**	Integrates with identity providers (SAML, OIDC, LDAP) to manage user identities; enforces MFA at the gateway.	**ODP:** authoritative identity source, vaulting scope, injection methods, MFA factors (TOTP, email, SMS, hardware tokens) **Evidence:** IdP integration, credential vault settings, MFA policy configuration
	PR.AT – Awareness and Training	Supports role-specific training and awareness efforts by providing session playback and audit logs for incident reviews, lessons-learned exercises, and compliance training programs.	**ODP:** role-specific training topics, training frequency, incident review cadence **Evidence:** training curriculum referencing session playback examples, incident review records with lessons learned
	PR.DS – Data Security	Encrypts communication between clients and gateway (TLS); enforces session controls to prevent unauthorized data exfiltration; command logging captures data access and modification activity.	**ODP:** encryption standards, session control policies, data sensitivity classifications **Evidence:** cipher suite and TLS configuration, session control settings, encryption key management records, data handling logs
	PR.PS – Platform Security	Generates session and command-level log records; exports logs in SIEM-compatible formats (syslog, JSON, CEF); session recording provides visibility into unauthorized changes and supports deterrence and forensic investigation.	**ODP:** log event types, retention period, SIEM tools, export frequency **Evidence:** log generation policy, SIEM integration, session recordings, log retention policy, archival procedures
	PR.IR – Technology Infrastructure Resilience	Isolates application-level access from network exposure; supports agentless connectivity to reduce infrastructure footprint and patching requirements.	**ODP:** supported applications, network segmentation scope, agent-less connectivity **Evidence:** access policy rules, network segmentation documentation, session flow logs
Detect (DE)	**DE.CM – Continuous Monitoring**	Provides real-time visibility into privileged access via session logging, live session monitoring, configurable alerts for anomalous activity, and SIEM integration for cross-system correlation.	**ODP:** monitoring scope, alert thresholds (failed auth, policy violations), SIEM tools, review cadence **Evidence:** live session monitoring, SIEM integration and alert rules, session logs showing anomaly detection
	DE.AE – Adverse Event Analysis	Supports incident investigation through session logs and playback; correlates Safous activity with security events from other tools; time-stamped logs enable precise forensic reconstruction.	**ODP:** investigation procedures, correlation data sources, incident declaration criteria **Evidence:** session playback, log correlation queries, incident declaration records

NIST Category	CSF 2.0 Reference	How Safous Helps	ODP/Evidence
Respond (RS)	**RS.MA – Incident Management**	Enables rapid response through immediate session termination and credential revocation; approval records support coordination and remediation tracking.	**ODP:** incident response triggers, termination procedures, credential revocation SLA **Evidence:** session termination and termination logs, approval records reviewed during response
	RS.AN – Incident Analysis	Enables timeline reconstruction with session recordings and command-level logs; supports tamper-resistant audit trails and log integrity controls to maintain evidentiary value during forensic investigations.	**ODP:** log retention period, integrity controls, forensic review procedures **Evidence:** session recording and log retention policy, session playback examples, log exports with digital signatures, forensic analysis reports
	RS.MI – Incident Mitigation	Prevents lateral movement through app-level isolation; blocks attacker credential reuse via credential vaulting; audit logs identify all affected systems during incident window.	**ODP:** lateral movement detection rules, credential revocation, system impact assessment **Evidence:** session isolation logs, containment actions and post-incident analysis report
Recover (RC)	**RC.RP – Incident Recovery Plan Execution**	Enables controlled re-approval of access after recovery; time-bound access policies automatically revoke access after recovery window closes; maintains audit trail of all recovery-phase access.	**ODP:** re-approval authority, time-bound access, recovery window definition **Evidence:** re-approval workflow, time-bound access policies, recovery completion logs
	RC.CO – Incident Recovery Communication	Provides evidence of recovery-phase access via audit logs and session records; supports post-incident review through audit findings; informs improved access governance policies.	**ODP:** stakeholder communication procedures, lessons learned review frequency, policy update triggers **Evidence:** logs showing Safous activity during recovery, records documenting recovery actions, lessons learned meeting notes, revised access policies

How Safous Helps Businesses Meet NIST CSF 2.0 Requirements

Safous offers:

- **Identity-based access** with MFA and least-privilege, just-in-time session controls
- **Full session recording** and command-level logs for compliance audits and forensics
- **Credential vaulting t**o eliminate shared passwords and standing privileges
- **Agentless remote connections** without VPN clients or host-based agents
- **Centralized access governance** and approval workflows across IT, OT, and cloud systems
- **Third-party and vendor access management** with time-limited, task-scoped policies
- **SIEM-ready log export** (syslog, JSON, CEF) for continuous monitoring and threat hunting
- **Flexible deployment and licensing** to meet your organizational and operational needs

Simplify NIST CSF 2.0 Compliance With Safous

Safous Privileged Remote Access provides a unified access control platform for IT, OT, and hybrid environments, helping your organization establish and demonstrate alignment with NIST CSF 2.0 controls – without adding infrastructure complexity or network exposure.

Talk to our team today to see how Safous can help your organization support NIST CSF 2.0 outcomes with unified privileged access governance.

EXPLORE SAFOUS