safous

CIS CONTROLS V8.1 COMPLIANCE CHECKLIST

Operationalize CIS Controls v8.1 With Safous Privileged Remote Access

CIS Controls v8.1 represents the most widely adopted, prescriptive cybersecurity framework for defending against real-world attacks. It translates attack data into actionable outcomes to give organizations a clear path from planning to implementation. However, putting those outcomes into practice requires the right tools and processes.

Safous Privileged Remote Access supports the operationalization of this framework by providing the governance, identity, and accountability capabilities that several controls demand. Organizations using Safous can enforce least-privilege access, maintain complete audit trails, and demonstrate alignment with CIS Controls v8.1 to auditors and stakeholders – all without adding complexity to existing infrastructure.

Safous Privileged Remote Access provides technical and governance controls that support customer alignment with CIS Controls v8.1. Businesses remain responsible for implementing and maintaining their cybersecurity risk management programs in accordance with CIS Controls v8.1 and their organizational context.

Safous and CIS Controls v8.1 Alignment

CIS Control	Intent	How Safous Helps	Outcome
Control 5 – Account Management	**Safeguard 5.1 –** Establish and maintain an inventory of all accounts managed in the enterprise.	Integrates with identity providers (SAML, OIDC, LDAP) to centrally manage accounts; maintains audit logs showing all account access and activity.	Complete, verified account inventory tracked to a person or function.
	Safeguard 5.2 – Use unique passwords for all enterprise assets.	Supports credential rotation; eliminates shared credentials.	Users and service accounts have unique, regularly rotated credentials
	Safeguard 5.4 – Restrict administrator privileges to dedicated admin accounts on enterprise assets.	Enforces separation between user and administrator accounts; logs all administrative sessions separately.	Administrative accounts are segregated and tracked independently.
	Safeguard 5.5 – Establish and maintain an inventory of service accounts.	Automates provisioning and de-provisioning through approval workflows; integrates with HR and identity systems.	Account management is repeatable, auditable, and reduces manual error.
	Safeguard 5.6 – Centralize account management through a directory or identity service.	Vaults service credentials; injects at session time; supports rotation; prevents hardcoded or embedded credentials.	Service account credentials are never exposed and are managed centrally through the access gateway.

CIS Control	Intent	How Safous Helps	Outcome
Control 6 – Access Control Management	**Safeguard 6.1 & 6.2 –** Establish and follow a process for granting and revoking access to enterprise assets upon role change.	Implements approval workflows and tracks approver and approval date; enables immediate session termination; maintains audit logs of revocation; alerts on revocation triggers.	Access grants and revocation are auditable and traceable with clear decision records; former employees and transferred users cannot access systems.
	Safeguard 6.3 – Require all externally-exposed enterprise or third-party applications to enforce MFA.	Enforces MFA at the gateway; supports TOTP, email, SMS, hardware tokens; logs MFA success/failure.	Remote access is protected by MFA, and MFA enforcement is consistently applied at the access gateway.
	Safeguard 6.4 & 6.5 – Require MFA for remote network access and all administrative access accounts.	Mandates MFA at the gateway for all privileged sessions; enforced before any administrative action.	Remote privileged access and administrative access require MFA and are enforced prior to session establishment.
	Safeguard 6.6 – Establish and maintain an inventory of the enterprise's authentication and authorization systems.	Generates access privilege reports; tracks access by user, role, and system; supports review workflows.	Unused privileges are identified and removed through regular access reviews.
	Safeguard 6.7 – Centralize access control for all enterprise assets.	Provides a centralized policy engine for all access decisions; enforces consistent policies across IT, OT, and cloud.	All access decisions flow through a single, auditable system regardless of asset type or location.
	Safeguard 6.8 – Define and maintain role-based access control.	Centralizes role-based and attribute-based access policies; maps users to roles; supports the principle of least privilege.	Access is standardized and repeatable, and users with the same role have consistent, minimal access levels aligned with job function.
Control 8 – Audit Log Management	**Safeguard 8.1 –** Establish and maintain a documented audit log management process that defines the enterprise's logging requirements.	Provides a framework for logging design; integrates with multiple log sources; documents collection, review, and retention.	Clear, documented approach to audit logging aligned with CIS Controls v8.1 and regulatory requirements.
	Safeguard 8.2 & 8.5– Collect audit logs for enterprise assets.	Captures detailed logs on every session and action with verified user identity; export logs in SIEM-compatible formats (syslog, JSON, CEF)	Compliance audits and incident investigations have sufficient and verifiable evidence of all privileged access.
	Safeguard 8.9– Centralize audit log collection and retention across enterprise assets.	Generates structured, centralized logs; aggregates IT, OT, and hybrid logs.	All access logs are consolidated into a single platform, enabling comprehensive visibility and correlation.

CIS Control	Intent	How Safous Helps	Outcome
Control 8 – Audit Log Management	**Safeguard 8.10–** Retain audit logs across enterprise assets for a minimum of 90 days.	Supports configurable retention policies; maintains immutable archives; automates archival and purge.	Logs are retained to support incident investigation and compliance reviews.
	Safeguard 8.11 – Conduct regularly scheduled reviews of audit logs.	Provides session playback for investigation; supports log searching by user, system, time, or activity.	Investigators can easily review logs, reconstruct incidents, and identify unauthorized activities.

How Safous Helps Operationalize CIS Controls v8.1 in OT/ICS Environments

CIS Controls v8.1 apply universally, but OT/ICS environments present unique challenges. Supply chain dependencies mean vendors and system integrators require remote access to critical systems. Legacy equipment lacks native identity management and logging, and operational constraints like uptime requirements and minimal downtime windows limit infrastructure changes.

Safous provides identity and access governance without disrupting operations or requiring changes to legacy systems by:

Centralizing and time-limiting vendor and third-party access through approval workflows.

Logging remote maintenance at the application layer (SSH, VNC, HTTP) to create complete audit trails.

Agentless connectivity avoids introducing additional access infrastructure in constrained OT environments.

Ensuring vendor and third-party access is time-limited, individually attributable, and fully logged.

Improving access visibility and control across all enterprise assets in IT, OT, and cloud systems.

Simplifying reporting for audits and forensics with full session recording and command-level logs.

Safous Privileged Remote Access serves as a practical enabler for CIS Controls v8.1 adoption. **Contact us today** to get started.

EXPLORE SAFOUS