



GitProtect.io

Backup and recovery for **SOC 2** with **GitProtect**

Quick reference for SOC 2 audit preparation
and backup-and-recovery readiness



Why Backup and Recovery Are Key To Pass **SOC 2 Auditing**

SOC 2 is an attestation framework built on the AICPA Trust Services Criteria. It evaluates how well your internal controls operate over time across three categories:

- Systems are protected from unauthorized access (Security).
- Systems remain available for operation (Availability).
- Confidential data is protected (Confidentiality).

Backup and recovery are a core part of that picture and one of the clearest ways to show enterprise clients that you can protect their data and operate as a secure part of their supply chain.

- Data can be restored after an incident.
- Backup data is protected through encryption.
- Access is limited to authorized users.
- Recovery processes are tested regularly.
- Disaster recovery planning supports timely restoration.

78% of enterprise clients now require SOC 2 Type II certification from their service providers (Source: Gartner).

SOC 2 Backup and Recovery: What Auditors Usually Look For?

- ▶ Your backup and recovery policy
- ▶ Backup configuration and retention settings
- ▶ Sampled backup-success logs from specific dates
- ▶ Restore-test evidence with timestamps and outcomes
- ▶ Access lists for users who can modify or restore backups
- ▶ Proof that RPO and RTO targets are defined and realistic
- ▶ Disaster recovery procedures and test results



GitProtect supports the technical control layer by helping teams automate backups, protect backup data, monitor failures, run restores, support disaster recovery scenarios, and export operational evidence.

See how it can help your organization prepare for the audit.

Audit Preparation: Availability Controls

These mappings show where GitProtect most directly supports SOC 2 backup-and-recovery expectations. Final control ownership and auditor interpretation remain customer-specific.

SOC 2 Type II Control	How GitProtect helps preparation	GitProtect features to reference	Audit-ready evidence you can present
A1.2 Backup scope, scheduling, retention, and monitoring	Replaces ad hoc backup routines with centralized, repeatable backup execution.	• Central management • Automated backups • Flexible scheduler • Policy-based plans • Long-term retention • Backup of repositories and metadata	✓ Backup and Replication Summary ✓ Policy screenshots ✓ Scheduler and retention settings ✓ Sample backup-success logs ✓ Compliance Report
A1.2 Separate and resilient backup storage	Reduces single-point-of-failure risk by separating backups from production, supporting redundancy, and enabling isolated backup-storage designs.	• Own cloud or on-prem storage • Multiple storage options • Replication • Data residency of choice • Immutable storage • Air-gap design	✓ Storage destination settings ✓ Replication configuration ✓ Architecture screenshot showing separation from production
A1.3 Restore testing and recovery validation	Helps prove that recovery works in practice and within target expectations.	• Granular restore • Point-in-time restore • Restore to the same or a new device or account	✓ Restore test tickets ✓ Restore screenshots and logs ✓ Timing records against internal RTO/RPO

Audit Preparation: Confidentiality and Access Controls

These mappings show where GitProtect most directly supports SOC 2 backup-and-recovery expectations. Final control ownership and auditor interpretation remain customer-specific.

SOC 2 Type II Control	How GitProtect helps preparation	GitProtect features to reference	Audit-ready evidence you can present
C1.2 Protect confidential backup data	Protects backup content throughout its lifecycle with encryption and customer-controlled safeguards.	• Encryption in transit and at rest • AES-256 options • BYOK (bring your own key) • Zero-knowledge option	✓ Screenshots of encryption settings ✓ Key-management configuration ✓ Screenshots showing encryption enabled
CC6.1/CC6.2 Restrict backup administration and restore access	Supports least-privilege access and role-based authorization.	• RBAC roles • SSO • SAML • MFA/2FA for GitProtect accounts • Multiple admin and user accounts • Separation of duties	✓ Access matrix ✓ SSO/SAML configuration ✓ RBAC screenshots ✓ List of backup admins and restore-capable users
CC6.1 Create an auditable trail of access and change	Shows who accessed backup settings and who changed them.	• Advanced audit logs • Centralized management console	✓ Audit log exports ✓ Change history ✓ Evidence of privileged-user review

Audit Preparation: Disaster Recovery Controls

These mappings show where GitProtect most directly supports SOC 2 backup-and-recovery expectations. Final control ownership and auditor interpretation remain customer-specific.

SOC 2 Type II Control	How GitProtect helps preparation	GitProtect features to reference	Audit-ready evidence you can present
CC7.5 Recover from ransomware, deletion, corruption, or other incidents	Helps teams restore data and resume operations after a security event.	• Point-in-time restore • Granular restore • Cross-over recovery • Immutable storage • Non-executable backup copy	✓ Incident ticket ✓ Timestamped restore evidence ✓ Post-incident review ✓ Screenshot of successful recovery from an earlier point in time
CC9.1 Plan for major disruption scenarios	Supports broader resilience planning through alternate restore paths and replicated backup data.	• Replication • Restore to a new account • Cross-over recovery • Disaster recovery options • Data residency choice	✓ DR runbook referencing GitProtect ✓ Tabletop or failover test results ✓ Replication settings ✓ Alternate-restore screenshots
A1.3 Prove recovery procedures are tested and refined	Provides repeatable evidence that recovery procedures are tested and operate effectively.	• Restore features • Detailed task monitoring • Advanced audit logs • Alerts and reports	✓ Restore-test history ✓ Remediation records ✓ Recurring reports showing repeated execution ✓ <u>Restore Summary</u>

Common Audit Failure Points

Weak evidence, poor testing, loose access, or a gap between policy and technical reality can undermine audit credibility. Here is how GitProtect helps address those issues.

SOC 2 Type II Control	The failure point	How GitProtect helps resolve the problem
Availability A1.2	Policy says one thing, but the system does another.	Helps align actual schedules, retention, storage, and monitoring settings with the documented backup policy.
Availability A1.3, Recovery from security incidents CC7.5	No evidence of restore testing	Delivers proof that restore works and is repeatable.
Logical and physical access CC6.1/ CC6.2	Too many users can access, modify, or delete backups.	Supports least privilege and traceability.
Availability A1.2 , Risk mitigation CC9.1	Backups are stored too close to production,	Helps create separation and resilience if production is hit by outage or attack.
	Backups are stored only on-site.	Moves backup strategy away from single-location dependency and toward off-site or geographically diverse resilience.
Availability A1.2 , A1.3	RTO/RPO promises do not match reality.	Helps validate recovery expectations through monitoring, restore timing and reporting.

GitProtect: A Partner That Understands SOC 2 Audit Expectations



Backed by its own SOC 2 Type I and Type II audits and ISO 27001 certification, GitProtect is built around the same controls, processes, and standards its customers are expected to meet.

You work with a vendor that understands how backup, recovery, security controls, and audit evidence are evaluated during a SOC 2 audit.

[See case study](#)



**How Zoop, a
Fintech processing
2B+ financial
operations monthly,
backs up and
restores GitHub
repositories**

Financial institutions and their operations need reliable and proven protection. Zoop's approach can be an excellent example of the best security practices for other companies, not only financial ones



What you'll get with GitProtect

GitProtect is an automated backup and disaster recovery solution built for DevOps environments, including GitHub, GitLab, Bitbucket and Jira.

It protects source code and DevOps metadata from accidental deletion, ransomware, and service outages, so teams can restore quickly and keep delivery moving.

GitProtect helps you reduce backup-and-recovery risk and prepare the documentation needed for audit readiness and ongoing reviews.

Ready to see it in action?

[Book a demo](#)

