



GitProtect.io

How can GitProtect help you ace **your ISO 27001 certification audit?**

Quick reference for ISO 27001 preparation
and audit readiness in the technological area



ISO 27001: What it means for your business



Builds trust with customers and partners by **showing disciplined information security**.



Facilitates procurement and vendor risk reviews, especially in European markets.



Supports compliance with broader EU regulations, including NIS2.



Requires ongoing verification: controls **must be implemented, maintained, and audited**.



ISO 27001 controls fall into four groups: Organizational, People, Physical and **Technological**.

GitProtect supports the Technological group and strengthens the core principles tied to data security: availability, confidentiality, and integrity.

Audit Preparation: Resilience & Data Lifecycle

This table shows how requirements map to features, practical audit value, and typical evidence — use it to get orientation and assess fit against your ISO 27001 scope.

ISO 27001:2022 Control	How GitProtect helps preparation	GitProtect features to reference	Audit-ready evidence you can present
A.5.30 ICT readiness for business continuity	Supports recoverability for covered DevOps/Atlassian/M365 services through repeatable restore exercises.	• Restore capabilities ◦ point-in-time ◦ granular • Monitoring • Restore evidence	✓ DR exercise record ✓ Restore Summary ✓ Task monitoring (duration, status, restored resources) ✓ Audit log entries for restore events.
A.8.13 + A.5.30 Ransomware isolation	Supports survivable backup design against ransomware and recovery readiness.	• Immutable/WORM-style storage support (via your storage configuration), • Non-executable backup copy claim • Multi-storage • Replication • Air-gap design	✓ Evidence immutability is enabled on target storage ✓ Multi-storage configuration ✓ Replication configuration ✓ Restore test proof ✓ Describe air-gap as a design choice, not default.
A.8.10 Information deletion	Supports retention enforcement and controlled cleanup of backup data for compliance/archiving.	• Retention modes (time, copies, unlimited) • Documented deletion workflows for backup copies	✓ Retention configuration screenshots ✓ Deletion records (ticket, proof of deletion action) Note: immutability prevents early deletion until retention expires.

Audit Preparation: Security & Access Controls

This table shows how requirements map to features, practical audit value, and typical evidence — use it to get orientation and assess fit against your ISO 27001 scope.

ISO 27001:2022 Control	How GitProtect helps preparation	GitProtect features to reference	Audit-ready evidence you can present
A.8.24 Use of cryptography	Protects backup confidentiality and supports cryptography requirements for backups.	• Encryption in transit and at rest • AES-256 options • BYOK (your own key) • Zero-knowledge option, • Built-in password vault	✓ Screenshots of encryption settings ✓ Documented key approach ✓ Evidence of vault usage.
A.8.3 Information access restriction	Enforces least privilege in the backup/restore system.	• RBAC roles • Separation of duties • Advanced Audit Logs	✓ Role assignment screenshot ✓ Sample audit logs showing admin actions and restore actions.
A.8.5 Secure authentication	Aligns GitProtect console access with corporate authentication controls.	• SSO support • SAML 2.0 IdP integration (if enabled) • MFA/2FA for GitProtect account	✓ Screenshot of SSO/SAML configuration ✓ Internal rule “SSO/SAML required” ✓ Evidence of MFA enabled (if used).

Audit Preparation: Backup Management

This table shows how requirements map to features, practical audit value, and typical evidence — use it to get orientation and assess fit against your ISO 27001 scope.

ISO 27001:2022 Control	How GitProtect helps preparation	GitProtect features to reference	Audit-ready evidence you can present
A.8.13 Information backup (This control replaced A.12.3.1 from ISO 27001:2013)	Runs reliable, policy-aligned backups across supported platforms.	• Scheduler options • Retention rules • Scope-by-rules • LFS backup support • Compression controls • Workload controls ◦ backup window ◦ concurrency • Throttling resilience	✓ Backup plan exports (scope, schedule, retention) ✓ Monitoring view showing job success or fail ✓ Advanced audit logs export (backup start, backup end, errors) ✓ Compliance Report with information on: ✓ percentage of resources with an active backup plan ✓ SLA from last 24h ✓ encryption ✓ replication ✓ notifications ✓ reports usage
	Enables regular restore testing with traceable proof.	• Restore Summary • Detailed task monitoring • Advanced audit logs • Granular and point-in-time restore	✓ Restore test record ✓ Restore Summary screenshot/export ✓ Matching audit log entries

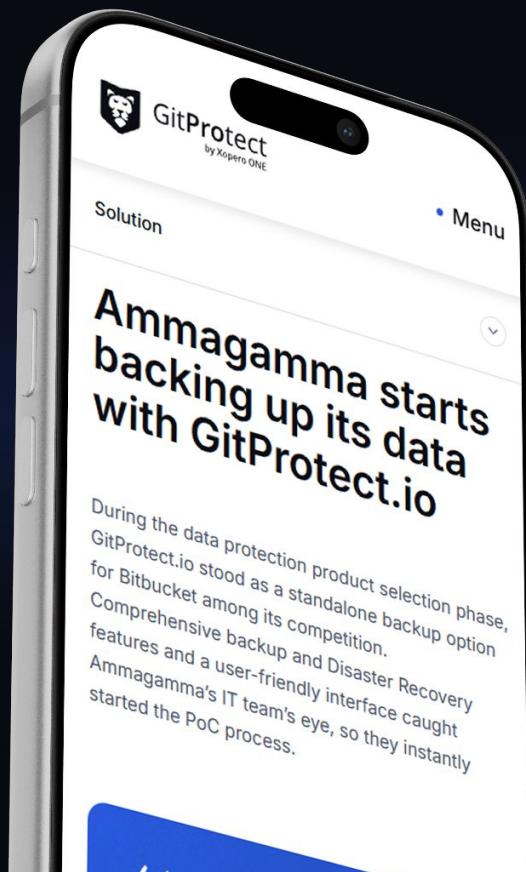
GitProtect: Your ISO 27001-certified partner



Backed by our own ISO 27001 certification and SOC2 Type II audit, GitProtect is built with the same discipline that certification requires.

We follow these controls ourselves, so you work with a partner who understands what auditors expect.

[See case study](#)





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 certification and ongoing audits.

Ready to see it in action?

[Book a demo](#)

