GitProtect.io

DevOps recoverability for NIS2 readiness

How GitProtect helps DevOps teams protect and recover critical data

NIS2 is in force, but implementation remains uneven

NIS2 came into force in January 2023. Member States had until October 2024 to transpose it into national law.

The deadline has already passed, but implementation still varies across the EU. Organizations operating in Europe should review local laws country by country to confirm scope, obligations, and enforcement details.

Non-EU providers should check NIS2 exposure. Covered providers may need to appoint an EU representative and follow the rules of the Member State with jurisdiction.

Pay attention if you:

- **operate as an essential or important entity in the EU**
- **provide in-scope digital or ICT services in the EU**
- **support regulated customers whose software delivery depends on your platforms, services or data**

How GitProtect supports NIS2-aligned recovery controls

GitProtect provides backup and disaster recovery for SaaS and software delivery assets across GitHub, GitLab, Bitbucket, Azure DevOps, Jira, Confluence, and Microsoft 365.

The table shows where those capabilities support NIS2-related continuity, control, and evidence needs.

NIS2 expectations	What organizations need to prove	How GitProtect helps
Business continuity, backup management, and disaster recovery	Critical data can be recovered after disruption.	DevOps backup and disaster recovery
Risk analysis and information system security policies	Backup scope and restore points reflect data and service criticality.	Risk-based backup planning
Incident handling	Teams can recover after data loss, outage, ransomware, or account compromise.	Controlled DevOps recovery

How GitProtect supports NIS2-aligned recovery controls

NIS2 expectations	What organizations need to prove	How GitProtect helps
Control effectiveness checks	Backup and recovery controls can be tested and reviewed.	Recovery monitoring and evidence
Cryptography and encryption	Backup data is protected from unauthorized access.	Encrypted backup storage
Access control	Backup and restore access is restricted.	Access governance
Supply chain security	Recovery paths exist beyond primary SaaS and DevOps platforms.	Platform independent backup
All-hazards approach	Organizations can recover from cyber, technical, or infrastructure disruption.	Resilient recovery architecture

Prove DevOps backup coverage for NIS2-related reviews

NIS2 risk management requires a clear backup scope. Organizations have to know which DevOps data is protected before an incident tests the plan.

GitProtect helps teams keep coverage reviewable with:

- Backup scope for DevOps data and metadata
- Defined backup plans
- Automatic inclusion of new resources
- Coverage visibility
- Protection across supported DevOps and SaaS platforms.

NIS2 value

Organizations can show which DevOps data is protected, where coverage applies, and whether new resources are included in the backup policy

35% of IT professionals **don't know if their backups are succeeding**, revealing a critical lack of coverage visibility for compliance.

Source: State of SaaS Backup and Recovery Report (2025)

Support RPO targets with with reliable restore points

RPO targets require matching backup frequency. Fast-moving DevOps environments need restore points that reflect the data and service criticality.

GitProtect helps teams create those restore points with:

- Scheduled backups
- On-demand backups before risky changes
- Backup frequency set by policy
- Time-zone-aware scheduling
- Handling of missed or overdue runs.

NIS2 value

Backup operations support defined RPO targets and risk-based backup policies.

92% of leaders are confident they can meet recovery targets, but only 39% actually achieve them during major operational disruptions.

Source: Optro / Corporate Compliance Insights Survey (2026)

Validate RTO with tested DevOps recovery paths

RTO targets depend on recovery paths that teams can run, test, and review.

GitProtect helps teams restore DevOps data with:

- Point-in-time restore
- Granular recovery of repositories and metadata
- Restore to the same location
- Restore to a new organization account
- Cross-over recovery to another platform
- Restore to a local device or local instance for DR scenarios.

NIS2 value

Recovery paths support business continuity and disaster recovery plans, RTO validation, recovery tests, and post-incident review.

_pit—

pit-cup GmbH **improved RTO by 50%** and cut security audit time by 60% after centralizing DevOps and Microsoft 365 backup with GitProtect.

Read case study

Prove recovery copies are retained, isolated, and controlled

Backup policy under NIS2 requires clear rules for retention, storage location, copy isolation, ransomware resistance, and access.

GitProtect supports those controls across 4 areas:

NIS2 value

Organizations can show how recovery copies are kept, protected, and restricted.

Retention

- retention policies
- long-term retention for audit and recovery needs

Isolation

- immutable S3 storage
- WORM policy
- S3 Object Lock

Storage control

- replication between storage locations
- cloud, on-premise, and hybrid storage

Access protection

- AES-GCM Encryption
- limited access to storage credentials
- access & least-privilege setup

Document backup and recovery controls for NIS2 audits

CISO and compliance teams need records that show backup and recovery controls were configured, executed, and reviewed.

GitProtect helps organizations document:

- Backup status and alerts
- Restore execution history
- Retention settings
- Access and activity logs
- Restore test evidence
- RTO and RPO comparison records.

versino

Versino AG **reduced audit preparation time by 30%** after replacing native backups with GitProtect.

Read case study

DevOps backup for NIS2 readiness

See how **GitProtect supports NIS2**-related backup, disaster recovery, and evidence needs for DevOps environments.

Ready to see it in action?

Book a demo