GitProtect.io

GitProtect for DORA

Backup, recovery, and audit-ready evidence for software delivery assets in financial services

DORA recoverability extends to DevOps assets

DORA requires financial entities to define what is backed up, test how it can be restored, and keep evidence that recovery controls work.

That requirement can extend to software delivery assets when repositories, CI/CD pipelines, and engineering metadata support critical or important functions.

These assets are often outside standard backup inventories. General-purpose tools and native DevOps platform features are not designed to protect the full working context needed for controlled recovery.

GitProtect brings governed backup, controlled restore, and audit-ready evidence to this layer.

Gartner recommends focusing on recovery assurance alongside traditional RTO and RPO metrics. Organizations must know what they can restore, but also trust the data they are restoring.

How GitProtect supports DORA recovery controls

GitProtect is an enterprise-grade backup and disaster recovery platform for critical SaaS and software delivery assets, covering GitHub, GitLab, Bitbucket, Azure DevOps, Jira, Confluence, and Microsoft 365 services.

Controlled backup operations

Scheduled backups and policy-based retention make protection consistent, governed, and less dependent on manual action.

Full-context recovery

Backup covers core data and metadata, helping teams restore complete DevOps working context after disruption.

Resilient recovery options

Point-in-time restore, alternative restore destinations, and replication strengthen recoverability and reduce dependency on a single environment.

Audit-ready evidence

SLA reports, logs, alerts, and compliance-oriented summaries make backup status easier to review, document, and demonstrate to auditors.

How GitProtect supports backup and restoration requirements

DORA requirement	How GitProtect helps	Useful GitProtect capabilities
Art. 12.1, backup policies and procedures, restoration and recovery procedures and methods	Backup and recovery procedures are defined, repeatable, and governed.	• defined backup scope • scheduled backups • auto-discovery of new sources • policy-based unlimited retention
Art. 12.2, backup systems and periodic testing of backup procedures and restoration/recovery methods	Restore methods can be tested, reviewed, and documented.	• point-in-time recovery • transparent restore execution • task summaries and details
Art. 12.3, segregated restoration systems and timely restoration of services	Recovery does not depend only on the primary environment.	• multiple storage destinations • replication • restore to an alternative destination • cross-restore options

How GitProtect supports response and recovery requirements

DORA requirement	How GitProtect helps	Useful GitProtect capabilities
Art. 11.2(a), continuity of critical or important functions	Software delivery assets supporting critical or important functions can be recovered.	• backup of core data with supported metadata • complete operational context • controlled recovery
Art. 11.2(b), response and recovery actions that prioritise resumption of activities	Teams can restore the right version to the right target.	• point-in-time recovery • granular restore • restore to original or alternative target environment
Art. 11.5, business impact analysis and redundancy of critical components	Recovery architecture reduces dependency on one storage location or failure domain.	• multi-storage architecture • storage flexibility • hybrid storage setup

How GitProtect supports protection and prevention requirements

DORA requirement	How GitProtect helps	Useful GitProtect capabilities
Art. 9.3(b), minimising the risk of corruption or loss of data, unauthorised access, and technical flaws	Backup routines reduce exposure and preserve recovery history.	• missed-run handling • retention that preserves restore chains • long-term retention history
Art. 9.3(c), preventing lack of availability, impairment of authenticity and integrity, breaches of confidentiality, and loss of data	Backup copies are protected against tampering, deletion, and unauthorised access.	• AES-GCM encryption • customer-defined encryption key • Object Lock/WORM support • zero-knowledge encryption modeL
Art. 9.4(b), limiting access, strong authentication, and key protection	High-impact backup and restore actions are restricted.	• RBAC • separation of backup and restore permissions • SAML SSO • MFA/2FA • Password Manager

Audit-ready evidence for DORA recoverability

When auditors ask, teams should not have to chase screenshots, logs, and status updates across tools.

GitProtect turns backup and restore activity into clear evidence teams can review, export, and explain.

Trace every action

Event logs, task states, searchable archives, and activity records to support incident review, accountability, and audit trails.

See protection status

SLA status, backup and restore activity, and compliance views in one place.

Detect issues promptly

Outcome-based alerts via email, Slack, or webhooks, along with daily summaries.

Export evidence quickly

SLA and compliance-oriented reports for audits, reviews, and governance checks.

DORA requires recoverability. GitProtect makes it demonstrable.

Financial entities subject to DORA need documented procedures, tested recovery, and audit-ready evidence. GitProtect delivers DORA-relevant backup and recovery controls for software delivery assets used in critical operations.

Ready to see it in action?

Book a demo