ISO27001 Gap Assessment - XDC Gateway

ISO/IEC 27001:2022 Gap Assessment Report

Organization: XDC Gateway (xdcrpc.com)
Assessment Date: March 2026
Assessor: Internal Security Team
Report Version: 1.0
Classification: Confidential

Executive Summary

XDC Gateway completed an internal ISO/IEC 27001:2022 gap assessment in March 2026. This report identifies the current state of our Information Security Management System (ISMS) controls relative to ISO 27001 requirements and establishes a remediation roadmap for formal certification.

Overall Compliance Score: 78%
Target Certification Date: Q3 2026

Scope

This assessment covers:

- XDC Gateway production infrastructure (xdcrpc.com, api.xdcrpc.com, platform.xdcrpc.com)
- Trust Center (trust.xdcrpc.com)
- Application layer including Next.js web app, API services, eRPC proxy
- Data storage: PostgreSQL databases, Redis caches
- Personnel: Engineering, Operations, and Customer Success teams
- Third-party sub-processors and vendor relationships

Clause Assessment Summary

Clause 4 — Context of the Organization

Requirement	Status	Notes
4.1 Understanding the organization	Implemented	Business context documented in ARCHITECTURE.md
4.2 Interested parties	Implemented	Customers, regulators, investors identified
4.3 ISMS scope defined	Implemented	Scope covers all production systems
4.4 ISMS processes	⚠ Partial	Formal ISMS document in draft

Clause 5 — Leadership

Requirement	Status	Notes
5.1 Leadership commitment	Implemented	CTO sponsors security program
5.2 Security policy	Implemented	Published Jan 2026
5.3 Roles and responsibilities	⚠ Partial	RACI matrix pending formal sign-off

Clause 6 — Planning

Requirement	Status	Notes
6.1 Risk assessment methodology	⚠ Partial	Risk register exists; formal methodology in progress
6.2 Risk treatment plan	⚠ Partial	Treatment options defined; acceptance criteria pending
6.3 Security objectives	Implemented	Availability 99.99%, recovery < 4 hours

Clause 7 — Support

Requirement	Status	Notes
7.1 Resources	Implemented	Dedicated security budget allocated
7.2 Competence	Implemented	Engineering team holds relevant certifications
7.3 Awareness	⚠ Partial	Annual security awareness training planned
7.4 Communication	Implemented	Incident comms via Telegram + email
7.5 Documented information	⚠ Partial	Some procedures not yet formally documented

Clause 8 — Operation

Requirement	Status	Notes
8.1 Operational planning	Implemented	Change management process in place
8.2 Risk assessment	⚠ Partial	Needs scheduling cadence (quarterly target)
8.3 Risk treatment	Implemented	Controls mapped to treatment plan

Clause 9 — Performance Evaluation

Requirement	Status	Notes
9.1 Monitoring and measurement	Implemented	PM2 metrics, Uptime Robot, custom dashboards
9.2 Internal audit	Gap	Internal audit program not yet established
9.3 Management review	⚠ Partial	Ad-hoc reviews; formal quarterly schedule needed

Clause 10 — Improvement

Requirement	Status	Notes
10.1 Nonconformity and corrective action	⚠ Partial	Incident process exists; formal CAR process needed
10.2 Continual improvement	Implemented	Monthly retrospectives include security items

Annex A Controls Assessment

A.5 — Organizational Controls

Control	Status
A.5.1 Policies for information security	Implemented
A.5.2 Information security roles	Implemented
A.5.15 Access control	Implemented
A.5.23 Information security for cloud services	Implemented

A.6 — People Controls

Control	Status
A.6.1 Screening	Implemented
A.6.3 Information security awareness	⚠ Partial
A.6.7 Remote working	Implemented
A.6.8 Information security event reporting	Implemented

A.7 — Physical Controls

Control	Status
A.7.1 Physical security perimeters	Implemented (data center)
A.7.4 Physical security monitoring	Implemented (via Hetzner)
A.7.8 Equipment siting and protection	Implemented

A.8 — Technological Controls

Control	Status
A.8.1 User endpoint devices	Implemented
A.8.2 Privileged access rights	Implemented
A.8.3 Information access restriction	Implemented
A.8.5 Secure authentication	Implemented (MFA enforced)
A.8.7 Protection against malware	Implemented
A.8.9 Configuration management	Implemented
A.8.12 Data leakage prevention	⚠ Partial
A.8.16 Monitoring activities	Implemented
A.8.20 Networks security	Implemented
A.8.23 Web filtering	Implemented
A.8.24 Use of cryptography	Implemented (TLS 1.3, AES-256)
A.8.28 Secure coding	Implemented
A.8.29 Security testing in development	⚠ Partial
A.8.34 Protection of information systems during audit testing	⚠ Partial

Key Gaps and Remediation Plan

Critical Gaps

Gap	Priority	Target Date
Formal internal audit program	High	Q2 2026
Security awareness training program	High	Q2 2026
Formal risk assessment methodology	High	Q2 2026

Medium Gaps

Gap	Priority	Target Date
Management review cadence	Medium	Q2 2026

Gap	Priority	Target Date
Corrective Action Request (CAR) process	Medium	Q3 2026
DLP tooling implementation	Medium	Q3 2026
Formal ISMS document	Medium	Q2 2026

Next Steps

1. **Q2 2026:** Close critical gaps (audit program, awareness training, risk methodology)
2. **Q2 2026:** Engage ISO 27001 certification body for pre-assessment
3. **Q3 2026:** Formal Stage 1 audit (documentation review)
4. **Q3 2026:** Stage 2 audit (on-site/remote implementation review)
5. **Q3 2026:** Target certification receipt

Conclusion

XDC Gateway has a strong foundational security posture with 78% of ISO 27001 controls implemented. The primary gaps are process documentation, formal audit programs, and management review cadence — areas that are well-understood and have clear remediation paths. We are on track for Q3 2026 certification.
