Continuous Compliance & Certification Program

ISO Standards & Global Certification Readiness

CONFIDENTIALITY NOTICE

This document contains certification roadmaps and compliance monitoring procedures. Distribution is restricted to Compliance, IT Security, Operations leadership, and Board committees.

1. ISO & Global Certification Roadmap

Global Dot Bank's systems and operational frameworks are architected for ISO and global certification standards, demonstrating commitment to world-class operational excellence.

Certification	Scope	Status
ISO 27001	Information Security Management System (ISMS)	Target: Q2 2026
ISO 22301	Business Continuity Management System (BCMS)	Target: Q2 2026
ISO 9001	Quality Management System (QMS)	Target: Q3 2026
SOC 2 Type II	Data Security, Availability, Confidentiality	Target: Q4 2025
PCI DSS	Payment Card Industry Data Security Standard	Target: Q1 2026

2. Certification Requirements & Implementation

2.1 ISO 27001: Information Security Management

- Comprehensive risk assessment and treatment process
- Documented ISMS policies and procedures
- Access control, encryption, and incident management protocols
- Annual internal audits and management reviews
- Third-party certification audit by accredited body

2.2 ISO 22301: Business Continuity & Resilience

- Business Impact Analysis (BIA) for all critical functions
- Documented BCP with RTO and RPO targets

- Regular testing and simulation exercises
- Crisis management and communication protocols
- Continuous improvement and lessons learned process

2.3 ISO 9001: Quality Management

- Customer-focused quality objectives
- Process approach to service delivery
- Evidence-based decision making
- Continuous improvement culture (Plan-Do-Check-Act)
- Leadership commitment and accountability

2.4 SOC 2 Type II: Trust Services Criteria

- Security: System protection against unauthorized access
- Availability: System operational as committed
- Processing Integrity: System processing is complete, valid, accurate
- Confidentiality: Confidential information protected as committed
- Privacy: Personal information collected, used, retained, and disclosed in conformity with commitments

2.5 PCI DSS: Cardholder Data Protection

- Build and maintain secure network and systems
- Protect cardholder data with encryption
- Maintain vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain information security policy

3. Ongoing Monitoring & Maintenance

- **Automated Compliance Dashboard: Real-time monitoring of certification controls**
- **Regulatory Update Engine: Adapts workflows to global rule changes**
- **Quarterly Certification Audits: Internal reviews to maintain readiness**
- **Annual Surveillance Audits: External certification body reviews**
- **Continuous Training: All staff trained on relevant certification requirements**

Certification Breach Protocol

Any non-conformance identified during surveillance audits must be addressed within 30 days. Major non-conformances require immediate escalation to COO and Board Risk Committee with corrective action plan.