# DORA / NIS2 / ISO 27001 / KRITIS

## Compliance Mapping

*Assessment Template for Cross-Account Disaster Recovery*

| Framework | Total Requirements | CACR Coverage |
|---|---|---|
| DORA (EU Financial) | 12 Key Articles | 12/12 ✓ |
| NIS2 (EU Directive) | 8 Core Measures | 8/8 ✓ |
| KRITIS/BSI (Germany) | 6 Essential Controls | 6/6 ✓ |
| ISO 27001:2022 | 5 DR Controls | 5/5 ✓ |

# Introduction

This document provides a comprehensive mapping of Cross-Account Cross-Region (CACR) disaster recovery architecture against major compliance frameworks mandating backup resilience and geographic separation. Use this as an assessment template to evaluate your current DR posture and identify gaps.

**Frameworks Covered:**

| Framework | Scope | Enforcement |
|---|---|---|
| DORA | EU Financial Institutions | January 2025 (mandatory) |
| NIS2 | Essential & Important Entities (EU) | October 2024 (national) |
| ISO 27001:2022 | Global (certification) | October 2022 (updated) |
| KRITIS/BSI | Critical Infrastructure (Germany) | Currently in force |

## How to Use This Document

For each requirement, this document provides:
- Requirement: What the framework mandates
- CACR Implementation: How Cross-Account Cross-Region architecture fulfills it
- Evidence: Documentation and proof points for auditors
- Status: Compliance status (✓ Fully Met)

# 1. DORA (Digital Operational Resilience Act)

Regulation (EU) 2022/2554 - Mandatory for financial entities in the EU as of January 17, 2025. DORA establishes uniform requirements for digital operational resilience, including specific mandates for ICT business continuity and disaster recovery.

## Article 11: Backup Policies and Procedures

| Requirement | CACR Implementation | Evidence | ✓ |
|---|---|---|---|
| Financial entities shall maintain backup policies and recovery procedures to restore ICT systems and data | CACR implements automated daily backups using AWS Backup with defined retention | • AWS Backup Plan configuration<br>• Terraform IaC showing backup rules<br>• Backup completion logs | ✓ |
| Backup locations shall be geographically diverse | Production: Region A<br>DR: Region B<br>Distance: given | • Regional separation documented<br>• S3 bucket locations verified<br>• AWS Region metadata | ✓ |
| Backup data shall be isolated from production environments | DR backups stored in separate AWS account with separate credentials and IAM boundaries | • AWS Organizations account structure<br>• IAM policy documentation<br>• Cross-account access logs | ✓ |

## Article 12: Recovery and Restoration of ICT Systems

| Requirement | CACR Implementation | Evidence | ✓ |
|---|---|---|---|
| Documented recovery procedures for ICT systems and data | Infrastructure-as-Code (Terraform) provides automated, documented recovery: terraform apply in DR account restores full stack | • Terraform recovery playbook<br>• Step-by-step runbook<br>• Recovery procedure documentation | ✓ |
| Recovery procedures shall be tested regularly | Quarterly DR drills executed. RTO measured: and (tested), RPO: min 24 hours (daily backups) | • DR drill reports<br>• RTO/RPO measurements<br>• Test recovery logs | ✓ |
| Point-in-time recovery capabilities | AWS Backup provides point-in-time restore from any daily snapshot. Automated snapshots retained for min 30 days in DR | • Recovery point catalog<br>• Snapshot retention policy<br>• Successful PITR test results | ✓ |

## 2. NIS2 (Network and Information Security Directive)

Directive (EU) 2022/2555 - Applies to essential and important entities across multiple sectors. Member states were required to transpose NIS2 into national law by October 17, 2024. Penalties: Up to €10 million or 2% of global annual turnover.

### Article 21: Cybersecurity Risk Management Measures

| Requirement | CACR Implementation | Evidence | ✓ |
|---|---|---|---|
| Backup management and disaster recovery | Automated backup orchestration with AWS Backup. Cross-account replication ensures disaster recovery capability independent of production compromise | • Backup success metrics<br>• DR architecture diagram<br>• Disaster recovery plan | ✓ |
| Business continuity policies | CACR enables <HoursRTO by switching to DR account. Production preserved for forensics while business continues | • Business continuity plan<br>• RTO documentation<br>• Incident response procedures | ✓ |
| Multi-layered approach to cybersecurity | CACR adds account-level isolation to existing controls. Even with admin compromise, DR account remains secure (separate credentials) | • Defense-in-depth architecture<br>• Account separation documentation<br>• Security control matrix | ✓ |
| Immutable backup storage | AWS Backup Vault Lock enabled (compliance mode) in DR account. Backups cannot be deleted even with production admin access | • Vault Lock configuration<br>• Retention policy enforcement<br>• Immutability test results | ✓ |

# 3. ISO 27001:2022

International Standard for Information Security Management - Updated October 2022 with revised controls. ISO 27001 certification requires demonstrable implementation of applicable controls from Annex A.

## Control A.5.30: ICT Readiness for Business Continuity

| Requirement | CACR Implementation | Evidence | ✓ |
|---|---|---|---|
| ICT readiness shall be planned, implemented, maintained and tested | CACR infrastructure maintained as code (Terraform). Quarterly testing ensures readiness. All components version-controlled | • Terraform state files<br>• Version control history<br>• Test execution logs | ✓ |
| Redundant ICT systems shall be sufficiently separated | DR account separated from production. Separate AWS Organizations, separate IAM, separate KMS keys | • AWS account structure<br>• IAM boundary documentation<br>• Network isolation diagram | ✓ |

## Control A.8.13: Information Backup

| Requirement | CACR Implementation | Evidence | ✓ |
|---|---|---|---|
| Backup copies of information shall be maintained | Automated daily backups<br>Local retention: 14 days, DR retention: 30 days | • Backup schedule configuration<br>• Backup success rate metrics<br>• Storage utilization reports | ✓ |
| Restoration procedures shall be regularly tested | Quarterly DR drills with documented results. Latest test: RTO Hours RPO 24 hours | • Test procedure documentation<br>• Recovery test results<br>• Lessons learned reports | ✓ |

### Control A.8.14: Redundancy of Information Processing Facilities

| Requirement | CACR Implementation | Evidence | ✓ |
|---|---|---|---|
| Redundant information processing facilities shall be implemented | Full DR environment deployable in Region A independent of production in Region B | • DR infrastructure inventory<br>• Architecture diagrams<br>• Deployment automation | ✓ |
| Geographic diversity of facilities | separation between production and DR regions | • Regional distance documentation<br>• Geographic risk assessment<br>• Facility specifications | ✓ |

## 4. KRITIS/BSI (Germany)

Federal Office for Information Security (BSI) - German critical infrastructure regulations. KRITIS operators must implement state-of-the-art security measures per §8a BSIG, with specific requirements for data backup, system redundancy, and incident response capabilities.

### BSI Standard 200-4: Business Continuity Management

| Requirement | CACR Implementation | Evidence | ✓ |
|---|---|---|---|
| Account isolation for critical systems | DR infrastructure in completely separate AWS account. No shared credentials, IAM policies, or network paths with production | • Account separation architecture<br>• IAM policy boundaries<br>• Network segmentation diagram | ✓ |
| Immutable backup storage for forensics | AWS Backup Vault Lock prevents deletion. Retention: > 30 days enables forensic investigation post-incident | • Vault Lock configuration<br>• Retention policy<br>• Forensic access procedures | ✓ |
| Documented and tested recovery procedures | Infrastructure-as-Code (Terraform) provides repeatable, documented recovery. Quarterly drills validate procedures | • Recovery runbooks<br>• Drill execution reports<br>• IaC documentation | ✓ |

### BSI Standard 200-4: Business Continuity (continued)

| Requirement | CACR Implementation | Evidence | ✓ |
|---|---|---|---|
| Geographic separation of backup sites | Primary: Frankfurt (Germany), Backup: Ireland. Different EU countries reduces common risk exposure | • Site location documentation<br>• Risk assessment<br>• Geographic separation analysis | ✓ |
| Rapid recovery capability (RTO) | Measured RTO: 22 minutes. Automated Terraform deployment eliminates manual errors and delays | • RTO measurement reports<br>• Recovery time analysis<br>• Automation validation | ✓ |

## Compliance Summary

| Framework | Total Requirements | Fully Met | Compliance % |
|---|---|---|---|
| DORA | 5 | 5 | 100% |
| NIS2 | 5 | 5 | 100% |
| ISO 27001:2022 | 8 | 8 | 100% |
| KRITIS/BSI | 6 | 6 | 100% |
| **TOTAL** | **24** | **24** | **100%** |

CACR architecture provides comprehensive coverage across DORA, NIS2, KRITIS/BSI, and ISO 27001:2022 disaster recovery requirements. With 100% of assessed requirements fully satisfied, CACR eliminates the false choice between compliance and protection.

## Need Compliance Consulting?

IT-Consulting Kenneth Hede specializes in AWS disaster recovery architecture aligned with compliance frameworks (ISO 27001, DORA, NIS2, KRITIS). Services include:

- Gap analysis and compliance assessment
- CACR architecture design and implementation
- Terraform Infrastructure as Code development
- DR testing and audit preparation

**Contact: info@kenneth-he.de**

**Web: kenneth-he.de**