ITSEC

CBUAE Security Standards Gap Analysis

Generated: December 8, 2025

Executive Summary

This gap analysis template enables self-assessment against Central Bank of UAE cybersecurity requirements.

Pre-filled with control mappings to ISO 27001:2022 and NIST Cybersecurity Framework (CSF) 2.0.

Assessment Methodology

For each control, rate your current implementation status:

- Not Implemented (0) - Control does not exist
- Partially Implemented (1) - Control exists but inconsistently applied
- Largely Implemented (2) - Control exists with minor gaps
- Fully Implemented (3) - Control is fully operational and tested

1. Governance Controls

Control 1.1: Information Security Policy [ISO 27001 A.5.1] [NIST ID.GV-1]

Requirement: Documented security policy approved by senior management

Current Status: ___ Gap Description: ____________________

Control 1.2: Security Roles & Responsibilities [ISO 27001 A.5.2] [NIST ID.GV-2]

Requirement: Defined security roles with clear accountability

Current Status: ___ Gap Description: ____________________

Control 1.3: Risk Management Framework [ISO 27001 A.5.7] [NIST ID.RA-1]

Requirement: Formal risk assessment and treatment process

Current Status: ___ Gap Description: ____________________

2. Technical Controls

Control 2.1: Access Control [ISO 27001 A.8.3] [NIST PR.AC-1]

Requirement: Role-based access with least privilege principle

Current Status: ___ Gap Description: ____________________

Control 2.2: Cryptography [ISO 27001 A.8.24] [NIST PR.DS-1]

Requirement: Encryption for data at rest and in transit

Current Status: ___ Gap Description: ____________________

Control 2.3: Network Security [ISO 27001 A.8.20] [NIST PR.AC-5]

Requirement: Network segmentation and monitoring

Current Status: ___ Gap Description: ____________________

2. Technical Controls (Continued)

Control 2.4: Endpoint Protection [ISO 27001 A.8.7] [NIST PR.PT-1]

Requirement: Anti-malware and endpoint detection solutions

Current Status: ___ Gap Description: ___________________

Control 2.5: Vulnerability Management [ISO 27001 A.8.8] [NIST ID.RA-1]

Requirement: Regular vulnerability scanning and patching

Current Status: ___ Gap Description: ___________________

3. Operational Controls

Control 3.1: Security Monitoring [ISO 27001 A.8.16] [NIST DE.CM-1]

Requirement: 24/7 security operations and log monitoring

Current Status: ___ Gap Description: ___________________

Control 3.2: Incident Response [ISO 27001 A.5.26] [NIST RS.RP-1]

Requirement: Documented incident response procedures

Current Status: ___ Gap Description: ___________________

Control 3.3: Business Continuity [ISO 27001 A.5.30] [NIST PR.IP-9]

Requirement: BCP/DRP with regular testing

Current Status: ___ Gap Description: ___________________

Remediation Roadmap Template

Priority 1 (0-30 days): Critical gaps affecting regulatory compliance

Priority 2 (30-90 days): High-risk gaps with significant exposure

Priority 3 (90-180 days): Medium-risk gaps requiring process changes

Priority 4 (180+ days): Low-risk enhancements and optimizations