CER Implementation Plan for Critical Entities

Entity Type: National Infrastructure Operator (e.g., Transport, Energy, Water, Health)

Key2XS®
your access to success

Executive Summary 4

Strategic Objectives 5

Organizational Reform 6

1. Appoint a Chief Resilience Officer (CRO) 6
2. Establish a Resilience Steering Committee 6
3. Update Governance Policies 6

Legal & Regulatory Adjustments 7

1. Gap Assessment 7
2. Update Internal Policies 7
3. Contractual Amendments 7
4. National Authority Coordination 7

IT and Cybersecurity Adjustments 8

1. Asset and Risk Inventory 8
2. Implement Resilient Architecture 8
3. Enhance Cybersecurity Operations 8
4. Identity & Access Management 8

Business Continuity & Incident Response 9

1. Business Continuity Plan (BCP) 9
2. Crisis Communication Protocols 9
3. Incident Drills and Tabletop Exercises 9
4. CER-Aligned Incident Playbooks 9

Supply Chain and Procurement Reform 10

1. Third-Party Risk Management 10
2. Procurement Policy Update 10
3. Cross-Border Coordination 10

Training & Culture Change 11

1. Awareness Campaigns 11
2. Executive and Board Briefings 11
3. Specialized Training Programs 11
4. CER E-learning Module 11

Timeline and Milestones 12

Budgeting and Governance 13

1. Budget Requirements 13

2. Performance Monitoring 13

3. Board Reporting 13

Executive Summary

This implementation plan outlines the necessary organizational, legal, technological, and procurement reforms for critical entities to comply with the EU Critical Entities Resilience (CER) Directive. The plan provides a 12–18 month roadmap and identifies key roles, investments, and policy changes needed to meet the directive's requirements.

Strategic Objectives

- Ensure full compliance with the CER Directive before the enforcement deadline.
- Establish enterprise-wide resilience across physical, cyber, and operational domains.
- Define accountability and reporting structures, including the appointment of a Chief Resilience Officer (CRO).
- Enhance cross-sector and public-private coordination in risk preparedness.
- Embed resilience into procurement and supplier governance frameworks.

Organizational Reform

1. Appoint a Chief Resilience Officer (CRO)

- Reports directly to CEO/Board
- Authority over crisis management, business continuity, and incident reporting

2. Establish a Resilience Steering Committee

- Include CRO, CISO, CIO, General Counsel, HR, and Operations

3. Update Governance Policies

- Incorporate CER principles into enterprise risk management (ERM)
- Develop a CER compliance charter and internal reporting structures

Legal & Regulatory Adjustments

1. Gap Assessment

- Conduct a legal audit against CER requirements
- Identify compliance risks in incident reporting, third-party contracts, and documentation

2. Update Internal Policies

- Incident notification workflows
- Data retention and audit trail obligations

3. Contractual Amendments

- Revise service-level agreements (SLAs) and procurement contracts to include:
  - CER resilience requirements
  - Notification obligations
  - Audit rights and remediation timelines

4. National Authority Coordination

- Formalize engagement channels with relevant CER supervisory bodies

IT and Cybersecurity Adjustments

1. Asset and Risk Inventory

- Classify IT/OT assets supporting essential services
- Conduct cyber-physical risk assessment

2. Implement Resilient Architecture

- Redundant systems, secure SCADA/ICS, remote access controls
- Logging, anomaly detection, and system segregation

3. Enhance Cybersecurity Operations

- 24/7 SOC monitoring, SIEM integration
- Align with NIS2 and ENISA best practices

4. Identity & Access Management

- Role-based access controls integrated with Identity Governance
- Auditable and revocable key systems

Business Continuity & Incident Response

1. Business Continuity Plan (BCP)

- Address natural disasters, cyberattacks, insider threats, and sabotage

2. Crisis Communication Protocols

- Internal and public messaging templates
- Authority approval workflows

3. Incident Drills and Tabletop Exercises

- Simulate hybrid threats (e.g., flood + cyberattack)
- Test regulatory reporting timeframes (24h / 72h)

4. CER-Aligned Incident Playbooks

- Custom scenarios for sector-specific threats

Supply Chain and Procurement Reform

1. Third-Party Risk Management

- Supplier audits and resilience scoring
- Continuous monitoring of critical vendors

2. Procurement Policy Update

- CER resilience as a precondition for eligibility
- Embed resilience KPIs into contracts

3. Cross-Border Coordination

- Apply EU resilience standards for multinational suppliers
- Align procurement frameworks with other CER-regulated entities

Training & Culture Change

1. Awareness Campaigns

- CER obligations and impact explained to all staff

2. Executive and Board Briefings

- Focus on legal liability, strategic risk, and governance reform

3. Specialized Training Programs

- Resilience planning (CRO, legal, IT)
- Emergency response (operations, facilities)

4. CER E-learning Module

- Integrated into onboarding for all new hires

Timeline and Milestones

Month	Milestone
1	CRO appointed, legal audit begins
3	Gap analysis and risk inventory complete
6	New BCP & incident response plan tested
9	Key vendor contracts updated
12	Final audit and CER compliance report submitted

Budgeting and Governance

1. Budget Requirements

- CRO function & committee operations
- IT infrastructure upgrades
- External legal & audit consultants
- Training and awareness programs

2. Performance Monitoring

- KPIs: incident response time, BCP test success rate, supplier risk reduction

3. Board Reporting

- Quarterly CRO reports
- Annual CER compliance review