

NIS2 Applicability Statement - World Bank

Document Version: 1.0

Publication Date: June 2, 2025

Author: [Your Name/CISO Office]

Approver(s): Board of Directors, CEO

Status: Draft

1. Introduction and Purpose

Use Case: This document formally declares and documents "World Bank's" status under the EU Network and Information Systems 2 Directive (NIS2). It identifies the relevant EU Member States of operation, defines the specific services and organizational units covered by the Directive, and outlines the bank's commitment to achieving and maintaining compliance. This statement serves as the foundational agreement on the scope of the NIS2 compliance effort within "World Bank."

The purpose of this Applicability Statement is to:

- Clearly define "World Bank's" obligations under the NIS2 Directive.
- Establish the scope of services, systems, and operations subject to NIS2 requirements.
- Identify relevant national authorities.
- Communicate the bank's commitment to cybersecurity resilience as mandated by NIS2.

2. Confirmation of "Essential Entity" Status

"World Bank" is confirmed as an **Essential Entity** under the NIS2 Directive. This determination is based on:

- **Article 3(1)(a) of the NIS2 Directive** and its classification within **Annex I, Section 3: Banking**. As a credit institution, "World Bank" provides services critical to the functioning of the economy and society.
- The bank's operational scale, including exceeding the employee and/or turnover thresholds for large undertakings as defined by the Commission Recommendation 2003/361/EC, where applicable under national transpositions.

3. Relevant EU Member States of Operation

"World Bank" conducts operations and provides essential services in the following EU Member States:

1. Netherlands (Primary EU Headquarters)
2. Germany
3. France
4. Italy
5. Spain
6. Poland
7. Belgium
8. Ireland
9. Sweden
10. Austria

○ *(Further Member States to be listed as applicable)*

4. Identification of National Competent Authorities (NCAs) and CSIRTs

For each Member State listed above, the relevant National Competent Authorities (NCAs) responsible for NIS2 oversight and the designated national Computer Security Incident Response Teams (CSIRTs) will be identified and documented in **Appendix A: List of NCAs and CSIRTs** (to be developed). This appendix will be maintained and updated as necessary.

Initial examples for Netherlands:

- **NCA (Example):** [To be identified based on Dutch national transposition - e.g., Agentschap Telecom or a newly designated body for the financial sector under NIS2]
- **CSIRT (Example):** Nationaal Cyber Security Centrum (NCSC-NL)

5. Scope of Applicability within "World Bank"

The NIS2 Directive applies to all network and information systems used by "World Bank" for the provision of its essential services within the EU. This includes, but is not limited to:

5.1. Essential Services Covered:

1. Retail Banking (Current Accounts, Savings, Loans, Mortgages)
2. Corporate Banking (Lending, Treasury Services, Trade Finance)
3. Payment Processing Services (SEPA, SWIFT, Card Payments)
4. Online and Mobile Banking Platforms
5. ATM Network Operations
6. Securities Trading and Settlement Services

7. Custody Services
8. Core Banking Operations
9. Financial Market Infrastructure services provided by the bank (if any)
10. Customer Data Management and Protection Services

5.2. Organizational Units Covered:

1. All EU-based branches and subsidiaries.
2. IT Department (Infrastructure, Applications, Security Operations).
3. Operations Departments supporting the essential services listed above.
4. Risk Management Department.
5. Legal and Compliance Departments.
6. Customer Service Departments interacting with essential services.
7. Third-Party Management functions related to critical suppliers.
8. Human Resources (regarding personnel security and training).
9. Internal Audit.
10. Data Centers and critical facilities supporting EU operations.

5.3. Network and Information Systems Covered: This includes all hardware, software, data, communication networks, and physical facilities that support the above-mentioned services and organizational units. A detailed inventory is maintained in the "List of Critical Services and Supporting Systems."

6. Key NIS2 Articles Directly Impacting "World Bank"

While the entire Directive is relevant, particular focus will be given to compliance with, but not limited to, the following articles:

1. **Article 20:** Governance
2. **Article 21:** Cybersecurity risk-management measures
3. **Article 23:** Reporting obligations
4. **Article 24:** Use of European cybersecurity certification schemes
5. **Article 25:** Standardisation
6. **Article 28:** Jurisdiction and registration
7. **Article 30:** General provisions concerning supervision and enforcement
8. **Article 32:** Supervisory and enforcement measures in relation to essential entities

9. Provisions related to supply chain security.

10. Provisions related to vulnerability handling and disclosure.

7. Exclusions

At this stage, no specific services or systems directly supporting the provision of essential services within the EU are considered for exclusion from the scope of NIS2. Any potential future exclusions will be rigorously assessed against the Directive's requirements and documented with full justification, subject to approval by the Board of Directors and consultation with legal counsel.

8. Statement of Commitment to NIS2 Compliance

"World Bank" is fully committed to achieving and maintaining compliance with the NIS2 Directive. We recognize the importance of robust cybersecurity measures to protect our customers, our operations, and the financial system. We will allocate the necessary resources and implement the required technical, operational, and organizational measures to meet our obligations under this Directive. Management at all levels is accountable for ensuring the effective implementation and oversight of our NIS2 compliance program.

9. Review and Update Cycle

This NIS2 Applicability Statement will be reviewed at least annually, or as significant changes occur within "World Bank" operations, the regulatory landscape, or the NIS2 Directive itself. Updates will be approved by the Board of Directors.

Appendix A: List of NCAs and CSIRTs (To be developed and attached)