PRIVACY PARTNERS

(CSP)

Prepared for: National Bank of Moldova

2025-08-29

Table of Contents

1. Executive Summary

This proposal outlines the approach, methodology, and project plan for conducting a SWIFT Customer Security Programme (CSP) assessment at National Bank of Moldova (NBM). The assessment will assess compliance with SWIFT's mandatory and advisory controls, identify potential gaps, and provide actionable recommendations for achieving full compliance and strengthening cyber resilience. The engagement will follow internationally recognized auditing and security assessment standards to ensure an independent, accurate, and comprehensive evaluation.

On our side we do offer extensive knowledge in audit methodologies, work in Republic of Lithuania and international bank's branches.

This document outlines scope and service delivery terms. Pricing is enclosed in separate document.

Customer SWIFT code: NBMDMD2X

SWIFT architecture (planned for assessment) – A1 or any lower level architecture

Physical location: depending on customer's requirements, Moldova, Chișinău

OFFICIAL REQUIREMENTS

SWIFT requirements to independent assessors:

Have sufficient training and knowledge of SWIFT and SWIFT security – including understanding of the SWIFT security control framework and detailed mandatory and advisory controls

Hold recognized industry qualifications: consultants should maintain industry recognized security qualifications or certifications such as QSA, CISSP, CISA, CISM, ISO certs

Are otherwise suitable for your needs and purposes, including successful completion of SWIFT CSP training tests

Privacy Partners UAB expertise:

PP consultants worked for number of years in banking environment, payment processing and PCI DSS areas, including QSA expertise, therefore team well know security assessment frameworks and SWIFT CSCF

PP consultants are Certified SWIFT CSP assessors and hold CISSP, CISA, CISM,
ISO/IEC 27001 LA certificates

Privacy Partners UAB has been included into official directory of SWIFT Customer Security Program Certified Assessors and are provided with SWIFT PIC (SWIFT Partner Identification Code) which will be included into assessment report as an evidence of independent assessment provided by eligible independent external party.

2. Understanding of Project Objectives and Scope

The main objective of this engagement is to provide NBM with an independent assessment of its adherence to SWIFT CSP mandatory and advisory controls. Generally, assessment includes those security and ICT governance areas:

- evaluating governance,
- risk management,
- security architecture,
- system hardening,
- access controls,
- incident response,
- compliance reporting.

Specific scope of proposed assessment is defined by SWIFT Customer Security Controls Framework. Most recent version will be used (CSCF v2026). In the table below (section 4.2) list of exact SWIFT security controls for typical A1 architecture is presented (control's numbers with A letter – Advisory controls). In case there will be different type of SWIFT architecture and underlying infrastructure - controls list may differ as it is reflected in *Table No.1*.

3. Working Assumptions

The following assumptions underlie the project:
- NBM will provide access to relevant documentation, systems, and personnel.
- The assessment will focus only on SWIFT-related infrastructure and processes.
- NBM will designate a project liaison to coordinate activities.
- Information and required data access will be granted in a timely manner.
- The assessment will be completed within the agreed timeframe.

Working language: official English, other languages which may be used according customer preferences – Russian.

Assessment will include at least 2 days on-site visit (audit) and one day visit for presentation of assessment results if it is requested by NBM.

4. Methodology and Approach

4.1 Methodology

Our audit approach is based on industry-recognized standards (ISO 27001, ISACA COBIT) and SWIFT CSP requirements. The methodology includes:

1. Planning and Initiation
2. Documentation Review

3. Technical Validation and Testing
4. Compliance Assessment

4.2. Reporting and Recommendations

As mentioned, most recent CSCF framework version (v2026) will be used. Key security controls for evaluation (for architecture A1, may be adjusted in the course of assessment planning):

Mandatory and Advisory Security Controls	Architecture Type				
	A1	A2	A3	A4	B
1 Restrict Internet Access and Protect Critical Systems from General IT Environment					
1.1 Swift Environment Protection	•	•	•		
1.2 Operating System Privileged Account Control	•	•	•	•	•
1.3 Virtualisation or Cloud Platform Protection	•	•	•	•	•
1.4 Restriction of Internet Access	•	•	•	•	•
1.5 Customer Environment Protection				•	
2 Reduce Attack Surface and Vulnerabilities					
2.1 Internal Data Flow Security	•	•	•		
2.2 Security Updates	•	•	•	•	•
2.3 System Hardening	•	•	•	•	•
2.4 Back Office Data Flow Security	•	•	•	•	
2.5A External Transmission Data Protection	•	•	•	•	
2.6 Operator Session Confidentiality and Integrity	•	•	•	•	•
2.7 Vulnerability Scanning	•	•	•	•	•
2.8 Outsourced Critical Activity Protection	•	•	•	•	•
2.9 Transaction Business Controls	•	•	•	•	•
2.10 Application Hardening	•	•	•		
2.11A RMA Business Controls	•	•	•	•	•
3 Physically Secure the Environment					
3.1 Physical Security	•	•	•	•	•
4 Prevent Compromise of Credentials					
4.1 Password Policy	•	•	•	•	•
4.2 Multi-Factor Authentication	•	•	•	•	•
5 Manage Identities and Separate Privileges					
5.1 Logical Access Control	•	•	•	•	•
5.2 Token Management	•	•	•	•	•
5.3A Staff Screening Process	•	•	•	•	•
5.4 Password Repository Protection	•	•	•	•	•
6 Detect Anomalous Activity to Systems or Transaction Records					
6.1 Malware Protection	•	•	•	•	•
6.2 Software Integrity	•	•	•	•	
6.3 Database Integrity	•	•		•	
6.4 Logging and Monitoring	•	•	•	•	•
6.5A Intrusion Detection	•	•	•	•	
7 Plan for Incident Response and Information Sharing					
7.1 Cyber Incident Response Planning	•	•	•	•	•
7.2 Security Training and Awareness	•	•	•	•	•
7.3A Penetration Testing	•	•	•	•	•
7.4A Scenario-based Risk Assessment	•	•	•	•	•

Table No. 1 – applicable SWIFT CSCF controls to be evaluated

Advisory controls typically are not required in the assessment, however depending on NMB intent also can be included in the scope

4.3 Tools

Tools and means which may be used during evaluation mainly include official SWIFT methodologies (high level testing plans, CSCF, other auxiliary materials) and interview frameworks.

We do work using minimal intervention principles. No customer systems can be accessed during assessment, any demonstrations or evidence collection is based on actions of authorized Customer employees which are specifically instructed how to support SWIFT assessment activities.

Documentation and evidence collection is carried out in accordance with security and confidentiality requirements. Depending on customer preferences – we may work in separately dedicated customer's environments (such as dedicated Microsoft Sharepoint library or Google Workspace G-drive folders) to ensure that any documentation used in the course of the assessment is not transferred through email and other

No external tools such as vulnerability scanners, configuration analyzers, penetration testing tools are planned to be used during this assessment. Connection to the systems are not planned.

There will be no change in evaluated systems configuration or state, such as granting guest or other access rights.

5. Response to Requirements

This proposal addresses all requirements outlined in the technical specifications, including:
- Comprehensive project scope and clear delineation of in-scope and out-of-scope activities.
- A structured and well-documented SWFT CSP assessment methodology.
- Compliance with SWIFT CSP standards and alignment with best practices.
- Provision of evidence, templates, and examples of deliverables.
- Inclusion of risk registers, communication templates, and project reports.

6. Project Management and allocated resources

The project will be managed using PMI PMBOK methodologies to ensure effective planning, execution, monitoring, and closure. Specific allocated experts:

Arūnas Krušas, SWIFT CSP certified assessor, CISSP, CISA, CISM – Project lead and manager; https://www.linkedin.com/in/arunaskrusas/

Martynas Bieliūnas, SWIFT CSP certified assessor, ISO 27001 Lead Auditor, CIPP/E, CIPM – review and some audit functions https://www.linkedin.com/in/martynas-bieliunas/

Company which will do official SWIFT CSP audit: UAB "Privacy Partners (included into SWIFT officially approved assessors registry.

Other staff form Privacy Partners Group team may be included for specific tasks.

7. Deliverables

Key deliverables for this engagement include:

- Project initiation documents
- Assessment work plan and schedule
- Interim assessment updates
- Draft assessment report
- Presentation to NBM management and stakeholders if requested by NBM
- Final SWIFT CSP assessment report
- Letter of Completion

SWIFT CSP assessment results should be manually entered into SWIFT KYC/SA portal by NBM.

8. Risk Management and Quality Assurance

Risks will be managed through continuous monitoring and mitigation strategies. Key risks include:
- Delays in access to information or personnel
- Changes in system configurations during the assessment
- Resource availability

Quality assurance will involve peer review of assessment findings, adherence to international standards, and structured reporting using SWIFT approved templates.

9. Proposed Timeline

The project is expected to last at maximum 3 months weeks, divided into phases:
1. Planning & Initiation – 2 weeks
2. Documentation Review – 4 weeks
4. Compliance Assessment – 4 weeks
5. Reporting & Closure – 2 weeks

The timeline may be adjusted based on NBM availability and system access.

10. Conclusion

This proposal presents a structured, compliant, and risk-aware approach to conducting the SWIFT CSP assessment for National Bank of Moldova. By following this methodology, NBM will receive a comprehensive assessment of its compliance posture, a clear roadmap for remediation, and enhanced cyber resilience in line with SWIFT requirements and industry best practices. Additionally, assessment results will be ready to be presented into official SWIFT directories.

Martynas Bieliūnas
CEO, Privacy Partners Group
Privacy Partners

PRIVACY PARTNERS ● NAUGARDUKO 41B, LT-03227, VILNIUS, LITHUANIA
INFO@PRIVACYPARTNERS.LT ● HTTPS://WWW.PRIVACYPARTNERS.LT ●
Ph.+370 5 254 8240
LEI CODE: 6488CGJ97GH1SX488335 ● BIC: PTSALTDD
LT COMPANY CODE: 304846919 ● VAT CODE: LT100011699818