Technical Offer

to provide SWIFT CSP audit services
for National Bank of Moldova

Submitted to:

National Bank of Moldova
1 Grigore Vieru Avenue, MD-2005,
Chișinău

Submitted by:

SC2labs sp. z o.o.
ul.Hrubieszowska 20
20-303 Lublin, Poland
T: +48 814669200

TAX (NIP): PL 946 259 25 25
ID (KRS): 0000340668

biuro@sc2labs.com
http://www.sc2labs.com

01.09.2025

INDEX

Confidential note

Introduction

SC2labs sp. z o.o. is pleased to offer our bid to provide audit services for SWIFT CSP

Scope of this offer includes assessment services in adherence to SWIFT Independent Assessment Process Guidelines.

For clarity our offered solution has been described below in detail.

We hope the proposed methodology, audit scope, experience and professional knowledge, as well as individual approach and cost-effectiveness will help you achieve SWIFT CSP compliance.
Should you have any questions or require additional information, please do not hesitate to contact our sales manager directly.

Mrs Joanna Busz
Sales Director
T: +48 505 94 04 74
@: joanna.busz@sc2labs.com

I.1 Company overview

SC2labs Sp. z o.o. (Limited) is a Polish company that delivers security consultancy and IT audit services to help our customers fight fraud, decrease lost and protect against crime and achieve compliance with international security standards like PCI DSS, ISO-27001, SWIFT etc.

We hold accreditation to conduct validation :

- **PCI QSA**
- **PCI 3DS**
- **PCI QSA (P2PE)**
- **PCI PA-QSA (P2PE)**
- **PCI PIN**
- **PCI SSF (PCI SSA and PSI SLCA)**

SC2labs is also listed in the **SWIFT Certified Assessors** list.

Our customers are commonly, but not exclusively financial organizations and commercial companies seeking to protect business-critical services in today's challenging online environment.

I.2 Company technical and formal resources **(PCI DSS, SWIFT)**

One of areas that SC2labs specializes is PCI DSS compliance and consultancy to help our customers achieve PCI compliance. We provide annual PCI QSA on-site audits for organizations qualified by PCI and acquirers as Level 1-2, as well as quarterly PCI ASV scanning for Levels 1-4. For merchants qualified as Level 2-4 we offer help and assistance in completing SAQ forms in accordance with PCI DSS requirements. Additionally we offer consultancy services in project scoping to prepare company to achieve compliance.

We are insured with CFC Underwriting at Lloyd's Bank London to the total amount of USD 2,000,000 Worldwide for Professional Indemnity, Website Damage, Public/Products Liability etc. arising from the business activities delivered in accordance with the PCI Agreement.

Quality of our services are best expressed by our satisfied customers willing to serve as references. What makes us different is our ability to provide unmatched technical and consultancy support.

Quick and easy access to dedicated engineer/auditor, who will analyze problems and recommend fitted solution is often key to success.

REFERENCES : Below you can find a set of our customers (limited to companies that allow us to share such information):

Alior Bank	-	bank
Austria Card GmbH (Austria)	-	payment agent
Bank Pekao S.A.	-	bank
BlueMedia S.A.	-	payment agent
ING Bank Śląski	-	bank
ING Tech (Netherlands)	-	payment agent, integrator
National Bank of Serbia (Serbia)	-	bank
UniCredit Services (Austria)	-	bank
Centrum kart SA	-	payment agent
Comarch S.A.	-	technology company
Dotpay S.A.	-	payment agent
eCard S.A.	-	payment agent
EXORIGO S.A.	-	payment agent
GoPay s.r.o. (Czech Republic)	-	payment agent/technology company
IT CARD S.A.	-	payment agent
Jeronimo Martins Polska	-	chain retail stores
Krajowa Izba Rozliczeniowa	-	key infrastructure institution in the Polish bank sector responsible for correct course of settlements between banks
Papara (Turkey)	-	payment agent
Polish Airlines LOT	-	airline agency
Polski Standard Płatności (BLIK)	-	payment agent
PKN Orlen S.A.	-	oil & gas company
Santander Bank	-	bank
Trustpay (Slovakia)	-	payment agent
Verestro / uPaid Sp. z o.o.	-	payment agent (mobile payments
Unlimint (Cyprus)	-	payment agent

I.3 Company employees qualifications (SWIFT and PCI DSS related)

SC2labs brings together a blend of security experts with backgrounds in management, engineering, systems architecture and support, networking and programming to create a uniquely intelligent and creative IT security business.

Our experts in security team dedicated to PCI DSS are PCI QSA, PCI SSF, PCI QSA (P2PE), PA-QSA (P2PE), PCI 3DS, PCI QPA, PCIP certified and are additionally holders of internationally recognized information security certificates like: ISACA Certified Information Systems Auditor (CISA) and/or (ISC)2 Certified Information Systems Security Professional (CISSP). Other certifications held are Unix/Windows certified system administrators, Cisco CCNP (network), CCIE (security), Certified ITIL experts. SC2labs is also accredited to perform SWIFT validation.

All of our security employees are background-vetted with Polish Criminal Court Register (KRK) and other legal entities for international employees.

We selected our top PCI experts to provide you the best possible services :

LEAD ASSESSOR :

Mr Grzegorz Landecki has over 24 years' experience from the Information Security field. Greg holds certificates: PCI QSA, PCI 3DS, PCI QSA-P2PE, P2PE, PCI QPA (PIN), PCI SSF, CISSP, CISA, CCNP, as well as he is also a **SWIFT Certified Assessor**. He has been coordinating SC2labs to become PCI ASV and PCI QSA ,PCI PA QSA. He also created scanning labs in USA for Fidelity Investments and participated in many project for leading security corporations like Symantec in Europe, India and USA. Greg is not only excellent technical expert, but has also business know-how and vast experience in managing multi-million projects. Mr. Landecki holds the position of Information Security Director.

Certficates:

- PCI Qualified Security Assessor (PCI QSA)
- PCI Qualified PIN Assessor (PCI QPA)
- 3DS Assessor
- PCI QSA Point-to-Point Encryption(P2PE)
- PA-QSA Point-to-Point Encryption (PA-P2PE)
- PCI Security Software Auditor (PCI SSA , PCI SLCA)
- ISC2 Certified Information System Security Professional (CISSP)
- ISACA Certified Information System Auditor (CISA)
- Cisco Certified Network Professional (CCNP)
- Certified Ethical Hacker (CEH)
- Sun Solaris Administrator

SECONDARY ASSESSSOR:

Mr Grzegorz Kosmowski has been with SC2labs since February 2020. He has over 22 years experience of managing networks, Windows and Linux servers security. Grzegorz is **SWIFT Certified Assessor**, PCI QSA, PCI SSF and ISO 27001 auditor. He possess CEH, CCNP and CISSP certificates, as well. In recent 6 years he has been dealing with entities preparation for PCI certifications, including PCI DSS, PCI SSF, PCI PIN Security a PCI P2PE.

Certificates:

- PCI Qualified Security Assessor (PCI QSA)
- PCI Security Software Auditor (PCI SSA , PCI SLCA)
- ISO 27001 Lead Implementer
- ISO 27001 Leading Auditor
- ISC2 Certified Information System Security Professional (CISSP)

- ISACA Certified Information System Auditor (CISA)
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Design Professional (CCDP)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Design Associate (CCDA)
- Certified Ethical Hacker (CEH)

PCI EXPERTS :

Mr Tomasz Plachecki has been with SC2labs since 2014 and brings with him 22 years of IT and IT security experience. He is PCI QSA, as well as PCI QPA(PIN), CCIE Security, CCSP,CCSA,CS-CSFS, ISO 27001. Tomasz is top security expert in networking, systems and data center designs. He has worked with many large financial institutions and merchants on projects around PCI DSS. Tomasz has coordinated many European projects including banking, military and government.

Mr Paweł Zadrąg joined SC2Labs in January, 2018. He has been in Information Security for 20 years. Paweł is PCI QSA and lead auditor for ISO 27001. Mr. Zadrąg is security expert and auditor with strong background in Linux-like systems, networking, virtualization and DevOps tasks. He worked as IT expert in government and military institutions. In addition to performing audits, he has worked with clients to perform gap assessments, assist with their prioritized approach, and provide remediation consulting to assist them in achieving PCI DSS compliance.

II. Project approach, methodology and management

Initial teleconference is to be held to define project timeline, detailed schedule, required meetings and required outcome, reporting methods etc.

SWIFT Customer Security Controls Framework (SWIFT CSCF) Assessment

SC2labs will perform audit services related to the verification of compliance with the SWIFT CSP standard.

The external independent assessment will be performed by Certified SWIFT Assessors and will cover all mandatory controls set out in the latest version of Customers Security Control Framework that are applicable based on B architecture type and infrastructure.

Technical Offer for SWIFT CSP Audit

I. Background and Context

SWIFT CSP Requirements

The SWIFT Customer Security Programme (CSP) mandates that SWIFT users annually attest their compliance with the Customer Security Controls Framework (CSCF), including both mandatory and advisory controls. These controls align with three objectives: Secure Your Environment, Know and Limit Access, Detect and Respond. The latest CSCF version must be adhered to, and independent assessments are required to support annual attestations.

II. Technical Offer Structure

a. Understanding Project Objectives, Scope, and Out-of-Scope

Objective: Provide an independent assessment to verify compliance with SWIFT CSP/CSCF requirements for the National Bank of Moldova (NBM), serving as secure input into the KYC-SA application.

Scope:

- Review of documentation, internal controls, and policies related to SWIFT security.
- Technical testing of IT infrastructure (firewall, MFA, encryption, monitoring).
- Operational and procedural assessments (access, incident management, authorization, continuity).
- Identification and reporting of non-conformities and risk-level assessment.
- Final compliance report, including status per control, evidence, and recommendations.

Out-of-Scope:

- IT development or implementation tasks.
- Remediation services beyond advisory recommendations.
- Post-assessment training or repeat audits (unless explicitly contracted).

b. Executive Summary

The proposed SWIFT CSP audit for NBM follows a structured methodology including planning, documentation review, technical testing, operational assessment, gap identification, and final reporting. Deliverables include the Audit Plan, Interim Report, Final CSP Compliance Assessment Report, Scope Validation Document, and Independent Assessment Confirmation Letter.

Typical challenges include evolving CSCF requirements, segmentation enforcement, monitoring setup, and maintaining independence. These are mitigated through structured testing, experienced assessors, and proven documentation templates.

c. Working Assumptions

General assumptions include access to documentation, systems, and staff. The CSCF version and SWIFT architecture type will be confirmed. Testing will be non-disruptive and evidence provided will be complete.

Stage-specific assumptions include:
- Kick-off: scope and responsibilities defined
- Documentation Review: full policy and logs provided
- Technical Testing: infrastructure accessible
- Operational Review: staff available for interviews
- Reporting: draft reviewed by NBM prior to finalization

d. Approach, Methodologies, Techniques, Standards & Deliverables

Framework & Standards: Mapping CSCF mandatory & advisory controls (latest version) to ISO 27001/2, NIST, PCI DSS best practices, and SWIFT guidance.

Methodologies:
- Documentation Review
- Technical Testing (vulnerability scans, config review, MFA, SIEM, encryption)
- Operational Assessment (interviews, incident simulations)
- Gap Analysis & Risk Assessment

Deliverables:
- Audit Plan
- Interim/Progress Reports
- Final Compliance Report
- Scope Validation Document
- Independent Assessment Confirmation Letter
- Working papers and evidence files

e. Detailed Response to Requirements & Evidence

Responses include:
- Documentation review coverage matrix
- Technical scan reports and evidence
- Operational interview notes and process charts
- Non-conformity register with risk ratings
- Confidentiality and independence statements
- Secure retention of evidence for 5 years

f. Project Management Description

Organizational structure includes a Lead Assessor, Technical Lead, Documentation/Process Lead, and Project Manager.

Quality assurance is ensured by peer reviews and adherence to audit standards.

Project Management Plan includes:
- Project plan (timeline, stages, responsibilities)
- Quality management plan
- Risk management plan
- Resource management plan
- Communication plan (status updates, escalation paths)

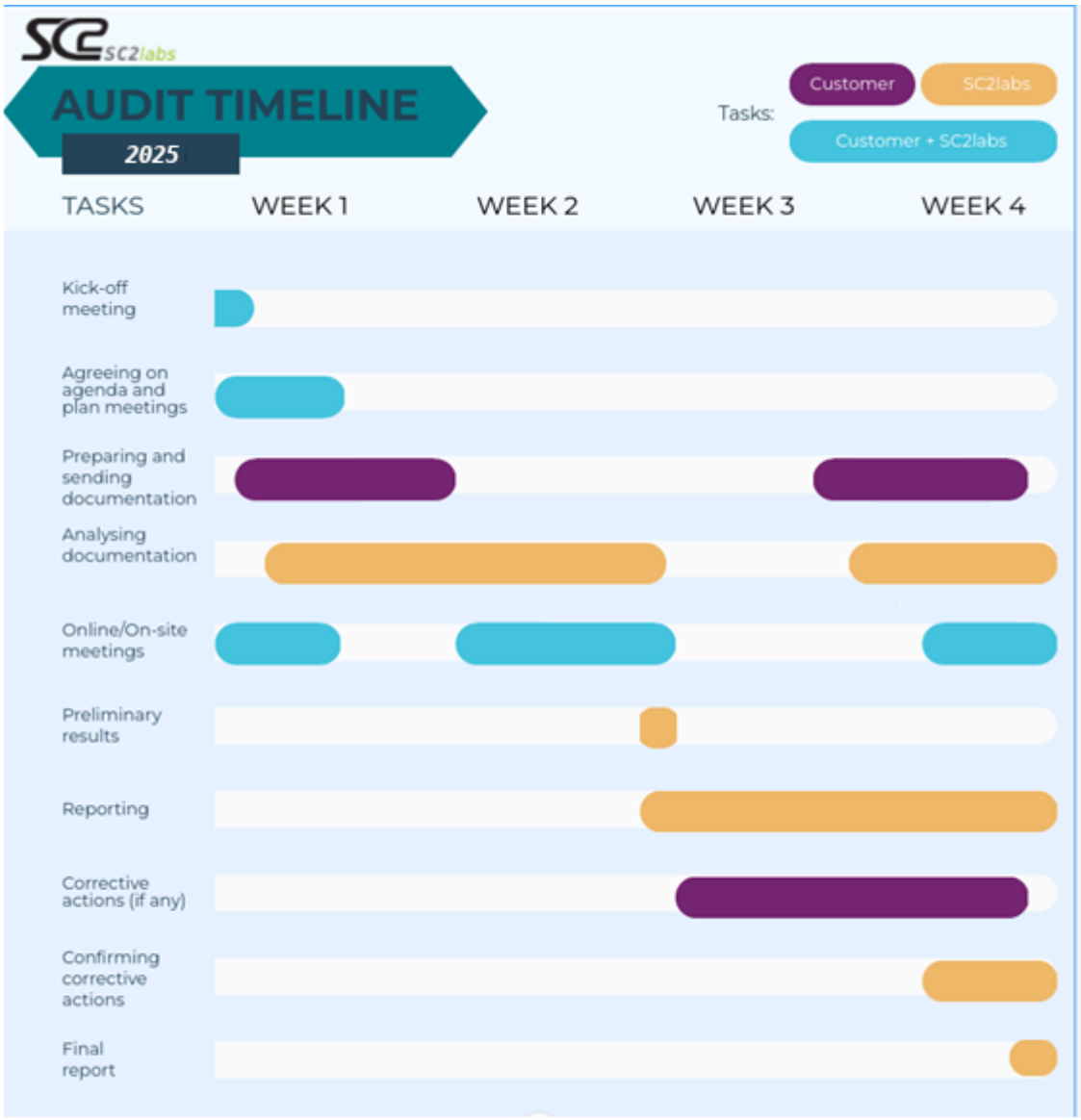
Appendices: risk register, issue log, deliverables tracker, communication log, templates for reports and meeting minutes.

III. Summary & Next Steps

This Technical Offer demonstrates understanding of SWIFT CSP/CSCF requirements and aligns with NBM's tender specifications. SC2Labs will deliver an independent and comprehensive compliance assessment.

Next Steps:
1. Confirm CSCF version.
2. Define SWIFT architecture type and scope.
3. Finalize timeline and logistics.
4. Sign confidentiality and engagement agreements.

Proposed general schedule:



III. Additional information

III.1 Terms and conditions:

This offer was prepared under following assumptions

- Calculation is based on the following data:
    - Service scope is estimated based on the documentation provided by the Customer
- During audit process customer will reduce to a minimum changes to network topology, audited systems, devices and applications to allow SC2labs auditors to provide realistic and authoritative assessment.
- Every work will be performed with strict cooperation with customer's representatives not to disrupt production systems or processes.
- Customer will provide all necessary access to required systems, devices, documents, services and employees to SC2labs auditors during audit.
- Deliverables will be provided in English.

III.2 Securing customer's data (overview):

Non-disclosure agreement will be signed with customer. Additionally SC2labs conforms to internal security standards.

Key points of securing customer data:

Place, methods and time of storage:

- Customer data is stored within encrypted container on SC2labs internal resource. Any working copy on laptop devices is encrypted.
- Encrypted containers are controlled by strong access-controls and available only on need-to-know basis
- Encrypted containers are securely deleted from network resource and archived on encrypted media.
- Archived results are stored for a maximum period of 3 years as required by PCI SSC and securely disposed

Transmission methods:

- Standard process of encrypting communication with customers is PGP
- In case PGP cannot be used, True crypt containers with passwords shared by different methods are used.
- Implementation of other methods are subject to approval

SC2labs employees

- Employees are requested to conform with SC2labs Code of Ethics
- SC2labs employees are required not to disclose any knowledge, information or data obtained from customer in the audit process.

Annex no.1
to the Specifications

Technical specifications

[This table will be completed by the Tenderer in columns 2,3,4,6,7 and by the NBM – in columns 1, 5]

Tender number: CPV Code: 72800000-8, 2025
Tender name: ***External independent assessment services in accordance with SWIFT Customer Security Programme (CSP)***

Name of services	The name of the model of the services	Countr y of origin	The manufacturer	Technical complete required specification	Technical complete offered specification	Standard reference
1	2	3	4	5	6	7
Lot : External independent assessment services in accordance with SWIFT Customer Security Programme (CSP)						
External independent assessment services in accordance with SWIFT Customer Security Programme (CSP)	SWIFT CSP assessment	Poland	SC2LABS	*In accordance with the detailed technical conditions which are described in Annex no. 3 of this Specifications (Requirements).*	Detailed in the Technical Proposal	SWIFT

Signed: _ _____ Digitally signed by Joanna Busz; SC2labs sp. z o.o. Date: 2025.09.01 12:17:09 +02'00' Name: Joanna Busz, Position: COO, Proxy

Tenderer:SC2LABS Sp. zo.o. Address: Poland, 20-303 Lublin, ul.Hrubieszowska 20