National Bank of Moldova

Proposal for IT Security Audit Services for SAPI Automated Interbank Payment System (technical description)

18 April 2023

bakertilly

ABOUT BAKER TILLY

Baker Tilly South East Europe is a full-service accounting and advisory group that offers assurance, tax and advisory services across all sectors of industry. Baker Tilly Advisory Services Limited is a member of the Baker Tilly South Easy Europe group specialised in transaction and other advisory services.

Every day, 500 professionals located in 16 offices throughout South East Europe (Cyprus, Greece, Romania, Bulgaria and Moldova) share their expertise to accelerate your growth.

At Baker Tilly we are ready Now, for tomorrow's challenges. We believe in the power of Great Relationships. We lead and listen for Great Conversations. We channel change into progress for Great Futures.

Over 25 years of successful experience in the markets of South East Europe

High quality services that meet your requirements and objectives

Understanding your business and experience in auditing enterprises in your industry

Providing professional support in accounting consulting, assurance, tax and advisory services

ISO 27001:2013
A globally recognised information security standard. Achieving accredited certification to ISO 27001 demonstrates that our organisation is following information security best practice.

ISO 9001:2015
Baker Tilly has implemented a quality management system and has been accredited with ISO 9001:2015 certification.

SWIFT CSP Assessment Provider
Baker Tilly Southeast Europe has been accepted and successfully registered with SWIFT as a CSP Assessment Provider, as part of its Customer Security Program.

DIGITAL AND RISK ADVISORY SERVICES

We can deliver tangible and measurable results through agile and flexible approaches which can accommodate even the most specific needs of our customers.

- **Cybersecurity Assessment & Improvement** (assess security of a client at process and system level and support the improvement program, including e.g. policies & procedures, technical security architecture, security incident response, security operations centre, support on certifications programs, e.g. ISO 27001)
- **Data Privacy** (assess adherence to GDPR or other regulations, implementation support, DPO services)
- **Business Resilience** (business continuity planning, IT disaster recovery services)
- **IT Transformation** (assess the overall IT environment of a client at people/process/technology level, benchmarking, IT strategy design and implementation)
- **Digital Transformation** (transform operating model to integrate digital technologies within the client's business model)
- **IT Program/Project Implementation Support** (system selection support, UAT, Project/Program/PMO management)
- **Enterprise Data Management** (data governance, reporting improvements, data analytics)

- **Internal Audit** (co-sourcing or outsourcing of Internal Audit services, risk assessment and audit planning)
- **Quality assurance review of Internal Audit functions** (review methods and practices of Internal Audit functions and provide recommendations for improvement)
- **Internal Controls setup and review** (design and review internal control systems, design and document policies and procedures)
- **Corporate Governance** (support clients to setup governance structures and document relevant policies and procedures)
- **Enterprise Risk Management** (support organizations to identify, assess and manage enterprise risks that could affect the achievement of business objectives)
- **Anti-Money Laundering** (help clients review, assess and improve their AML/KYC practices)
- **Environmental-Social-Governance (ESG)** frameworks (support clients build a framework and prepare for ESG reporting)
- **Assessment based on regulatory requirements** (e.g., Bank of Greece 2577 on internal controls, Capital Markets Corporate Governance requirements, etc.)

INDICATIVE PRIOR EXPERIENCE IN RELEVANT SERVICES IN SOUTHEAST EUROPE

IT AUDITS PERFORMED AT THE BANKING SECTOR

Moldova

- EXIM BANK
- ENERGBANK
- EUROCREDIT BANK
- MOLDICONBANK
- MOBIASBANCA
- PROCREDIT BANK

Romania

- IDEA BANK
- BANCA COMERCIALA FEROVIANA
- BRCI
- CREDIT COOP
- TECHVENTURES

Bulgaria

- UNICREDIT BULBANK
- POSTBANK
- PROCREDIT BANK
- PIRAEUS BANK
- D COMMERCE BANK

Greece

- PIRAEUS BANK
- ALPHA BANK
- INVESTMENT BANK OF GREECE

Cyprus

- HELLENIC BANK
- ALPHA BANK
- CYPRUS COOPERATIVE BANK
- BANK OF CYPRUS
- ASTROBANK

Our International team has also significant experience in providing IT audit services to central banks, e.g.

European Central Bank

IT AUDIT METHODOLOGICAL APPROACH

Our audit approach will be based on international IT, audit and security standards, as well as IT audit guidelines from the following institutions:

- ISACA
- NIST
- ISO
- OWASP

COBIT 5
AN ISACA® FRAMEWORK

ISO 27001

AUDIT PROCESS

The following diagram describes the project approach to be implemented, based also on the tender requirements:

Phases	1. Project Initiation	2. Audit Planning	3. Audit Execution	4. Reporting	5. Follow-up review
Key Activities	▪ Kick off meeting ▪ Prepare project plan ▪ Set up schedule and milestones ▪ Identify involved departments and stakeholders	▪ Understand the system components ▪ Review technical environment ▪ Identify and review relevant policies and procedures ▪ Prepare audit program and Information Request List	▪ Evaluate controls design, as per audit program ▪ Perform test of controls and technical assessment of in scope areas to assess controls effectiveness ▪ Conduct interviews with relevant teams	▪ Closing meeting to agree findings ▪ Document audit results / reporting ▪ Present audit report ▪ Agree action plans	▪ Analyze remediation actions performed ▪ Review and test where possible the findings closure ▪ Report and present the results of the follow-up
Deliverable	▪ Project Plan	▪ Audit Plan & Action Plan	▪ Progress Updates	▪ Audit Report	▪ Follow-up Report
Timeframe	▪ Approx. 1 week	▪ Approx. 2 weeks	▪ Approx. 4-6 weeks	▪ Approx. 1 week	▪ Approx. 1 week

Project Management & Monitoring

AUDIT SCOPE OF SERVICES

Audit Area	Audit Activities
The normative framework related to the system	Collect and review the policies, procedures and guidelines applicable to the operation of the SAPI system, and review against the design completeness based on international standards and NBM requirements.
Data security	Review the design of the data governance framework, data integrity and encryption, data replication and back up solutions, data classification and data leak prevention.
Identification and authentication of users	Review user management processes, registration and authorizations, allocation of access rights, user deactivation and access rights revoke, password standards and multifaction authentication, full access path review
Non-repudiation of transactions	Review the measures in place to verify the identify of the transaction originator, creation of audit trails and time stamps
Identity management and segregation of responsibilities	Review identity management, roles and responsibilities, conflicting roles and proper segregation of duties
Means of control for authorisation at system, database and application level	Review the access control mechanisms at system, application and database level, and network level if needed, and the credentials used to provide authorizations
Internal and external fraud	Review fraud risks internal (by NBM users, e.g. related to conflicting authorizations that allow a single user to perform a transaction) and externally (to execute unauthorized transactions or intercept transactions)
Audit journals	Review the mechanisms in place to record audit trails, their frequency and type, the storage parameters, who has access to view or modify, and the mechanisms for their analysis.

AUDIT SCOPE OF SERVICES (CONT.)

Audit Area	Audit Activities
Confidentiality of information in the process of data transport	Review the controls in place to protect data in transit, encryption at application/network level, internally and externally
Third-party security risk	Review the mechanisms to manage risks related to third parties, connectivity, contractual agreements, data protection, cybersecurity controls, network segmentation and monitoring
Physical security	Review the controls in place in data centers, physical access restrictions, environmental control restrictions
Incident management	Review the process for identifying events, their escalation to incidents, their classification and prioritization, responsible 1st/2nd/3rd line of support, incident resolution and recording
Vulnerability management	Review the process for periodically assessing the system components for security vulnerabilities, evaluate them and prioritize for mitigation, and follow-up measures
Effectiveness of the control measures implemented to manage cyber-attacks	Review the controls in place to mitigate cyber risks, such as ransomware, external intrusion, APT attacks, phishing attacks, etc.
Continuity of system operation	Review the mechanisms to ensure the system availability, in terms of backups, disaster recovery arrangements, system resilience and redundancy, etc.

bakertilly

Contact us

CONSTANTIN AGAFIȚĂ
Senior Audit Manager

I.C.S Baker Tilly Klitou and Partners S.R.L.
T: +373 22 233003 , Fax. +373 22 234044
Email: C.Agafita@bakertilly.md

ANESTIS DIMOPOULOS

Director, Head of Digital & Risk Advisory Services

Baker Tilly Business Consulting Services S.A.

Tel. +30 215 5006060 , Fax. +30 215 5006061

Email: a.dimopoulos@bakertilly.gr

Baker Tilly is a full-service accounting and advisory firm that offers industry specialised services in assurance, tax and advisory.

At Baker Tilly, we are ready now, for tomorrow's challenges. We believe in the power of great relationships. We lead and listen for great conversations. We channel change into progress for great futures.