Atomate

MTender Internal Audit

FINAL REPORT, 30 May 2020

Table of contents

Acronyms and Abbreviations used in the report

BA	Business Analysis (or Analyst)
BPE	Business Processing Engine
BPMN	Business Process Model Notation
CA	Contracting Authority
CDU	Central Database Unit
CE	Contracting Entity
CTIF	Center of Information Technologies in Finance
DDoS	Distributed Denial-of-Service
EA	Enterprise Architecture (or Architect)
EBRD	European Bank for Reconstruction and Development
EGOV	Agency for Electronic Governance
EO	Economic operator
eProcurement	Electronic Procurement
EU	European Union
GPA	Government Procurement Agreement
IPO	Input, Processing, Output
IS	Information System
JWT	JSON Web Token
MoF	Ministry of Finance (Moldova)
NEPP	Networking Electronic Procurement Platform
OCDS	Open Contracting Data Standard
PIN	Prior Information Notice
SDLC	Systems Development Life Cycle
SLA	Service Level Agreement
STISC	Information Technology and Cyber Security Service
UAT	User Acceptance Testing

Version control

The following is a list of all changes made to this document, the person making the change, the new version number and the reason why the change was necessary.

Version	Date	Description
0.1	10/12/2019	Interim Draft Report supplied by Atomate
0.2	17/12/2019	Interim Draft Report, with changes requested and commented by everis
0.3	11/01/2020	Draft Report, presented at the EBRD workshop
0.4	23/01/2020	Revised Draft Report supplied by Atomate
1.0	06/02/2020	Second Revised Draft Report updated by Atomate based on gathered feedback from Everis
1.1	17/02/2020	Third Revised Draft Report, with additional findings with regards to MTender deployment documentation
1.2	30/05/2020	Final Internal Audit Report - Additional findings and conclusions added based on the system deployment workshops - Comments from the implementation team - 2.4. Deployment Exercise / Workshop - 4.0 Alignment of MTender with EU Technical specifications - Updated conclusions and executive summaries - English editing and additional updates

1. Executive Summary

1.1 Overview of the internal audit

This is a final version of the internal audit report which summarises the results of examination and analysis of MTender – a multiplatform networking digital public procurement system, developed under the EBRD technical cooperation project: *Moldova - Policy and business advice and legislative support for eProcurement reforms (TCRS ID 1187)*, implemented by the EBRD between February 2016 and December 2019.
The objective of the internal audit report was:

- to provide a reasonable assurance that the MTender System - software and pilot implementation in Moldova is adequate and performing as designed, as well as identify any risks correlated with the solution and its associated data, sources, infrastructure and systems;
- to analyse and benchmark the MTender System against technical and functional requirements stipulated by the:
    - TECHNICAL CONCEPT for Automated Information System "State Register of Public Procurements" (MTender) to achieve digital public procurement cycle, forming an annex to Government Decision no. 705 of 11 July 2018;
    - TECHNICAL SPECIFICATIONS for the development of e-Procurement Information System (MTender), and IMPLEMENTATION SPECIFICATION Networking Multi-platform Electronic Public Procurement System MTender, developed for the EU Delegation to Moldova in September 2018.

The auditors revived technical cooperation documentation and MTender technical documentation, as available in the repository: https://my.huddle.net/workspace/36712039/files/#/folder/49506927/list , including MTender System pilot implementation review completed by Information Systems audit specialists.
This final internal audit report comments on system weaknesses identified by auditors that can affect the operations and further development of MTender as well as contains recommendations that address these weaknesses.

The key components examined during this Interim version of audit included:

- System alignment to the established technical requirements;
- Project implementation methodology assessment;
- Review of business processes implemented in the system.
- Platform security;
- Key interface efficiency and controls;
- Continuous monitoring.

1.2 Methodology

The audit approach and methodology follow the requirements set out in the Terms of Reference for the project: IT Audit of MTender.
Additionally, the assignment envisaged the review of business processes implemented in the system and ensured they follow the BPMN workflows based on standard bidding documents defined by the TC project.
The auditors also reviewed the system documentation, identified missing key points and where possible provided recommendations for its improvement.
The audit follows the basic principles of the Control Objectives for Information and Related Technology (COBIT) framework provided by ISACA and the IT Governance Institute. Additionally, In order to establish an objective overview, the auditor's consultants met and discussed the project with most of the

key organisations involved in the project.
Each section of the report includes brief information on used methodology, overview of the findings, detailed findings and related recommendations.

1.3 Summary of findings

This section summarises the findings for each of the audit topics.

The first item of the internal audit report contains results of analysis of MTender **alignment to the established technical requirements**. Components reviewed were working effectively and efficiently; while auditors were not able to ensure a review of MTender components outside control of the TC project team, in particular controlled by MTender Operator. We have identified shortcomings around missing architecture / functionality documents versioning. Our auditors were also unable to identify the minimal set of User Stories required to be implemented by NEPPs, which is important to be defined to avoid missing or incomplete implementation of the feature requirements as well as untested features.
Summary of the findings & recommendations:

- **Documents versioning should be revised in order to keep historical information handy for the interested parties**. Additionally, clear segregation of implementation phases should be covered by the documents;
- **The business process models in BPMNs are split between the MTender CDU, the NEPPs and the eGovernment services**, which may represent a risk, but is not an issue, rather than a highlight of the distributed architecture particularity;
- **A minimal set of User Stories for NEPPs is not defined** and it would be recommended to formalise a list so that precise flows are known to the NEPP developer before starting the implementation.

The second item of the internal audit report presents the results of our assessment of **project Implementation methodology** , where we worked closely with the developers to understand the methodology and identify any possible shortcomings. Overall, we were impressed by the quality and effectiveness of the project implementation team. However, we have identified that the MTender System maintenance and operations documentation was required to be improved. In addition, we found issues around acceptance of the features by TC project beneficiary and thus ineffective process of approval of changes to the MTender System. Among other findings we would like to highlight that MTender rely on functionality testing by the NEPPs and the MTender CDU releases and communication with the NEPPs would benefit from operational improvements.

Summary of the findings & recommendations:

- **Business Analysis and Architecture of the system is reliant on one key resource**. Most organizations separate the roles of the BA and EA and we recommend separating the key role.
- **Change approval process requires improvement**. We were unable to find confirmation of a clear change approval process with the involvement of project stakeholders.
- **Ownership of knowledge management and the systems that support it**. It appears that technical knowledge management systems are owned by the TC project team. We recommend that project owners establish and maintain ownership of critical systems, including repositories, knowledge management and other types of information and artefact storage systems.
- **System operation and maintenance documentation should be improved.** The deployment documentation is available, detailing the full process of the deployment of the platform and associated services. We found the quality and completeness of the deployment documentation satisfactory, however we maintain our recommendation that additional maintenance and system operations documentation may be needed.
- **CDU release process to NEPPs, as well as communication and documentation around this requires improvement**. We have identified that the release process is not streamlined and the parties

involved in handling CDU changes (NEPPs) are not satisfied with timelines and communication involved.

- **CDU User acceptance testing seems to be reliant on NEPPs**. Our investigations show that, while extensive testing is being performed upfront, the developer relies on NEPPs as the final acceptance testing. Our recommendation is to ensure Acceptance testing is performed with every release.
- **Limited automation testing implemented in both CDU & NEPPS**. Our investigations confirmed that limited automation testing is being performed on CDU and NEPPs. The recommendation is to increase the coverage of automated integration testing for both CDU and NEPPs, however this depends on the technical decision by the project leaders
- **Project beneficiaries not involved in acceptance of the features.** We recommend that stakeholders designate one or more resources representing their entities to be involved in the acceptance of features implemented by the system during the process of development.

The third item in the internal audit report focuses on auditing implemented **business processes**, with the objective to identify risks, recommendations and/or solutions with regards to missing or incomplete workflow implementations, missing or incomplete documentation as well outdated or undocumented changes to the initial specifications of the MTender System. While we are satisfied with the processes as being in good shape, we managed to identify a few weaknesses, mainly around missing processes and documentation.

Summary of the findings & recommendations:

- **The technical documentation file (*5.2. EBRD MTender Technical Specifications v16.0)* should be updated to clearly differentiate between the requirements for the specific piloting phases (MTender Pilot Phase 1, MTender Pilot Phase 2 and MTender Pilot Phase 3 and any future MTender functionality to be implemented**;
- **CE, EO and CA registration procedure within the NEPPs should be clearly differentiated on the NEPPs implementation**, which, subsequently, should be formally required in the SLA or the list of minimum required User Stories for NEPPs to implement.

The fourth item in the internal audit report analyses **MTender's system security.** The evaluation was conducted to identify any possible security weaknesses and risks. The audit results confirmed that the basic security mechanisms are quite robust, but the security of MTender integration with NEPPs should be reviewed and improved. In addition to this, we could not confirm essential security procedures and checks with regards to MTender performed by STISC or CTIF, (i.e. penetration testing, DDoS protection or regular security checks).

Summary of the findings & recommendations:

- **Database data is not encrypted as required by the security requirements**. The specifications require that "All data stored in various components of the system (including CDU & NEPPs) (i.e. servers, data storage, LDAP) must be encrypted.". Our opinion is that excessive encryption may be an overkill in some situations and it may lead to performance degradation and unnecessary complexity. As such, we don't see any reasons to encrypt publicly accessible data, and recommend encryption of only sensitive system data (i.e. passwords, personal data, tax information, security keys etc).

  Comment from everis: The specifications have been changed upon this recommendation.

- **We could not confirm essential security procedures and checks around the production system**. CTIF representatives (MTender Operator) confirmed that security procedures are STISC responsibility, but we could neither confirm this, nor see any security reports or papers with regards to MTender CDU. Our recommendations are to ensure that essential security procedures

and checks are taking place ensured by MTender Operator.

- **Missing NEPPs Security audits required for accreditation and security policies**. We identified accreditation reports for NEPPs completed in October 2018, but could not confirm whether security audits have been prepared by the NEPPs involved with MTender. The procedure of accreditation requires annual security audits, but it is unclear how NEPPs should proceed with this audit. Our recommendation is to enforce security compliance as defined in the document "Regulation on establishing operations of the MTender System".
- **MTender Operator testing of NEPPs**. We could not confirm whether MTender Operator has conducted full testing of existing NEPPs. The procedure of accreditation clearly states that one is required[1].
- **Additional certification requirements for NEPPs and other involved parties may be considered.** Our recommendation would be to consider requiring ISO 27001:2013, ISO/IEC 27018:2014 organisation certification for NEPPs. This will ensure processes are in place to reduce information security risks,

The fifth item in the internal audit report focuses on **key interface efficiency and controls.** The focus of the audit of the key interface efficiency and controls was to identify risks, recommendations and/or solutions with regards to potential data conversion or data integrity issues as well as identify and analyse controls in place. The audit discovered that most of the controls are identifiable and cover the data input, processing and output, however, it cannot be confirmed that performance and load testing has been performed on the CDU to ensure that the non-functional requirements are satisfied. Additional findings have been also documented, mainly regarding API documentation and the operation and transactions logs.

Summary of the findings & recommendations:

- Input Controls
  - **Operation and transactions logs access is unclear, we recommend defining the required access level in the documentation and describe the logging level;**
- Processing controls
  - **Processing controls need to be clearly defined;**
- Output controls
  - **Output controls need to be clearly defined;**
- Public API key efficiency
  - **Performance and load testing has not been done**, however, is mentioned in the *5.2. EBRD MTender Technical Specifications v16.0* document as a non-functional requirement and is recommended with each release. We support the recommendation and suggest performing the load and performance testing with each release.

Finally, the sixth item in the internal audit report reviews **continuous monitoring**, disaster recovery and business continuity**.** The evaluation was conducted to identify any possible risks with regards to the system's potential problems arising from its operation, as well as ensuring adequate maintenance, incident management and disaster recovery procedures. We have identified that the system's monitoring documentation is incomplete, which is helpful with operations and maintenance. Additionally, the audit identified serious shortcomings with regards to MTender Operator knowledge and capability to take ownership of the system. The audit was not also able to confirm that full Disaster Recovery processes are in place.

Summary of the findings & recommendations:

- **System operation and maintenance documentation should be improved.** The deployment

[1] As defined in the document "Regulation on establishing operations of the MTender System" (30), available here https://ebrd.huddle.net/workspace/36712039/files/#/7396016

documentation is available, detailing the full process of the deployment of the platform and associated services. We found the quality and completeness of the deployment documentation satisfactory, however we maintain our recommendation that additional maintenance and system operations documentation may be needed.

- **MTender Operator lacks system knowledge and capability.** MTender Operator (CTIF) stated that the operation team lacks MTender System knowledge. Our recommendation would be to ensure CTIF/STISC have trained resources in place to take responsibility for the operations of the MTender System.

> **Comment from Everis: A training to CTIF operator was provided in 20149 and training documentation was provided.**

- **MTender Operator team lacks understanding the operational requirements of the system.** MTender Operator (CTIF) confirmed that they don't have the information regarding minimum, optimal and maximum operational requirements of the system. Our recommendation would be to ensure CTIF obtains this information.
- **System monitoring documentation and scalability/performance recommendations.** In order to ensure that the MTender Operator is fully capable of performing monitoring and scalability operations, we recommend compiling additional documentation and guidelines in this regard.
- **Monitor NEPPs availability and functionality independently.** MTender Operator relies on NEPPs to communicate their availability figures[2]. Our recommendation is to set up NEPPs monitoring independently to obtain uptime figures directly to avoid relying on NEPPs to communicate failures.
- **CDU Disaster Recovery process is unconfirmed.** We could not get a confirmation from MTender CDU or STISC that some of the Disaster Recovery processes are put in place (e.g. Data and restoration) and are being monitored correspondingly. However, as the system is hosted in MCloud we believe Disaster Recovery has been at least partially addressed by the MTender Operator. Our recommendation is to ensure a full Disaster Recovery Plan is available and enabled by the MTender Operator.
- **Most incidents are currently dealt with and advised on by the TC project team.** Our recommendation is to ensure that the MTender Operator takes ownership of the incident management process to reduce reliance on the external resources.

1.4 Summary of conclusions

Overall, our opinion is that the system is technically and functionally competent, it is designed to be secure, scalable and stable, the project methodology used is mostly suitable.
The functional and non-functional requirements are mostly respected and the BPMNs work as expected.
The operational issues around the MTender System are mainly based on lack of knowledge and quality technical documentation, capacity and training of the MTender Operator and the lack of completion of the accreditation process of NEPPs.
The quality of technical documentation and understanding of the MTender System deployment process has been addressed by a separate workshop completed upon the request of the Bank in March 2020 (see 2.4 - Deployment Exercise / Workshop).

Analysis of the alignment of the current pilot versions of the MTender System (Pilot Phase 2 is deployed in productive environment in the MCloud (last release March 2019) and Pilot Phase 3 is deployed in the

[2] As defined in the document "Regulation on establishing operations of the MTender System", available here https://ebrd.huddle.net/workspace/36712039/files/#/73960165

MCloud sandbox (last release December 2019)) with Technical concept for Automated Information System "State Register of Public Procurements" (MTender) to achieve digital public procurement cycle (Annex to Government Decision no. 705 of 11 July 2018) and Technical Specifications for the development of e-Procurement Information System (MTender), and Implementation Specification Networking Multi-platform Electronic Public Procurement System MTender, developed for the EU Delegation to Moldova in September 2018, auditors have drawn two conclusions. In respect to Technical concept (Annex to Government Decision no. 705 of 11 July 2018), MTender Pilot Phase 2 and Phase 3 complies with requirements specified in the Technical concept, as appropriate for the piloting stage.
As regards alignment of the pilot versions of the MTender System with Technical Specifications and Implementation Specification developed for the EU Delegation to Moldova in September 2018, there are a few important differences, however these are conceptual. The main difference are a higher open data and transparency standards proposed in the MTender functional and technical specification, in particular online real time OCDS data publication and a principle of collaborative shared services (a distributed architecture system between the government and the private sector) as a leverage for better interoperability and further market development benefits.

2. About MTender

MTender is a multi-platform digital procurement service that comprises a government-operated web portal and the Open Data central database unit and is integrated with several commercial electronic platforms certified to support electronic tendering procedures for public sector and commercial clients.

The goal of MTender is to ensure improvement of the transparency and efficiency of procurement of goods, works and services aiming to benefit all stakeholders of public procurement processes: the Government, business community and citizens who use public services. One of its main tasks is to enable digital standardized procurement processes, decrease the amount of time the selling-buying cycle and encourage participation in public tenders by suppliers, service providers and contractors, as well as creating a transparent relationship between the Government and the local business community, small and medium-sized enterprises.

The version of the MTender under review is a **Phase 2 Pilot** deployed in productive environment in the MCloud (last release March 2019) and Pilot Phase 3 is deployed in the MCloud sandbox (last release December 2019, hence may not yet display all of the expected features of the final developed software. The audit process requires the IS auditor to gather evidence, evaluate the strengths and weaknesses of internal controls based on the evidence gathered through audit tests and prepare an audit report that presents weaknesses and recommendations for remediation in an objective manner to stakeholders.

2.1 Objective and Scope

The objective of the internal audit report was to provide reasonable assurance that the MTender software solution is adequate and performing as designed, as well as identify risks correlated with the application and its associated data, sources, infrastructure and systems.

The key components examined during this Interim version of audit included:

- System alignment to the established technical requirements;
- Project implementation methodology assessment;
- Review of business processes implemented in the system.
- Platform security;

- Key interface efficiency and controls;
- Continuous monitoring.

The report is important because it reveals the common information system weaknesses we identified that can affect the operations and future development of MTender. It also contains recommendations that address these weaknesses.

2.2 Approach and methodology

The audit approach and methodology follow the requirements set out in the Terms of Reference for the project: IT Audit of MTender.

The audit follows the basic principles of the Control Objectives for Information and Related Technology (COBIT) framework provided by ISACA and the IT Governance Institute:

- system alignment to the established technical requirements of MTender;
- system alignment to key reporting requirements and data lineage;
- key interface efficiency and controls;
- database security; and
- continuous monitoring.

Additionally, the assignment envisaged the review of business processes implemented in the system and ensured they follow the BPMN workflows defined by EBRD. The auditors also reviewed the system documentation, identified missing key points and where possible provided recommendations for its improvement.

Each section includes brief information on used methodology, overview of the findings, detailed findings and related recommendations.

2.3 Key meetings conducted by the team

During the duration of the audit, the auditor's consultants met and discussed the project with most of the key organisations involved in the project. The schedule of the meetings is presented below.

2.3.1 Meetings completed by Atomate Auditing team

Date	Participants	Topics reviewed
05/12/2019	Call with uStudio (Yulia Spasibova)	Project Implementation Methodology Security & Controls
09/12/2019	Meeting with Achizitii.md (Vadim Jeleascov)	NEPPs - experience, Functional requirements, Project development governance, API documentation, communication channels
16/12/2019	Call with Everis (Daniel Arosa Otero, Clara Raich Soler, Ivette Vilar Roldan)	Interim report clarifications & comments
18/12/2019	Meeting with E-licitatie.md (Tatiana Berlinski)	NEPPs - experience, Functional requirements, Project development governance, API documentation, communication channels
19/12/2019	Call with Everis and EBRD	General project discussions

	(Daniel Arosa Otero, Clara Raich Soler, Ivette Vilar Roldan, Eliza Niewiadomska)	
23/12/2019	Meeting with EGov (Dumitru Postu, Iurie Turcanu)	MTender history, EGov operations, participation of EGov in project implementation
23/12/2019	Meeting with Octavian Costas, Dorina Harcenco	MTender project history and implementation process
26/12/2019	Call with uStudio (Paul Boroday)	Project Implementation Methodology Security & Controls Continuous Monitoring
27/12/2019	Meeting with CTIF (Radu Cornea, Ștefan Condrea, Balan Vladimir)	Project Operations, Security & Continuous Monitoring
31/12/2019	Meeting with YPTender.md (Vitalie Aremescu)	NEPPs - experience, Functional requirements, Project development governance, API documentation, communication channels
09/01/2020	Meeting with MoF (Gabriela Cuneva)	General discussions around project implementation, technical issues and other relevant topics.
11/01/2020	Audit review session in London with Eliza Niewiadomska, everis, uStudio and other representatives	Atomate has presented the MTender audit report and answered questions in a review session in London.
27/02/2020 - 12/03/2020	Deployment Workshops with Everis and NetForce	Atomate took part in MTender deployment workshops organised by Everis and held by Netforce and UStudio developers.

2.3.2 Meetings requested but not confirmed yet

Date	Participants	Topics reviewed
	Meeting with STISC	Security Controls Continuous Monitoring

2.4 Deployment Exercise / Workshop

Between February, 27th 2020 and May 2020 Atomate undertake a new deployment of the MTender System from the deposited source code. Deployment workshops were provided for by everis and supported by technical specialists from uStudio and Netforce, an outsourcing IT company. The workshops lasted approximately 11 days and focused on detailing the deployment of the system to a quasi-production environment. Technical aspects of the infrastructure have been thoroughly discussed and analysed as well.

The source code used for the deployment used is available online: https://github.com/EBRD-Digital-Transformation-MTenderCode.

The deployment of the system has been completed on 12th of March 2020, on a cloud environment commissioned and configured by Netforce and Atomate specialists. There were 18 Linux virtual servers of various characteristics used in total. During the deployment exercise, the team undertaking the deployment carefully executed, analysed and discussed each step, in order to obtain a full understanding of all of the aspects of the deployment.
As a result, the system has been fully configured and system deployment has been followed up by a testing exercise with NEPPs. In order to confirm that the deployed system is working properly, a separate temporary NEPP instance has been installed, configured and tested. Testing exercise has been completed on 1 April 2020 and with the scope of the deployment achieved and documented, the quasi-production environment has been decommissioned in May 2020.

2.5 About Atomate

Atomate is an IT Consultancy established in 2011 in London, UK with a subsidiary in Moldova. Atomate offers services in information security, governance, enterprise risk management, compliance and assurance to clients. Our solutions are based on domain knowledge in finance, insurance, telecommunications, online gaming and e-commerce industries in Europe, the United States and the Middle East.

2.6 Atomate consultants involved in the audit

- **Andrei Lopatenco** - Team Leader and Senior Auditing Consultant;
- **Vitalie Chiperi** - Senior Auditing Consultant;
- **Vlad Mazureac** - Key Implementation Specialist & Agile Consultant;
- **Igor Marta** - Senior Security Expert;
- **Eugeniu Cucu** - Senior Continuous Monitoring Specialist.

3. Audit Findings

The section summarises the results gathered during our interim review of the system, analysis of the available documentation and interviews conducted with key persons involved.

3.1 System alignment to the established technical requirements of MTender

3.1.1 Background & Methodology

The objective of this assessment is to establish if MTender is in line with the technical requirements.

In order to establish the system's alignment to technical requirements, we collected and reviewed the existing MTender technical documentation and held interviews with stakeholders involved in the design and implementation of MTender. The following steps were conducted:

- Analysis: Collected and analysed technical documentation;
- Analysis: Discussed with key team members involved in the implementation MTender;
- Evaluation: Reviewed project management methodology and associated processes;
- Reporting: Compiled assessments and proposed recommendations.

The MTender system provides the following procurement methods as described by 5.1. *ARCHITECTURE CENTRAL UNIT OPEN OCDS UNCITRAL DIGITAL PROCUREMENT* document:

> - Single-stage competitive procedures (parallel and sequential);
> - Single-stage non-competitive procedures;
> - Multi-stage competitive procedures;
> - Multi-stage repetitive competitive procedures.

The stages are also mentioned in the " *The Annex II ToR_Annex II Technical specifications. Introduction: stages covered by MTender*". *Component 11: Workflows of Public Procurement Procedures* explains the requirements about public procurement procedures. These procedures are detailed in the Architecture documents. The stages and procedures and requirements associated with them are compliant with intended purposes.

The MTender Central Database Unit (CDU) public API is the only interface available for accessing and usage of the Central Business Process Engine. The Annex II ToR_Annex II Technical specifications. Components 12 to 22 have a first requirement as follows:"The module will expose a dedicated API to the NEPPs for data exchange and providing functional facilities." The requirement is compliant with intended purposes.

The Central Business Process Engine is the core of the MTender infrastructure, as described by 5.1. *ARCHITECTURE CENTRAL UNIT OPEN OCDS UNCITRAL DIGITAL PROCUREMENT* document:

> The business processing engine (BPE) is the logical layer responsible for identifying an event and then selecting and executing the appropriate reaction. It can also trigger a number of assertions. Processing involves tracking and analyzing streams of data from events to support better insight and decision making.
>
> The general set of BPE components separated into various procurement processes can be seen below:

Procurement process	Involved component

Budgeting	**eBudget**
Planning	**ePlanning**
Pre-Tendering	**eAccess**
Tendering	**eClarification** **eSubmission** **eQualification**
Evaluation	**eAuction** **eAwarding**
Contracting Implementation	**eContracting**
All procurement phases	**eNotice**

The procurement and other processes of MTender are clearly in line with the requirements of the EU technical specifications. (Section 4.3: main workflows of the IT system).

The list of components of the MTender system is aligned with the requirement of the EU technical specifications. (Section 5.1: Functional Requirements for the Central Data Base Unit). Accordingly, the MTender system would only need to accommodate new modules not foreseen during the current MTender implementation.

Effectively the MTender system consists of two main components, the CDU (backend) and the NEPPs (frontend). The business logic of the MTender system as well as the core functionality of the procurement lifecycle is integrated into the CDU.

This is compliant with the Annex II ToR_Annex II Technical specifications. The functionality of Central Database Unit MTender is structured in different modules, therefore, an update of the current modules and implementation of new modules will be more convenient than starting a new development from scratch.

It aggregates and processes the information provided by the NEPPs as well as integrates with other governmental information systems that provide relevant information about the public procurement parties / entities.

The implementation of the above-mentioned modules varies between the CDU and the NEPPs. The NEPPs responsibility is to develop the following set of components and integrate into the CDU:

- eRegistration;
- eAuthentication;
- eNotification;
- eAccess;
- eNotices;
- eSubmission/eTendering;
- eQualification;
- eEvaluation;
- eAwarding.

In addition to the entire procurement lifecycle implementation requirements, the CDU shall allow the MTender Administrator to grant or revoke access to the CDU public API entirely or in parts to/from the NEPPs as well as manage and administer the MTender system and the CDU in particular. This is in

compliance with section *6.5. Requirements for the Interoperability* of the EU technical specifications, which requires implementation of an API interoperable with different systems, and administered on the CDU side.

All the transactions, processes and phases of the public procurement are taking place on the CDU, that serves as the backend to the NEPPs, that consequently allow end users to make use of the MTender system, however, the NEPPs provide their own standalone features such as user registration, password retrieval, paid tender participation consultancy and other user-related functionality. NEPPs also allow end users to access and use the eGovernment services (treasury, state registers, etc) through the CDU. This follows the requirement presented in *section 5.1.1. Component 01: Workflows of Public Authorities* of the EU technical specifications.

DISCLAIMER: Only high level functionality has been tested. The audit process did not involve thorough testing of each functional requirement described by the technical specifications document.

During the audit, Atomate has discussed the implemented functionality with the CDU developer representatives as well as the NEPP representatives.

The architecture of the implemented system is described by 5.1*. ARCHITECTURE CENTRAL UNIT OPEN OCDS UNCITRAL DIGITAL PROCUREMENT* document, while the functional requirements have been described by the *5.2. EBRD MTender Technical Specifications v16.0* and subsequently by the Final Technical Specification document titled “Annex II ToR_Annex II Technical specifications”

3.1.2 Overview of the findings

Most of the components we managed to review were working effectively and efficiently. However, we have identified that the provided documentation may benefit from several amends, as well as it would be favourable for the general understanding of the requirements, to elaborate a document describing the exact User Stories that should be implemented by the NEPPs.

The architecture of the MTender procurement platform is well documented and described by 5.1*. ARCHITECTURE CENTRAL UNIT OPEN OCDS UNCITRAL DIGITAL PROCUREMENT* document. It covers all the eProcurement processes and modules and reflects the development product well, however, there is no clear linkage between the functional business requirements described by the technical specifications document and the de facto implemented functionality.

The guideline on documentation for NEPPs maintenance (APIs documentation and workflow description) is well documented by 5.3*. TECHNICAL DOCUMENTATION MTender Networking Multi-Platform Digital Procurement System* document.

3.1.3 Audit Findings

3.1.3.1 Missing architecture / functionality documents versioning

Description:
Architecture / functionality changes during the development are not easily traceable within the technical specifications and terms of reference documents, which may lead in the accumulation of technical debt, which, consequently, may result in technical bottlenecks and/or inconsistencies.

Recommendations:
The API documentation (*5.3. TECHNICAL DOCUMENTATION MTender Networking Multi-Platform Digital Procurement System*) is currently hosted on Google Docs and the versioning is realised by the Google Docs functionality, however, it would be beneficial for the analysis of the decisions made during the development, to add a versioning table within the document with a commentary to the new version updated as well as the author of the update.

This shall ease the process of identification of the appropriate person that can describe the changes applied to the system as well as provide a better understanding of the risks and issues during the development, which, consequently, may lead to an easier identification of potential bottlenecks of future developments to the system, should there be any.

Comment from everis: As of 5th of February 2020, we are evolving documentation towards Online documentation using GitHub pages. Versioning will be easier this way and further traceability will be ensured.

3.1.3.2 The Business Processes are split between the CDU, the NEPPs and the eGovernment services

Description:
The business processes features are split between the MTender components that result in shared responsibility, which may effectively lead to a greater resource involvement in the occurrence of an issue and the identification of the source of the issue may become challenging.

Recommendations
This is inline with the technical specifications document and the implementation specifications document, however, it would be beneficial for the MTender quality to ensure formal requirements for a minimal set of testing that shall be performed on the NEPPs, additionally to the testing requirements for the CDU.

3.1.3.3 No clearly defined minimal set of User Stories per NEPP

Description:
The entire procurement process is not described from various roles perspective, which can result in missing or incomplete implementation of the feature requirements as well as untested features.

User features are implemented on the NEPPs side and are part of the NEPPs responsibility. This is one of the core MTender principles, as recalled in section *1.3 Principles of the IT system* of the EU technical specifications.

However, this leads to uncertainty in terms of CDU features provided to all the NEPPS as described by the *5.2. EBRD MTender Technical Specifications v16.0* and subsequently by the EU Technical Specifications documents, since the NEPPs may or may not implement features provided by CDU, such as *the validation of budget availability, using CPV code of planned procurements and local budgetary classification code of the state budget line* of the ePlanning module.

Recommendations:
The following recommendations are based on the audit findings and may already be covered by newer versions of the MTender system:

- Establish appropriate formal minimal set of user stories or feature requirements for the NEPPs integration on the CDU;
- Establish a process to review the implementation of the formal list of User Stories;
- Develop a policy for updating the NEPPs upon CDU upgrade with feature additions and/or changes to ensure the NEPPs are inline with the latest CDU upgrades.

3.2 Project implementation methodology assessment

3.2.1 Background & Methodology

An assessment has been carried out in order to understand project implementation methodology and identify any possible risks and shortcomings with regards to implementation strategy.

The following steps are conducted to deliver an independent and professional opinion in regards to effectiveness and adequacy of the project implementation of the information systems:

- Analysis: Collected and analysed project implementation documentation;
- Analysis: Discussed with key team members involved in the design and implementation of MTender;
- Evaluation: Reviewed project management methodology and associated processes;
- Reporting: Compiled assessments and proposed recommendations.

DISCLAIMER: The findings given in these sections are based on the information obtained during the discussions with key persons involved in project implementation. The auditors were unable to obtain access to project implementation tools to perform the following activities:

- Review project issue logs;
- Review developer project documentation generated during the implementation.

3.2.2 Overview of Audit findings

Overall, we were satisfied by the competence, quality and effectiveness of the project implementation team. We have found the project implementation methodology to be in line with the SDLC current best modern practices. MTender is correctly developed and follows the requirements. The problems identified are in the lack of communication between the customer specialists and the development team. However, if the customer is not deeply involved, the same problems will repeat in MTender evolution and in a new application.

While we are confident that the project has been implemented correctly and the deliverables are stable, we think that the overall project implementation approach would benefit from an improvement, as detailed in the findings below.

3.2.3 General implementation methodology

Our findings on Project implementation methodology were based on analysis on the processes and existing produced documentation.

The following has been assessed and found to be of an acceptable level:

- Technical implementation methodology is in line with the SDLC current best modern practices. The team uses the right practices to ensure transparency, quality and timely deployments;
- Processes used for planning, support, implementation and quality controls are mostly respected (for details - please see Change Controls and Quality Controls below);
- Project management support tools are resourceful and exhaustive functionality-wise. It appears that the tools are used correctly and the workflows implied are well thought;
- Development tools used by the implementation team are in line with current best modern practices;
- Separation of development, testing and production environments is respected.

3.2.3.1 Project owners are not being involved in acceptance of the features

Description:
We have identified that the stakeholders (project sponsors/owners) don't participate in the acceptance of implemented requirements directly, during the process of development.

Recommendations:
The general recommendation is that the stakeholders (project sponsors/owners) designate one or more resources representing their entities to be involved in the acceptance of features implemented by the system during the process of development, by timely approving implementing features as completed. This ensures that the acceptance is employed early and the scope is understood and controlled by the project owners at every stage of development. We suggest stakeholders to be involved in approving every feature as it is being implemented, or alternatively with each minor release or module implementation.

3.2.4 Project Governance

Our findings with regards to Project implementation Governance were based on analysis on the processes around MTender implementation. The following has been assessed and found to be of an acceptable level:

- Governance arrangements covering unified decision-making and joint authority for managing contacts with owners, stakeholders and third parties;
- The adoption of a disciplined life cycle governance that includes approval gates;
- Recording and communicating decisions made at approval gates;
- Establishing clearly defined roles and responsibilities for governance;
- Ensuring that business cases are supported by information that allows reliable decision-making.

However, we have identified possible shortcomings which we documented below:

3.2.4.1 Business Analysis and Architecture of the system is reliant on one key resource

Description:
From our understanding, it appears that the technical knowledge around the project internals is mainly held by the developer (uStudio), which is normal during the implementation phase. However, we have identified that the decisions with regards to requirements Business Analysis (BA) as well as Enterprise Architecture (EA) are made by a single person.

Recommendations:
An Architect's role is to translate business requirements into capabilities that can be cost-effectively implemented, predictably managed, and reliably controlled. BAs are primarily tasked with requirements generation and facilitation of communications with technical groups to make sure those requirements are reliably implemented. In this regard, while an EA has both feet firmly planted on both sides of the business-IT divide, the BA (even an IT BA) is weighted towards the business. Most organizations separate the roles of the BA and EA.

3.2.4.2 Change approval process requires improvement

Description:
We understood from the project history, that there were significant changes to the system requested by various important stakeholders. The developer confirmed that they found

solutions, implemented and documented the changes in their internal systems. However, we were unable to find confirmation of a clear change approval process with the involvement of project stakeholders, especially focused on scrutinising and accepting implemented solutions.

Recommendations:
The general best practices recommendations is to employ a change approval process that would ensure participation of all stakeholders in the process of approving the changes to live platforms.

3.2.5 Knowledge Management

Our findings on Knowledge management were based on analysis on the processes and existing produced documentation. The following has been assessed and found to be to an acceptable level:

- Tools being used to manage knowledge during project implementation;
- Mechanisms for finding external knowledge and making it relevant internally;
- Mechanisms around identification and extraction of key lessons from projects, programmes and portfolios, including contextual information;
- Maintenance of the knowledge repository to ensure it is up to date;
- Processes that ensure knowledge is used effectively.

3.2.5.1 Ownership of knowledge management and the systems that support it

Description:
It appears that Technical Knowledge Management is owned by the developer's implementation team only. We understand that stakeholders don't have access to developer's maintained Knowledge management systems.

Recommendations:
The general best practices recommendations are for the project owners to establish and maintain ownership of critical systems, including repositories, knowledge management and other types of information and artifact storage systems. This can be a joint effort between the developer and project owner.

3.2.5.2 Some of the technical knowledge management is in Russian

Description:
It appears that most of the documentation generated by the developer is in English, however some of the developer's technical knowledge appears Russian language. As this is the native language of the team, it can be normal to have internal documentation in the native language.

Recommendations:
To reduce the risk, when documentation is critical to the system our recommendation is to use a single language. We would recommend reviewing the internal documentation and deciding on the translation of the existing key documentation.

3.2.5.3 System operation and maintenance documentation is incomplete

Description:
The deployment documentation is available, detailing the full process of the deployment of the platform and associated services. We found the quality and completeness of the deployment documentation satisfactory, however we maintain our recommendation that additional

maintenance and system operations documentation may be needed.

Recommendations:
We recommend the following aspects to be added to the documentation.

- Description of logging outputs generated by each application/service so that issues can be detected and correctly escalated.
- Maintenance recommendations, including how to stop the system for maintenance, the order in which the services must be stopped or started, how to maintain essential services).
- Mitigation of most common operational issues (i.e. scaling essential services if required, how to restart services)
- Documentation on the process of patching and updating each application/service.
- Any other documentation / recommendations critical to system's operations and maintenance
- Please also see 3.6.4.2 for monitoring recommendations.

3.2.6 Project Release & Integration

The following has been assessed and found to be to an acceptable level:

- Software Release Process;
- Software Release Documentation;
- Software build process and use of Continuous Integration Techniques;
- Software Release Rollback procedures.

3.2.6.1 CDU release process to NEPPs, as well as communication and documentation around this requires improvement

Description:
We confirmed that with every update of the CDU, the development team liases directly with representatives of the NEPPs to communicate information about changes and updates. We are also satisfied that internal documentation with regards to releases is produced, however we would recommend improvements to the process due to its important nature. We understand that the main developer uses Slack and email to communicate any new releases to NEPPs. We also understand that some of the NEPPs may not implement the changes immediately due to internal resourcing.

Recommendations:
Since NEPPs are a very important component of the whole system, the release process, communication and documentation are vital for the NEPPs to be able to implement the changes.

As such, we recommend:

- All releases to be accompanied with full implementation documentation;
- All releases to be accompanied with additional documentation focusing on only what has changed from previous version, including a migration guide if necessary;
- All releases which change core functionality and to be announced in a timely manner to the NEPPs so that they can plan for the necessary resources to be available in time;
- Allow NEPPs enough time to implement changes required and communicate the deadline clearly;
- Set up an online repository for release documentation so that the NEPPs can consult the

changes from version to version without the need to search Slack or email messages.

3.2.6.2 CDU release rollback process to NEPPs depends on Devops availability

Description:
We confirmed in case of problems with one of the releases, there is a rollback process which the developer invokes, performed mainly by the Devops resources employed in the project by the developer.

Recommendations:
While this is normal, we would recommend automating the rollback processes so that the system can be rolled back with minimum human involvement. This will reduce the risk of resources not being available when a rollback is needed.

3.2.7 Quality Controls

The following has been assessed and found to be to an acceptable level:

- Technical quality control processes;
- Types of testing being performed by developer QA team has been found to be in sync SDLC and current best modern practices;
- Regression testing processes with every release;
- Separation of development, testing and production environments;
- Availability of CDU sandbox environments for integrating parties (NEPPs).

3.2.7.1 CDU User acceptance testing seems to be reliant on NEPPs

Description:
Our investigations show that, while extensive testing is being performed upfront, the developer relies on NEPPs as the final acceptance testing. This is a potential risk, since the acceptance testing performed by NEPPS may be voluntary, incomplete or may not happen at all.

Recommendations:
Our recommendation is to ensure Acceptance testing is performed with every release. Ideally Acceptance testing would be done externally by the actors under direct supervision by the stakeholders.

3.2.7.2 Controls for testing the application - Limited automation testing implemented

Description:
Our investigations confirmed that limited automation testing is being performed on CDU and NEPPs. Automated testing is highly effective in identifying issues during active development.

Recommendations:
Our recommendation is to increase the coverage of automated integration testing for both CDU and NEPPs, however this depends on the technical decision by the project leaders.

3.3 Review of business processes implemented in the system

3.3.1 Background & Methodology

The focus of the audit of the implemented business processes was to identify risks, recommendations and/or solutions with regards to missing or incomplete workflow implementations, missing or incomplete documentation as well outdated or undocumented changes to the initial specifications of the MTender system.

The following activities were conducted during the audit of the implemented business processes:

- Analysis: Collected and analysed MTender Architecture, Technical Specifications and Technical concept Terms of Reference documentation;
- Analysis: Analysed MTender BPMN workflows;
- Analysis: Discussed with key team members involved in the design and implementation of MTender;
- Analysis: Identified processes required to assess and test each workflow;
- Evaluation: Carried out testing and review of the business processes using the achizitii.md (NEPP) sandbox test platform;
- Reporting: Compiled assessments and proposed recommendations.

The MTender system shall provide the following business processes as described by the EBRD BPMNs document (*19.09.24 Moldova 52c PB*) for the 1st implementation stage:

- Registration in NEPPs;
    - EO Registration in NEPPs;
    - CA Registration in NEPPs;
    - CE Registration in NEPPs;
- EU GPA Procedure Open Tender;
- Request for price quotations. Simplified Open tender;
- Direct Award Contract / Negotiated procedure without publication;
- Contract online signing and registration for offline procedures;
- CA Procurement Plan with PINs.

The following BPMNs were provided in the BPMNs document, however, shall not be developed during the implementation of Phase 2 Pilot and are currently under development:

- EU GPA Procedure Restricted Tender;
- Micro value procedure based on Electronic Reverse Auction;

DISCLAIMER: The public procurement business workflows are described by the EBRD BPMNs document (*19.09.24 Moldova 52c PB*) and *Annex II ToR_Annex II Technical specifications*. The main workflows of the IT System explains the need for detailed BPMN. This confirms that processes required in the EU technical specifications are up-to-date.

These documents are deemed final and up-to-date at the time of the audit.

The architecture of the implemented system is described by 5.1*. ARCHITECTURE CENTRAL UNIT OPEN OCDS UNCITRAL DIGITAL PROCUREMENT* document, while the functional requirements have been described by the *5.2. EBRD MTender Technical Specifications v16.0* document and subsequently by the Final Technical Specification document titled “Annex II ToR_Annex II Technical specifications”.

The API functionality is described by 5.3*. TECHNICAL DOCUMENTATION MTender Networking Multi-*

Platform Digital Procurement System document. The API documentation is not completed yet.

During the audit, Atomate has discussed the implemented functionality with the CDU developer representatives as well as the NEPP representatives. Additionally, Atomate conducted high-level testing for the business processes on the achizitii.md NEPP sandbox environment using a provided test account.
Only high level business processes have been tested. The audit process did not involve thorough testing of each Business Process described by the EBRD BPMNs document.

3.3.2 Overview of Audit Findings

The audit discovered that not all the BPMNs described by the EBRD BPMNs document (*19.09.24 Moldova 52c PB*) were implemented or can be identified at the time of review.

The following BPMNs can be identified and tested using the achizitii.md NEPP sandbox environment:

- Registration in NEPPs;
  - EO Registration in NEPPs;
  - CE Registration in NEPPs;
- EU GPA Procedure Open Tender;
- Request for price quotations. Simplified Open tender;
- Micro value procedure based on Electronic Reverse Auction;
- Contract online signing and registration for offline procedures;
- CA Procurement Plan with PINs.

All the procurement processes implemented in MTender are in alignment with the EU technical specifications (although the entire range of procedures to be implemented in MTender are not covered through the current implementation). Additional procedures reflected here (registration, contact signing, procurement planning) are also reflected in the EU technical specifications are up-to-date.

The following BMPNs are, however, not found in the achizitii.md NEPP sandbox implementation:

- Registration in NEPPs;
  - CA Registration in NEPPs;

3.3.3 Audit Findings

3.3.3.1 Ambiguous CE, EO and CA registration procedure within the NEPPs, missing CA registration process

Description:
According to the EBRD BPMNs document (*19.09.24 Moldova 52c PB*), the Economic Operator (EO), Contracting Entity (CE) and Contracting Authority (CA) registration processes clearly differentiate at multiple workflow steps.

The *5.3. TECHNICAL DOCUMENTATION MTender Networking Multi-Platform Digital Procurement System* document describes the **4.1 Operating Entities: CAs and EOs** attributes as well as enframes these within the OCDS attributes. These are distinctly dissimilar since each legal entity has a specific dataset, therefore, the registration process for each of the legal entities shall collect discrete data about each of the entities, however, no mention of the Contracting Entity can be identified on the registration page or during the entity registration process.

In this regard, different NEPPs do provide a registration page that allows to specify various organisation data as per the OCDS, however, it is unclear whether the automated Treasury Register verification for the Contracting Authorities is in place.

Recommendations:
Develop and implement a CA, CE and EO registration process policy across all the NEPPs connected to the CDU, so that during the registration process it is clearly identifiable which legal entity completes the registration.

3.4 System security

This section reflects the results of the security audit. The evaluation was conducted to identify any possible security weaknesses and risks that could be potentially misused by possible attackers.

3.4.1 Background & Methodology

The following steps are conducted to deliver an independent and professional opinion in regards to effectiveness and adequacy of the project implementation of the information systems:

- Analysis: Identified the majority of security controls within the system;
- Analysis: Discussed with key team members involved in the design and implementation of MTender;
- Analysis: Discussed with key team members involved in ownership operations of MTender (CTIF & STISC);
- Evaluation: Reviewed project management methodology and associated processes;
- Reporting: Compiled assessments and proposed recommendations.

The majority of security controls were analysed following a standardised approach, and measures for their remediation were proposed.

DISCLAIMER: A detailed and thorough analysis of the system has been performed, however, due to circumstances outside of our control, we were unable to obtain a meeting with STISC yet.

3.4.2 Overview of Audit findings

The results of the assessed areas led to the impression that the basic mechanisms are quite robust from an application security perspective, but the security of MTender integration with NEPPs should be reviewed and improved. In addition to this, we could not confirm essential security procedures and checks with regards to MTender performed by STISC or CTIF, (i.e. penetration testing, DDoS protection or regular security checks).

Overall, we have found the MTender system to be in alignment with the section "*6.11. Requirements for the information security*" of the EU technical specifications.

The following list the most important findings identified and suggested remediation recommendations.

3.4.3 Security related to CDU and integrated Services

Our findings on CDU security implementation were based on analysis on the analysis of the system, supplied documentation and information obtained during meetings with representatives of uStudio, CTIF and other involved parties.

The following has been assessed and found to be of an acceptable level:

- Network and remote access of the IT system control;
- Shadow IT & External services;
- Cryptographic key management;
- System security risks relating to unauthorised access to systems and/or data;
- Incident Management and history of system's incidents to date.

The MTender system is in alignment with the section "*6.11. Requirements for the information security*" of the EU technical specifications.

3.4.3.1 Database data is not encrypted as required by the security requirements

Description:
MTender system non functional requirements state that "All data stored in various components of the system (including CDU & NEPPs) (i.e. servers, data storage, LDAP) must be encrypted." Based on our findings, there is no encryption of stored data in CDU and NEPPS.

EU Technical Specifications require database encryption. Nevertheless, under the open data principles of MTender, this requirement is not implemented.

Recommendations:
Note that excessive encryption may be an overkill in some situations and it may lead to performance degradation and unnecessary complications. When data is publicly accessible and can be downloaded from NEPPs easily, we see no reasons for it to be encrypted. However, using appropriate encryption measures will somewhat lessen the privacy impact and notification requirements should there be a breach. As such, we recommend encryption of sensitive system data (i.e. passwords, personal data, tax information, security keys etc).

Comment from Everis: The specifications have been changed upon this recommendation.

3.4.3.2 We could not confirm essential security procedures and checks around the production system

Description:
We could not confirm essential security procedures and checks with regards to MTender performed by STISC or CTIF. CTIF representatives confirmed that security procedures are STISC responsibility, but we could neither confirm this, nor see any security reports or papers with regards to CDU.
The developer confirmed that security testing is CTIF/STISC's responsibility.

Recommendations:
Our recommendations are to ensure that essential security procedures and checks are taking place by ensuring that MTender Operator.

3.4.3.3 Ownership of some of the domains lies with the developer

Description:
Some of the components used to monitor CDU rely on domain names registered on the developer (md.kibana.procurement.systems, portainer.procurement.systems)[3]. This has been confirmed by the developer of MTender - uStudio.

Recommendations:
We think that the domain names should not be reliant on the developer, but solely controlled by the owner of MTender. Our recommendation is to transfer the domains to the owner of MTender and additionally review all domains involved.

3.4.3.4 Some of the MTender monitoring tools are publicly accessible, although secured

[3] MTender System Documentation - https://ebrd.huddle.net/workspace/36712039/files/#/75622628

Description:
We have identified that some of the monitoring tools used by MTender are publicly accessible, although secured with access controls (ie. Kibana in ELK stack - http://md.kibana.eprocurement.systems/).

Recommendations:
Our recommendation is to review access controls and apply additional security constraints to disallow public access (such as IP Filtering).

3.4.3.5 MTender Development reliance on external services adds additional risks

Description:
Current development process requires access to external systems run by other companies, such as BItbucket (Atlassian), DockerHub (Docker). Some of these systems are critical to the project's continuity, and as such reliance on external systems adds additional risk associated with availability and security of the system. The external services used for the MTender platform are reliable and well-known, hence, the risk can be considered only a highlight rather than an issue that requires immediate actions.

Recommendation:
In order to minimise security risks, consider setting up a health monitor to check on the external services status and report to the operator in case of issues. Alternatively, consider moving away from external systems to local run servers controlled by MTender Operator.

3.4.4 Security related to NEPPs

Our security findings were based on analysis on the processes and existing produced documentation.

The following has been assessed and found to be of an acceptable level:

- Rules and Procedures regarding security policy for the NEPPs (Minimum security requirements for the MTender Operator in charge of the Central Database Unit and for the Networking Electronic Procurement Platforms (NEPPs)).

3.4.4.1 Missing NEPPs Security audits required for accreditation and security policies

Description:
We could not confirm whether security audits have been prepared by the NEPPs involved with MTender. The procedure of accreditation clearly states that such an audit is required[4] before the NEPP can be connected to CDU.

Recommendations:
While we understand there are still decisions to be taken by the parties involved in discussions around MTender, we think that without security compliance the system is at risk of being compromised and constitutes a security risk. Our recommendation is to enforce security compliance as defined in the document "Regulation on establishing operations of the MTender System", or discontinue access to production CDU to non-compliant NEPPs.

[4]As defined in the document "Regulation on establishing operations of the MTender System" (19-20), available here https://ebrd.huddle.net/workspace/36712039/files/#/73960165

3.4.4.2 MTender Operator testing of NEPPS

Description:
We could not confirm whether MTender Operator has conducted the testing of existing NEPPs. The procedure of accreditation clearly states that one is required[5].

Recommendations:
It is important to ensure that the functionality of the NEPPs compliance with the required use cases and conform to the corresponding level of accreditation. We recommend testing to take place.

3.4.4.3 Additional certification requirements for NEPPs and other involved parties may be considered

Description:
While security policies defined and applied to NEPPs are sensible and strong, they seem to focus on the context of activities, controls and operations around the MTender System. The NEPPs as organisations are not required to hold security related certifications company wide.

Recommendations:
Our recommendation would be to consider requiring ISO 27001:2013, ISO/IEC 27018:2014 organisation certification for NEPPs. This will ensure processes are in place to reduce information security risks, allowing NEPPs to be prepared and trained independently. The policy towards ISO 27001 certified companies can be simplified once they demonstrate effective security, reducing the need for repeat audits.

[5]As defined in the document "Regulation on establishing operations of the MTender System" (30), available here https://ebrd.huddle.net/workspace/36712039/files/#/73960165

3.5 Key interface efficiency and controls

3.5.1 Background & Methodology

The focus of the audit of the key interface efficiency and controls was to identify risks, recommendations and/or solutions with regards to potential data conversion or data integrity issues as well as identify and analyse controls in place.

The following activities were conducted during the audit of the implemented business processes:

- Analysis: Discussed with key team members involved in the design and implementation of MTender;
- Analysis: Discussed the implemented functionality with the NEPP representatives;
- Analysis: Identified external and internal data interfaces;
- Analysis: Identified the significant application components; the flow of transactions through the MTender system and gained an understanding of the application by reviewing MTender documentation and source code;
- Evaluation: Reviewed MTender system testing;
- Evaluation: Review system integrity risks relating to the incomplete, inaccurate, untimely, or unauthorised processing of data;
- Reporting: Compiled assessments and proposed recommendations.

MTender controls refer to the transactions and data relating to the application system, therefore, they are specific to each workflow described by the EBRD BPMNs document *(19.09.24 Moldova 52c PB)*.

The objectives of MTender controls are to ensure the completeness and accuracy of the records and the validity of the amends or entries made to them. MTender controls are controls over IPO (input, processing, output) functions and include methods for ensuring that:

- Only complete, accurate and valid data are entered and updated in an application system;
- Processing accomplishes the designed and correct task;
- The processing results meet expectations;
- Data is maintained.

DISCLAIMER: The public procurement business workflows are described by the EBRD BPMNs document (*19.09.24 Moldova 52c PB*). This document is deemed final and up-to-date at the time of the audit. The architecture of the implemented system is described by 5.1*. ARCHITECTURE CENTRAL UNIT OPEN OCDS UNCITRAL DIGITAL PROCUREMENT* document, while the functional requirements have been described by the *5.2. EBRD MTender Technical Specifications v16.0* documents. The API functionality is described by the *5.3. TECHNICAL DOCUMENTATION MTender Networking Multi-Platform Digital Procurement System* document. The API is still in progress, hence the final API functionality will be described later.

During the audit, Atomate has discussed the implemented functionality with the CDU developer representatives, the NEPPs' representatives, CTIF, Ministry of Finance and EBRD representatives.

3.5.2 Overview of Audit Findings

Processing controls within the MTender system should ensure that only valid data and program files are used, that processing is complete and accurate and that processed data has been written to the correct files.

There should be controls to detect the incomplete or inaccurate processing of input data. Application processes may perform further validation of transactions by checking data for duplication and consistency with other information held by other parts of the system.

Additionally, the MTender system should maintain a log of the transactions processed. The transaction and operation logs should contain sufficient information to identify the source of each transaction. Errors detected during processing should be brought to the attention of users. Unprocessed or unclear transactions shall be monitored and reported by a specific control. There should be procedures which allow identifying and reviewing all unclear transactions beyond a certain age.

The audit discovered that most of the controls are identifiable and cover the data input, processing and output, however, it cannot be confirmed that performance and load testing has been performed on the CDU to ensure that the non-functional requirements described by the *5.2. EBRD MTender Technical Specifications v16.0* documents and subsequently by the Final Technical Specification document titled "Annex II ToR_Annex II Technical specifications" are satisfied.

Additionally, the API documentation is not properly versioned, which makes it hard to trace changes to the system as well as identify the patches and fixes to the system during the development and the issues faced.

Furthermore, the operation and transactions logs are only accessible at the BPE and OperationService levels, while authorisation and authentication to them is obfuscated and neither the operator (CTIF), nor the NEPPs could confirm access to them. MLog integration is envisaged, however, not confirmed. It is highly suggested to provide clear and discrete access to the operation and transactions logs to the operator of the MTender system so that periodic monitoring and analysis is done based on the gathered logs.

3.5.3 Input Controls

The objective of Input control is to ensure that the procedures and controls reasonably guarantee that:

- The data received for processing are genuine, complete, not previously processed, accurate and properly authorised;
- Data are entered accurately and without duplication.

Input control is extremely important as the most important source of error or fraud in software systems is incorrect or fraudulent input. Controls over input are vital to the integrity of the system.

Weak input control may increase the risk of:

- Entry of unauthorised data;
- Data entered in to the application may be irrelevant;
- Incomplete data entry;
- Entry of duplicate/redundant data.

The data input controls of the MTender system are well covered by various services and validations, depending on the related procedure. Additionally, the API documentation provides detailed and comprehensive information about the object fields, keys, purpose, type, value and schema. The requirement is explained in Annex II ToR_Annex II Technical Specifications Requirements for the data validation mechanism.

The effective controls are described below and the corresponding service that validates the input data.

Control	Control objective
Canonical JSON scheme	● Accuracy of data input.
DTO (data transfer object) validation	● Completeness of data input. ● Assignment of data input duties (e.g. originating, entering and processing data and distributing output).
Component validation (varies depending on the component)	● Timeliness of data input.
System Chronograph validation	● Data input processing schedules.
AuthService control	● API calls key verification; ● Restriction of overrides and bypasses to supervisory personnel; ● Automatic recording and submission of overrides and bypasses to supervisors for analysis; ● Security checks for data entry endpoints; ● Passwords for entering business transactions through endpoints; ● Reports of unauthorised API use.
OperationService control	● Monitoring for overrides and bypasses; ● Automatic recording of transaction errors; ● Monitoring of rejected transactions for correcting and reentering them on a timely basis; ● Logs of transactions entered through the API endpoints.
BPE control	● Automatic recording of transaction errors; ● Monitoring of rejected transactions for correcting and reentering them on a timely basis; ● Logs of transactions entered through the API endpoints.
Documented API endpoint processes	● Written procedures for data input processes. **Note: API endpoints and processes are described by the *5.3. TECHNICAL DOCUMENTATION MTender Networking Multi-Platform Digital Procurement System* document. The API is still in development, hence, the document shall not be deemed final**
Error message handling	● Appropriate error messages for all data error conditions. **Note: certain error messages do not provide clear error description and/or are too technical to comprehend**

3.5.3.1 The API Documentation is not versioned

Description:
The public API is still being developed, therefore, the API document is continuously edited/updated but does not provide a clear way of identifying the latest deployment changes and/or updates. It effectively does not allow NEPPs to identify changes to the API prior to the deployment taking place, which may result in sandbox downtime that shall require immediate actions from the NEPPs representatives in order to ensure continuous functioning of the MTender system. API endpoints versioning, given the implemented CQRS architectural pattern of the public API, is not required, however the API documentation may benefit from adding release notes as well as dates and amends to the API document upon each minor deployment.

Recommendations:
Add API documentation versioning and update it correspondingly with each minor release. Ensure the involved parties are timely notified about the API amendments so that appropriate planning is done by all sides, e.g. the NEPPs shall prepare the resources for the updates integrations and/or verification.

Comment from everis: As of 5th of February 2020, we are evolving documentation towards Online documentation using GitHub pages. Versioning will be easier this way and further traceability will be ensured.

3.5.3.2 API Documentation is being edited while the CDU is developed and sometimes after the releasing onto pre-production sandbox environment

Description:
The public API is still being developed, therefore, the API document is continuously edited/updated and for certain endpoints and/or objects. It occurred that the API documentation was updated after the release onto the sandbox took place. This lead to NEPPs being non-functional for limited periods, however, this has directly affected the NEPPs sandbox environments and demanded immediate intervention by the NEPPs representatives.

Recommendations:
Set up a policy to update the API documentation with each incremental or minor update once the amendment decision has been taken. Set up a policy to retrieve approval from the appropriate stakeholders and notify NEPPs about the upcoming API updates with a formal periodicity.

3.5.3.3 Operation and transactions logs access is obscured

Description:
The MTender system operator (CTIF) could not confirm access to the operation and transactions logs. The logs are, however, generated, but currently only the developer (uStudio) could confirm access to them.

Recommendations:
Set up a discrete, restricted and clear access policy to the operation and transactions log. The system operator shall be responsible for system maintenance and shall unconditionally have access to all the operation logs in order to clarify, identify and mitigate any issues of the system (or notify the appropriate resolution team). The input logs review shall be done periodically to ensure no errors and/or erroneous data is saved on the CDU.

3.5.4 Processing controls

The objectives for processing controls are to ensure that:

- Transactions processing is accurate;
- Transactions processing is complete;
- Transactions are unique (i.e. no duplicates);
- All transactions are valid;
- The computer processes are auditable.

This objective is achieved by providing controls for:

- Adequately validating input and generated data;
- Processing correct files;
- Detecting and rejecting errors during processing and referring them back to the originators for re-processing;
- Proper transfer of data from one processing stage to another.

Weak process controls would lead to:

- Inaccurate processing of transactions leading to wrong or erroneous outputs/results;
- Some of the transactions being processed by the MTender System may remain incomplete;
- Unauthorised changes or amendments to the existing data;
- Absence of audit trail rendering, sometimes, the application unauditable.

The audit found that the processing controls are identifiable, however, not entirely documented and may require additional description.

A comprehensive list of processing controls shall be elaborated additionally to the given Sequence Diagrams defined in the *5.1. ARCHITECTURE CENTRAL UNIT OPEN OCDS UNCITRAL DIGITAL PROCUREMENT* document.

The following processing controls shall be documented and confirmed:

Control	Control objective
Audit trails and overrides	● Automated tracking of changes made to data, associating the change with a specific user and/or platform; ● Automated tracking and highlighting of overrides to normal processes.
Validation of new data	● Data sequence check; ● Data limit check; ● Data range check; ● Data validity check; ● Existence check (for ID validations); ● Data key verification; ● Data duplication check; ● Data logical relationship check.
Interface balancing	● Automated checking of data received from feeder systems (such as Treasury and eGov services); ● Automated checking that balances on both systems

	match, or if not, an exception report is generated and used.
Generic processing controls	● Input data completeness throughout processing; ● Abnormal termination or conditions; ● Correct and timely reentry of unfinished transactions; ● Concurrent update protection procedures; ● Error messages printed out for each error condition; ● Maintenance of API calls history files; ● Procedures ensuring that the right versions of modules are run; ● Procedures for controlling errors.

3.5.4.1 Processing controls need to be clearly defined

Description:
The MTender system documentation does not provide clear information as to the validation, balancing and tracking of the data processing activity. It is understood that the processing of data takes place in various system components, depending on the activity and separated to the appropriate module by the BPE, however, the described implemented business logic also incorporates processing controls, which, eventually, may be made available for manual verification and/or management.

Recommendations:
Clearly define all processing controls as follows:

- Audit trails and overrides;
- Validation of new data (also covered by the input controls);
- Interface balancing;
- Generic processing controls.

Document these and make them available to the NEPPs as well as the MTender system operator for review and management. Processing controls should be reviewed periodically to ensure the completeness, timeliness and sufficiency of the integrated controls. With future developments, it is recommended to develop a cabinet allowing administrators and operators to identify validation rules and formulate comprehensive requests with regards to amends to the system, if eventually required.

3.5.5 Output controls

Output controls ensure that all output is:

- Produced and distributed on time;
- Physically controlled at all times, depending on the confidentiality of the document;
- Errors and exceptions are properly investigated and acted upon.

Weak output controls would lead to:

- Repeated errors in the output generated leading to loss of data, loss of credibility of the system as well as that of the system owner;
- Non-availability of the data at a time when it is desired;
- Even sometimes, the information which may be of very confidential nature may go to the wrong hands.

The audit identified that the output controls are described and complemented by the *5.3. TECHNICAL DOCUMENTATION MTender Networking Multi-Platform Digital Procurement System* document, however, would highly benefit from additional clear description.

The following output controls shall be documented and confirmed:

Control	Control objective
Output controls	● Completeness of output; ● Timeliness of output; ● Logs for output production and delivery (covered by BPE and OperationService control logs, however, not accessible for confirmation); ● Clear output error messages; ● A history of output errors; ● Procedures for user responses made on the basis of output information.

3.5.5.1 Operation and transactions logs access is obscured

Description:
The MTender system operator (CTIF) could not confirm access to the operation and transactions logs. The logs are generated, but currently only the developer (uStudio) could confirm access to them.

Recommendations:
Set up a discrete, restricted and clear access policy to the operation and transactions log. The system operator shall be responsible for system maintenance and shall have access to all the operation logs in order to clarify, identify and mitigate any issues of the system (or notify the appropriate resolution team). The output logs review shall be done periodically to ensure no errors and/or erroneous data is transitioned to the NEPPs.

3.5.5.2 Output controls need to be clearly defined

Description:
The MTender system documentation does not provide a clear definition to the logging level, content, timing and triggers.

Processing of data for different business processes takes place in various modules, which may result in propagation of erroneous data through different tendering activities, thus, a single logging mechanism and location shall be applied for all the system components in order to avoid lengthy investigation for issue identification.

Recommendations:
Clearly define all output controls and implement a unified logging system. Formally describe the logging level and structure in order to easily browse through the logs during analysis and/or investigation.

3.5.6 Public API key efficiency

The purpose of the public API efficiency and effectiveness are to ensure that:

- No data is lost during the normal operation of the MTender system;
- No data is lost during the peak times of the MTender system operation;
- No data is altered or corrupted during the normal operation of the MTender system due to downgraded system performance;
- No data is altered or corrupted during the peak times of the MTender system operation due to degraded system performance;
- All system users are able to use the system simultaneously without delays in response times and/or timeouts to their requests, regardless of the reason and nature of the load that the MTender system experiences (minimal required indicators are described below, listed as non-functional requirements in the *5.2. EBRD MTender Technical Specifications v16.0* document).

Non-functional requirement	Requirement indicator
Concurrent requests minimal required performance	● up to 5 system administrators; ● up to 1.000 active users; ● up to 5 members for each single user cabinet; ● up to 25,000 read-only users of the general public.
Data storage requirements	● up to 5,000 contracting authorities; ● up to 40,000 registered bidders.
Response times requirements (not exceeding)	● 1 second for the execution of 90% of simple queries; ● 3 seconds for the execution of 99% of simple queries; ● 3 seconds for the execution of 90% of complex queries; ● 10 seconds for the execution of 99% of complex queries; ● 3 seconds for the generation of 90% of reports; ● 10 seconds for the generation of 99% of reports; ● 3 seconds for the execution of 90% of document management activities; ● 10 seconds for the execution of 99% of document management activities.

Key efficiency objective is achieved by selecting the right approach and architecture for the public API as well as by securing the following criteria:

- Ensure the public API is vertically scalable;
- Ensure the MTender components (modules) are horizontally scalable;
- Estimate the data flow by performing load and performance testing of the system with various volumes of data and simulated procedure scripts;
- Ensure no redundancy takes place at all levels of the operation of the MTender system;
- Maintain full records to:
    - Trace any transaction items;
    - Provide a full audit trail;
    - Provide a full record of all transactions;
- Evaluate the actual bandwidth and resource usage for each of the modules and adapt the resourcing appropriately.

The defined architecture of the MTender system envisages high load on reading information and less load on writing data to the database, hence the decision to develop it using the CQRS principle for the public API, which, subsequently, provides a segregation of the read/write procedures, is entirely justified.

Additionally, the selected technology stack complements the required modularity of the online electronic public procurement, which shall allow for granular adaptation to the region requirements as well as provide an easier maintenance of the system by separating the responsibilities based on the MTender system components.

3.5.6.1 Performance and load testing has not been done

Description:
Neither a performance testing report nor a load testing report have been provided or uploaded onto the Huddle workspace for review. It cannot be confirmed that the system is able to hold the required number of concurrent requests and meet the response times requirements, described by the *5.2. EBRD MTender Technical Specifications v16.0* document.

Recommendations:
Run performance and load testing upon the release of each minor version onto pre-production environment and patch weak efficiency endpoints, if any are identified.

More importantly, performance and load testing is usually done before the system becomes available to the public as it uncovers what needs to be improved. Without performance testing, software is likely to suffer from issues such as:

- Running slow while several users use it simultaneously;
- Inconsistencies across different operating systems;
- Poor usability.

During the piloting, the MTender system would have not been used to the maximum and did not reach peak load conditions, endurance load conditions, therefore, it is highly important to do performance and load testing before releasing a major version to the public and it is suggested to run it testing with each minor update deploy.

3.6 Continuous monitoring

This section reflects the results of the continuous monitoring audit. The evaluation was conducted to identify any possible risks with regards to the system's potential problems arising from its operation, as well as ensuring adequate maintenance, incident management and disaster recovery procedures.

3.6.1 Background & Methodology

The following steps were conducted to deliver an independent and professional opinion in regards to continuous monitoring of MTender System:

- Identified ongoing MTender maintenance process
- Identify system maintainability risks relating to the inability to update the system when required in a manner that continues to provide for system availability, security, and integrity
- Assessment of risks regarding system availability and lack of systems operational capability.
- Assessment of Disaster Recovery and Business Continuity
- Review Configuration management
- Review incident management and history of system's incidents to date
- Reporting: Compile and propose assessment and recommendations

DISCLAIMER: A detailed and thorough analysis of the system has been performed, however, due to circumstances outside of our control, we were unable to obtain information from one of the key organisations involved in operation of the MTender - STISC.

3.6.2 Overview of Audit findings

Overall, the audit identified serious shortcomings with regards to incomplete maintenance and operations documentation, as well as MTender's Operator knowledge and capability to take ownership of the system. The audit was not also able to confirm that full Disaster Recovery processes are in place.

The following list the most important findings identified and suggested remediation recommendations.

3.6.3 System Maintenance and Operations

The following has been assessed and found to be of an acceptable level:

- Technical maintenance process & system maintainability;
- The level of documentation available regarding system maintenance and operations.

3.6.3.1 System operation and maintenance documentation is incomplete

Description:
The deployment documentation is available, detailing the full process of the deployment of the platform and associated services. We found the quality and completeness of the deployment documentation satisfactory, however we maintain our recommendation that additional maintenance and system operations documentation may be needed.

Recommendations:
We recommend the following aspects to be added to the documentation.

- Description of logging outputs generated by each application/service so that issues can be detected and correctly escalated.

- Maintenance recommendations, including how to stop the system for maintenance, the order in which the services must be stopped or started, how to maintain essential services).
- Mitigation of most common operational issues (i.e. scaling essential services if required, how to restart services)
- Documentation on the process of patching and updating each application/service.
- Any other documentation / recommendations critical to system's operations and maintenance
- Please also see 3.6.4.2 for monitoring recommendations.

3.6.3.2 MTender Operator lacks system knowledge and capability

Description:
During our meetings MTender Operator (CTIF) confirmed that the operation team lacks MTender System knowledge. They confirmed that partial training received and knowledge has been transferred, however, they don't think this is sufficient. As a result, operators are only able to manage basic operations of the system, but are not able to apply changes.

Recommendations:
Our recommendation would be to ensure CTIF/STISC have trained resources in place to take full ownership of the MTender System.

3.6.3.3 MTender Operator lacks understanding the operational requirements of the system

Description:
In addition to the findings above, the MTender Operator (CTIF) confirmed that they don't have the information regarding minimum, optimal and maximum operational requirements of the system (i.e. number of recommended servers required for Production, bandwidth, disk space, computing required etc).

Recommendations:
Our recommendation would be to ensure CTIF obtains this information. From the project documentation, we could not identify such information as well.

3.6.4 Monitoring & Scalability

The following has been assessed and found to be of an acceptable level:

- Monitoring capability and suitability of tools used to monitor and scale the MTender system;
- The level of documentation available with regards to monitoring and scalability;
- The high level processes designed by the developer to ensure the system is robust and scalable.

3.6.4.1 Monitor NEPPS availability and functionality independently

Description:

It is our understanding that MTender Operator will rely on NEPPs to communicate their availability figures[6]. While this is nevertheless a good way to ensure NEPPs take availability and reliability seriously, we think additional monitoring will benefit the system, and ultimately its users.

Recommendations:

Our recommendation is to set up NEPPs monitoring independently to obtain uptime figures directly to avoid relying on NEPPs to communicate failures. This will ensure MTender Operator is aware of any downtimes and can decide pro-actively to liaise with the NEPP and resolve the problems.

3.6.4.2 System monitoring documentation and scalability/performance recommendations

Description:

In order to ensure that the MTender Operator is fully capable of performing monitoring and scalability operations, we recommend compiling additional documentation and guidelines in this regard. Some of the monitoring and scalability duties would be normally tackled by the team tasked to operate the system (e.g. load monitoring, essential maintenance, security,), however, our opinion is that the development team should normally supply information on systems operation so that the Development Operations team (devops) is knowledgeable and is able to take good care of the the system.

Recommendations:

Our recommendation is that additional monitoring and scalability documentation is needed, detailing the following:

- Guidance for monitoring of services for quality, performance and capacity
- Guidance for monitoring of system's integration with external services
- Guidance for disaster recovery strategy
- Description of logging outputs generated by each application/service so that issues can be detected and correctly escalated.
- Recommendations with regard to system's security monitoring & checks (SSL certificates, intrusion detection etc)

[6] As defined in the document "Regulation on establishing operations of the MTender System", available here https://ebrd.huddle.net/workspace/36712039/files/#/73960165

3.6.5 Business Continuity, Disaster Recovery and Incidents Management

3.6.5.1 CDU Disaster Recovery process is unconfirmed

Description:
We could not get a confirmation from CDU or STISC that some of the Disaster Recovery processes are put in place (e.g. Data and restoration) and are being monitored correspondingly. However, as the system is hosted in MCloud we believe Disaster Recovery has been at least partially addressed by the MTender Operator. As the system is essentially in Production, we think this is a major issue which needs to be addressed urgently.

The requirement is explained in Annex II ToR_Annex II Technical Specifications requirements for resilience and continuity.

Recommendations:
Our recommendation is to ensure a full Disaster Recovery Plan is available and enabled by the MTender Operator.

3.6.5.2 Most incidents are currently dealt with and advised on by the developer

Description:
We confirmed that there is an incident management process in place, however, based on the history of the incidents, we can confirm that most infrastructure, operational and quality related incidents have been dealt with and advised by the developer of the MTender System (UStudio).

Recommendations:
Our recommendation is to ensure that the MTender Operator takes ownership of the incident management process to reduce reliance on the developer.

4. Alignment of MTender with EU Technical specifications

The review of MTender System alignment with EU Technical specifications highlighted that there are important differences detailed below:

4.1. There is no Test NEPP:

One of the main MTender system's principles focuses on establishing a distributed system between the government and the private sector, as a leverage to gain further benefits. Implementing a test NEPP that can be eventually put in production by the government would confront these principles and pose a great risk in the MTender model.

4.2. Open data and transparency principle

The MTender system is based on open data and transparency principles that assure that all procurement information shall be disclosed and no encryption of the procurement database is implemented, following international best practices.

5. Conclusions

Our investigations revealed that the system is mostly inline with the technical requirements and implements the business processes as per the documented models. Some BPMNs are missing, but we understand that the system is still in development and have been assured that outstanding BPMNs are planned to be implemented further.

The internal, processing and output controls in place are sufficient to ensure completeness and accuracy of the records and the validity of the amends or entries made to them during the usage of the MTender workflows. Efficiency of the MTender system shall be verified by running appropriate testing.

The audit of project implementation methodology found the project to be in line with the SDLC current best modern practices. While we are confident that the project has been implemented correctly and the deliverables are stable, we think that the overall project implementation approach would benefit from an improvement, as detailed in the report's findings.

The audit of key efficiency and controls has revealed that the system has not been load and stress tested. Thorough load and stress testing is highly recommended.

The audit of security aspects has confirmed that the basic mechanisms are quite robust, but the security of MTender integration with NEPPs should be reviewed and improved. In addition to this, we could not confirm essential security procedures and checks with regards to MTender performed by STISC or CTIF, (i.e. penetration testing, DDoS protection or regular security checks).

The audit of continuous monitoring also reveals that while some of the continuous monitoring aspects seem to have been addressed, there are shortcomings with regards to maintenance and operations documentation, and subsequent MTender's Operator knowledge and capability to undertake ownership and maintenance of the system. The lack of documentation and understanding of the deployment process has been addressed by a separate workshop (see 2.4 - Deployment Exercise / Workshop), focused on detailing the deployment of the system to a quasi-production environment, which has been completed successfully.

The review of MTender System alignment with EU Technical specifications highlighted that there are a few important differences, however these are conceptual which arise from the main principles of the system: open data and transparency principle and the principle of establishing a distributed system between the government and the private sector, as a leverage to gain further benefits.

Overall, our opinion is that the system is technically and functionally competent, it is designed to be secure, scalable and stable, the project methodology used is mostly suitable. The functional and non-functional requirements are mostly respected and the BPMNs work as expected. The operational issues around the system are mainly based on lack of knowledge, capacity and training of the MTender Operator and the lack of completion of the accreditation process of NEPPs.

5. Contact Sheet

You can get in touch with us in any of the below ways:

By phone:

Office in the Republic of Moldova:
20 Puskin street
MD-2005 Chisinau
Republic of Moldova
Phone/Fax: +373 (0) 22 229500
Contact: Andrei Lopatenco

Office In UK:
Ravensbourne, 6 Penrose Way
Greenwich Peninsula
London SE10 0EW
Phone: +44 (0) 20 8090 0828
Contact: Vitalie Chiperi

By email

- Send all enquiries to: info@atomate.net
- Contact form also available on our website: https://www.atomate.net