Grant Thornton

e-Government Agency (AGE) – Security testing and audit services

Our Approach

Comments on the Terms of Reference

Understanding the Goal and Specific Objectives

Before going to the presentation of our methodology and implementation strategy, we would like to address some key issues and introduce our considerations, as well as assumptions that will allow us to better cover and align our proposal to the Terms of Reference (TOR).

As per our understanding, the assignment represents a strategic initiative by the e-Government Agency (AGE) of Moldova to strengthen the security posture of its expanding digital ecosystem. At its core, the objective is to procure specialized cybersecurity testing and audit services that go beyond traditional assessments, ensuring that critical platforms such as EVO Integrated Government Electronic Services, EVO-Sign for mobile identity and signature, and e-KYC for remote identification meet the highest standards of security, confidentiality, integrity, and availability. These platforms are not merely technical solutions; they are transformative instruments redefining citizen-state interaction, and their security is fundamental to sustaining public trust and operational resilience.

The specific objectives of the required services are multifaceted. They include the identification and exhaustive documentation of vulnerabilities across application, infrastructure, and source code layers; controlled simulation of real-world attack scenarios through penetration testing; and verification of compliance with international standards such as OWASP, ISO/IEC, NIST, and e-IDAS. Additionally, the engagement aims to provide actionable remediation recommendations, validate the effectiveness of corrective measures through follow-up testing, and integrate findings into AGE's bug-tracking systems to ensure full lifecycle management of security issues. These objectives collectively reflect a proactive approach to cybersecurity, emphasizing both preventive and corrective measures.

Having the carefully read the TOR, we believe that the purpose of this engagement is comprehensive: to identify vulnerabilities across application, infrastructure, and source code layers; to simulate real-world attack scenarios through penetration testing; and to validate compliance with international standards and best practices. This dual approach—offensive and defensive—ensures that AGE's systems are not only tested for weaknesses but also benchmarked against globally recognized frameworks such as OWASP, ISO/IEC, NIST, and e-IDAS. The assignment further emphasizes actionable remediation, follow-up validation, and integration with AGE's bug-tracking systems, creating a full lifecycle of security assurance rather than a one-time exercise.

Context and Its Strategic Importance

The context of this assignment is shaped by two converging dynamics: the rapid expansion of Moldova's digital public services and the escalating sophistication of cyber threats. AGE is launching next-generation platforms that handle sensitive identity credentials, authentication tokens, and biometric data, elements that are highly attractive to malicious actors. These systems introduce complex attack surfaces, including mobile applications, APIs, and biometric verification workflows, which demand advanced security validation techniques beyond conventional vulnerability scanning.

Equally critical is the regulatory dimension. Compliance with European frameworks such as e-IDAS and emerging standards for digital identity wallets is essential for interoperability and trust at the regional level. Failure to achieve compliance could isolate Moldova's digital services from broader European initiatives, limiting scalability and undermining credibility. Thus, this

assignment is not merely technical; it is a strategic imperative that underpins national digital governance, citizen trust, and Moldova's integration into the European digital ecosystem.

General Assumptions and Key Considerations

It is assumed that AGE's systems are operational or in advanced stages of development, requiring testing in environments that closely replicate production conditions. Full cooperation from AGE's technical and business teams is essential, including timely access to documentation, source code, and test environments. The provider is expected to adhere to strict confidentiality protocols and ethical guidelines, ensuring that testing activities do not disrupt live services or compromise sensitive data.

Key considerations include the diversity of technologies within AGE's ecosystem, necessitating a multi-framework approach that combines OWASP guidelines for web and mobile applications, ISO/IEC standards for information security and biometric systems, and NIST methodologies for structured testing. The methodology must be adaptive, covering web, mobile, and backend components, while addressing unique risks such as presentation attacks, replay exploits, and biometric link bypass scenarios in e-KYC workflows. Lifecycle security is another critical consideration: vulnerabilities must not only be identified but also remediated and validated through follow-up testing, with all findings integrated into AGE's bug-tracking systems for traceability and accountability.

Methodology and Technical Approach

The technical approach is structured and aligned with international best practices. It begins with a planning phase that defines scope, objectives, and engagement rules, followed by an evaluation phase involving vulnerability scanning, penetration testing, and compliance audits. Testing will cover critical areas such as secure deployment, authentication, access control, cryptographic security, API integrity, and business logic validation. For biometric systems, specialized tests will assess presentation attack resistance, liveness detection, and lifecycle security of biometric data. The final phase focuses on analysis, reporting, and follow-up testing to confirm remediation effectiveness. This structured methodology ensures not only comprehensive coverage but also knowledge transfer to AGE's teams, reinforcing long-term security resilience.

Deliverables and Reporting Framework

Deliverables are designed to provide clarity and actionable insights at both executive and technical levels. Reports will include concise executive summaries for decision-makers and detailed technical documentation for development and security teams. Each vulnerability will be classified using CVSS v4.0, accompanied by proof-of-concept evidence and prioritized remediation recommendations. Compliance audits will feature graphical summaries and detailed matrices mapping each requirement to its compliance status. Integration with AGE's bug-tracking system ensures that vulnerabilities are tracked from discovery to closure, creating a transparent and accountable remediation process.

The importance of this assignment extends beyond technical compliance. In an era where digital trust equates to national resilience, securing e-government platforms is a foundational requirement for sustainable digital transformation. By investing in structured security testing and audits, AGE demonstrates proactive governance, safeguards citizen data, and positions Moldova as a credible participant in regional digital initiatives. The outcomes of this engagement will not only mitigate immediate risks but also embed a culture of continuous security assurance, enabling Moldova to navigate the complexities of an interconnected digital future with confidence.

Particularities, Risks, and Sensitivity of Systems

The systems under consideration present unique characteristics and heightened sensitivity. EVO, as an integrated platform for electronic government services, aggregates multiple functionalities and data flows, making it a high-value target for attackers seeking systemic disruption. EVO-Sign introduces cryptographic mechanisms for mobile identity and digital signatures, where any compromise could invalidate trust in electronic transactions and legal documents. The e-KYC platform, handling biometric data and remote identity verification, is particularly sensitive due to the irreversible nature of biometric identifiers and the complexity of mitigating risks such as presentation attacks, replay exploits, and deep-fake-based fraud.

These particularities amplify the risks associated with the project. A successful attack on any of these systems could lead to identity theft, large-scale fraud, or even systemic failure of public services. Furthermore, the regulatory implications are

significant: non-compliance with e-IDAS and related European standards could jeopardize Moldova's interoperability within the EU digital ecosystem, undermining strategic objectives for regional integration.

General Vision for Achieving Objectives

The vision for achieving these objectives is grounded in a structured, standards-driven methodology that combines offensive and defensive security practices. The approach begins with a rigorous planning phase, defining scope, engagement rules, and compliance benchmarks. This is followed by comprehensive evaluation activities, including vulnerability scanning, penetration testing under multiple scenarios (black-box, gray-box, white-box), and security audits aligned with international frameworks. Specialized testing for biometric systems will address presentation attack resistance, liveness detection, and lifecycle security of biometric data.

The process culminates in detailed reporting and knowledge transfer, ensuring that AGE's technical and management teams fully understand the risks and recommended mitigations. Integration with AGE's bug-tracking systems will enable continuous monitoring and accountability, transforming security assurance from a one-time exercise into an ongoing governance practice. This vision emphasizes collaboration, transparency, and adaptability, ensuring that security measures evolve alongside technological advancements and emerging threats.

Main Challenges in the Project Context

Several challenges are anticipated in the execution of this assignment. First, the complexity and diversity of AGE's digital ecosystem require a multi-framework approach, demanding expertise across web, mobile, and biometric security domains. Second, the sensitivity of the data involved—particularly biometric identifiers—necessitates stringent confidentiality measures and ethical handling throughout the testing process. Third, the dynamic nature of cyber threats means that testing methodologies must remain agile, incorporating threat intelligence and evolving attack patterns. Finally, achieving compliance with European standards while maintaining operational continuity poses a delicate balance between regulatory rigor and practical feasibility.

Addressing these challenges will require not only technical proficiency but also strategic foresight, ensuring that the engagement delivers sustainable security outcomes that reinforce Moldova's digital transformation agenda.

Frameworks

The complexity and sensitivity of Moldova's eGovernment platforms - EVO, EVO-Sign, and e-KYC, - demand a security testing and audit approach grounded in internationally recognized frameworks. These frameworks provide structured methodologies, standardized practices, and proven techniques to ensure comprehensive coverage of vulnerabilities and compliance requirements. Their selection is not arbitrary; it reflects the need for rigor, interoperability, and adaptability in a rapidly evolving threat landscape.

For the purpose of this Project, we will use the set of internationally accepted standards in the area of cybersecurity, ICT governance, ICT assurance, and Information Security, such as:

- ISO/IEC 25010,
- ISO/IEC 27001,
- ISO/IEC 27005,
- NIST CSF 2.0,
- NIST SP 800-15,
- OWASP,
- eIDAS and EUDI Wallet Framework,
- MITRE ATT&CK Framework,
- Etc.

ISO/IEC 25000 Series (SQuaRE)

The ISO/IEC 25000 series, known as Systems and Software Quality Requirements and Evaluation (SQuaRE), is designed to establish a comprehensive framework for assessing software quality. Unlike purely security-focused standards, SQuaRE addresses multiple quality characteristics, including functionality, performance efficiency, compatibility, usability, reliability, maintainability, and security. For this assignment, its relevance lies in the ability to evaluate security as a quality attribute within a broader context of system robustness and user trust.

The primary advantage of ISO/IEC 25000 is its holistic perspective. By embedding security within the broader quality model, it ensures that AGE's platforms are not only secure but also reliable, user-friendly, and maintainable. This is particularly critical for systems like EVO and EVO-Sign, which must deliver seamless user experiences while maintaining stringent security controls. For e-KYC, where biometric verification introduces complex workflows, SQuaRE helps validate that security mechanisms do not compromise usability or system performance. Its importance in this project stems from the need to balance technical security with operational excellence, ensuring that digital services remain accessible and trustworthy.

OWASP Frameworks

The Open Web Application Security Project (OWASP) offers a suite of guidelines and standards tailored for web and mobile application security. For this assignment, OWASP's Web Security Testing Guide (WSTG) and Mobile Application Security Verification Standard (MASVS) are indispensable. WSTG provides a systematic approach to identifying vulnerabilities in web applications, covering areas such as input validation, authentication, and session management. MASVS, complemented by the Mobile Application Security Testing Guide (MASTG), ensures that mobile applications like EVO-Sign meet stringent security requirements, addressing risks such as insecure storage, weak cryptography, and improper platform usage.

The advantage of OWASP lies in its practical orientation and global acceptance. It offers clear testing methodologies, vulnerability taxonomies, and remediation strategies, making it highly relevant for platforms that handle sensitive identity and authentication data. Its importance in this context stems from the fact that EVO and EVO-Sign are user-facing applications, where flaws in logic or configuration could lead to large-scale exploitation.

ISO/IEC Standards

ISO/IEC frameworks provide a governance-oriented perspective, ensuring that security practices are embedded within organizational processes. ISO/IEC 27001 and 27002 establish the foundation for information security management systems, while ISO/IEC 27005 focuses on risk management. For biometric systems like e-KYC, ISO/IEC 30107 is critical, as it defines standards for presentation attack detection and biometric data protection.

The advantage of ISO/IEC standards lies in their holistic approach, combining technical controls with governance, risk management, and compliance. They are essential for ensuring that AGE's security posture aligns with international best practices and regulatory expectations. Their importance is amplified by the sensitivity of biometric data, which requires lifecycle security—from capture and storage to transmission and deletion.

NIST SP 800-115

The National Institute of Standards and Technology (NIST) provides a technical guide for security testing through SP 800-115, which outlines best practices for planning, executing, and documenting security assessments. This framework is particularly valuable for structuring penetration testing activities, ensuring consistency and repeatability across different systems and environments.

The advantage of NIST SP 800-115 lies in its clarity and adaptability. It offers detailed guidance on test execution, reporting, and risk analysis, making it ideal for complex ecosystems like EVO and EVO-Sign, where multiple components and integration points must be evaluated. Its importance in this project is tied to the need for a disciplined, evidence-based approach to vulnerability identification and exploitation.

eIDAS and EUDI Wallet Framework

Compliance with the eIDAS regulation and emerging European standards for the EUDI Wallet is non-negotiable for platforms handling digital identity and trust services. These frameworks define requirements for interoperability, trust assurance, and secure identity management across the EU. For EVO-Sign and EVO, adherence to these standards ensures that Moldova's digital services remain compatible with regional initiatives, reinforcing both technical and legal trust.

The advantage of these frameworks lies in their regulatory authority and their role in enabling cross-border digital services. Their importance cannot be overstated: failure to comply could isolate Moldova's platforms from European ecosystems, undermining strategic objectives for digital integration.

Other Supporting Frameworks

Additional methodologies such as MITRE ATT&CK**,** CIS Benchmarks, and PTES (Penetration Testing Execution Standard) provide specialized guidance for threat modeling, system hardening, and structured penetration testing. These frameworks enhance the depth and precision of security assessments, ensuring that testing activities reflect real-world attack scenarios and industry best practices.

The selection of these frameworks is not merely a technical choice; it is a strategic decision that underpins the credibility and resilience of Moldova's eGovernment ecosystem. Each framework addresses a distinct dimension of security—application-level vulnerabilities, governance and compliance, technical rigor, and regulatory alignment. Together, they form a comprehensive security assurance architecture that mitigates risks, safeguards sensitive data, and reinforces public trust in digital services.

Approach

Our methodology and approach are the subject to the following assumptions:

- All stages in the work plan are executed with no delays from AGE's Information technology and information Security departments/units,
- "Prepared by client" supporting documents are provided as requested and in a timely manner by AGE's Information Technology and Information Security Department/Unit,
- Timely delivery of final report is subject to timely input and feedback from the project stakeholders assigned by AGE,
- Grant Thornton ('GT') will not make management decisions and / or sign-off on behalf AGE, as well as GT will not provide any legal advice to AGE,
- The implementation of the gaps identified and highlighted in the risk analysis reports, IT security audit reports, as well as in penetration testing reports, if any, will be the sole responsibility of AGE,
- Our scope of services in this proposal is limited to the requirements defined in the TOR. Should the AGE require Grant Thornton to perform additional services outside the defined scope of work, this will be discussed and formally agreed upon with the AGE,
- As part of the pre-defined scope of work and during the assignment, Grant Thornton will not perform any system (software or hardware) modification.
-

For successfully implementation of the assignment (in terms of TOR for immediate response) we believe that cooperation and collaboration with AGE IT and Information Security teams is the main success principles that will allow us to achieve the required results and provide best services based on our experience, knowledge, and skills. At the stage of planning and scoping we are expecting to have a couple of meetings with the key stakeholders and establish an exact list of counterparts and our work relations with them including meetings, required data, etc. From our part we establish a team with the clear distribution of scope of work and tasks assigned to each of the team members.

Quality control and risk management

Quality control

As a member of Grant Thornton International, we are committed to providing professional services that conform to the highest quality and ethical standards, as prescribed by the CREST (https://www.crest-approved.org/), International Federation of Accountants (IFAC) independence standards, and the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA). As part of our commitment, we have established rigorous processes for relationship checking and client acceptance, which ensure compliance of services we provide with all applicable local and international regulatory requirements, as well as applicable industry standards. Achieving professional excellence means accepting and retaining clients that share Grant Thornton's values of quality and integrity. The Advisory Assignment Acceptance and Consultation Policy is designed to identify and assess those advisory assignments that could present significant risk to GTIL and its member firms, or where additional professional resources from across Grant Thornton's network might be required to ensure quality and excellence of the work, we do for you. This policy applies to assignments for prospective and existing clients that meet one or more of the defined criteria, for which consultation with GTI and prior approval is required.

During execution of the Project, we will conduct a quality control that is mandatory part of our corporate standard. Grant Thornton's review of the work conducted under the security testing and audit services of the eGovernment Agency's systems/products services is an integral part of applying due professional care. Before issuing the final report and considering the feedback from the various stakeholders from the Client and other stakeholders, we will review all prepared final documents and detailed working papers in terms of the Grant Thornton internal quality control policy. Responsibility for an engagement extends to every person who contributes to the final result; however, the Engagement Partner is fully accountable for the engagement. Reviewers for attestation engagements such as this consultancy services are conducted by the Global Audit Coordinator, the Global LTA project manager, and the Global Project Administrator. These will review the draft and final reports to determine if they conform to professional standards and Grant Thornton's policies and procedures, signing off only after being satisfied that all comments developed during this review were addressed, appropriate revisions made to the working papers, engagement documentation completed and that it is appropriate for Grant Thornton to issue the report. In addition, the Engagement Partner will ensure that both Grant Thornton's quality control standards and the engagement objectives of project are met

Independence and Risk

Internationally accepted ethical standards require that professional accountants in public practice be independent and avoid any conflict of interest that could impair their independence and impartiality. Prior to execution of our contract, we shall perform an Independence Relationship Check (IRC) throughout the Grant Thornton network, determining any past or current relationships between Grant Thornton member firms and entities within the corporate structure of the potential client. Through this check we ensure that our member firms do not currently provide or have not in the past provided services to the potential client or its related entities, which could potentially create significant conflicts of interest, posing a threat to our independence as professional public accountants. We will work with you early on in the contract execution process, to obtain required information regarding the corporate structure and to perform the IRC swiftly (within the timeframe of 4 business days after we receive the required information), thus eliminating any potential compliance issues and saving your valuable time in establishing a collaboration with our firm.

In addition, as prescribed by GTIL's client acceptance procedures, as well as the Global Advisory Assignment Acceptance and Consultation Policy, we shall perform certain background checks to exclude any other factors that may affect our ability to deliver services with professional excellence.

Achieving professional excellence means accepting and retaining clients that share Grant Thornton's values of quality and integrity. The Advisory Assignment Acceptance and Consultation Policy is designed to identify and assess those advisory assignments that could present significant risk to GTIL and its member firms, or where additional professional resources from across Grant Thornton's network might be required to ensure quality and excellence of the work, we do for you. This policy

applies to assignments for prospective and existing clients that meet one or more of the defined criteria, for which consultation with GTI and prior approval is required.

We shall inform you additionally if the proposed services require a GTIL clearance procedure and will execute the proposed advisory services only upon competition of the above-described procedures, given that they have not revealed any threat to our independence or other factors that may preclude us from undertaking the engagement.

Risk management

The key to a successful engagement is the thoughtful planning and management. However, despite careful development, all projects carry some level of risk. Furthermore, the unique risks of each project can make it challenging to transfer lessons learned from one milestone to the next. We believe that a continuous risk management process is one way to respond to unexpected project risks.

It is important to understand common risk management processes and risk mitigation strategies so that can drive successful project outcomes. The risk management process helps plan for and anticipate risks, while mitigation strategies offer tools to deal with them if they do happen. The risk management process, or lifecycle, is a structured way of tackling risks that can happen in particular project.

In order to manage the engagement risk and make sure that its goals and outputs are achieved, we will use the comprehensive approach to manage the risk life cycle during the implementation of engagement.

- Identify risks.
  - The first step to getting an information on potential risks is to know what they are. They can be logistics issues, availability of required staff, access to the systems, etc.
- Analyze potential risk impact
  - In the risk analysis stage, we explore the probability of each risk occurring, as well as the potential impact each risk will have on the engagement. The list of the identified risks will be putting in a risk register that is a chart that lays out each risk, followed by information like priority level and mitigation plans.
- Assign priority to risks
  - In this stage, we assign priority to risks by using the probability and impact of each risk to determine their risk levels. This means assigning each risk a high, medium, or low priority based on the factors you've determined. Evaluating the risks gives the GT team the chance to see where to focus their energy in mitigating risk
- Mitigate risks
  - Come up with a plan to mitigate each risk and record these plans in the risk register. The four most common ways to mitigate risks include avoiding, accepting, reducing, and transferring. Deciding which approach to use for each risk isn't an exact science, and we have to use our judgment and expertise to determine which is best.

It should be noted that all identified risks will be communicated to AGE team to update on the situation and agreed on the possible strategies of how to solve and mitigate the identified issues. The Engagement Partner will be constantly in touch with the AGE team on this and other important aspects of this Project.

Methodology

Project management

For the purpose of assignment implementation, Grant Thornton will execute its Project Management framework. The framework leverages the best practices of program management, project management, and performance management offered by traditional management disciplines, and integrates them to deliver a seamless, pragmatic approach to achieving project success. This set of processes and tools is based on widely accepted principles, such as those described within the Projects

IN Controlled Environments (PRINCE2) and PMI's PMBOK® Guide, Standard for Portfolio Management, and Organizational Project Management Maturity Model. Our methodology also comprises the best of what we have learned delivering projects in a timely, cost effective and predictable manner, and executing programs/projects in a practical, global, constructive and collegial fashion using an agile repeatable framework. This framework uses PRINCE2 components, process, and techniques, and is augmented from PMBOK® Guide and the Grant Thornton best practices process and techniques.

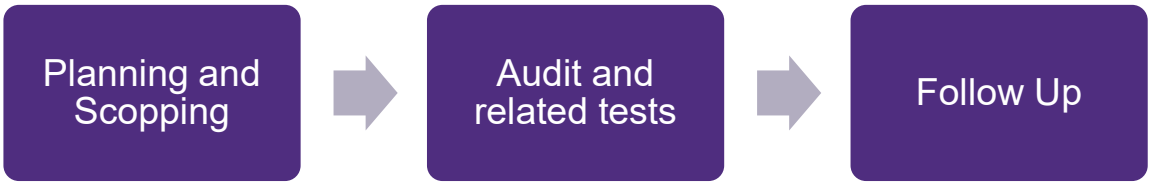
Based on our analysis of the audit objectives, related audit scope, and set of deliverables along with milestones set forth in the TOR, we suggest having the following project management principles applied for achievement of the audit objectives:

1. Keep it simple and practical. This includes developing a clear vision and structure for the audit and consistent use of simple tools and techniques that are easily understood by all stakeholders of the engagement.

2. Strong stakeholder engagement and communication. The engagement has multiple stakeholders, and it is therefore critical that we ensure full stakeholder engagement and ensure good communication over the whole project management cycle.

3. Strong project management. The assignment has several key deliverables that are interconnected with subsequent phases of the engagement. It is therefore particularly important for this engagement that we maintain firm control of time, cost and quality and actively manage the engagement risks.

The following engagement approach will be as follows:



In particular, the activities presented below will be performed under each of the engagement phases.

Before beginning any audit assignment, the security testing and audit services of the eGovernment Agency's systems/products should be planned in a manner appropriate for meeting the assurance objectives. The plan will act as a framework for the audit engagement and serve to address the audit objectives.

As part of the planning process, we will obtain a good understanding of the IT and application environment and the organization's approach to managing and execute instant payment solution to meet audit objectives. To execute the audit engagement according to a standardized and structured approach, we will identify appropriate control frameworks that could be useful for this audit.

We believe that implementing the tasks mentioned in TOR will be more effective and efficient if the detailed project plan, as well as audit program are prepared and agreed with AGE prior to commencement of the main activities.

Technical approach

The technical approach for this assignment is designed to ensure comprehensive security assurance for the eGovernment Agency's critical platforms: EVO, EVO-Sign, and e-KYC, through a structured methodology aligned with international best practices. This approach integrates offensive and defensive techniques, rigorous compliance checks, and specialized testing for biometric systems, ensuring that vulnerabilities are not only identified but also remediated and validated. The methodology combines globally recognized frameworks such as OWASP, NIST SP 800-115, ISO/IEC standards, eIDAS, and ISO/IEC 30107, applied in a manner tailored to the unique characteristics of each system.

Application of Standards and Frameworks

For EVO, which serves as an integrated platform for electronic services, the OWASP Web Security Testing Guide (WSTG) will be applied to evaluate web application security across critical areas such as input validation, session management, and authentication. Testing will include manual verification of OWASP Top 10 vulnerabilities, complemented by automated scanning tools. For EVO-Sign, the OWASP Mobile Application Security Verification Standard (MASVS) and Mobile Application Security Testing Guide (MASTG) will guide assessments of mobile-specific risks, including insecure storage and cryptographic weaknesses. Both platforms will also be evaluated against NIST SP 800-115 for structured penetration testing and ISO/IEC 27001 for governance alignment.

For e-KYC, compliance with ISO/IEC 30107 is paramount to validate biometric presentation attack detection mechanisms. Tests will simulate 2D and 3D spoofing attempts, deepfake-based attacks, and replay exploits, ensuring that liveness detection and biometric matching processes are resilient. Additionally, e-KYC workflows will be assessed for lifecycle security, covering data capture, transmission, storage, and deletion, in line with ISO/IEC 27002 and privacy principles.

Approach for Each Service Type

1 **Vulnerability Testing:**

The process begins with automated scanning using industry-leading tools such as Nessus, Nexpose, and NMAP, complemented by manual verification to eliminate false positives and uncover logic flaws. Vulnerability testing will target misconfigurations, outdated components, and insecure coding practices, ensuring exhaustive coverage of application and infrastructure layers.

Vulnerability testing will serve as the foundation for identifying weaknesses across application, infrastructure, and configuration layers. The process begins with automated scanning using industry-leading tools such as Nessus and Nexpose, complemented by open-source solutions like Nmap for network-level assessments. These tools will be configured to detect common vulnerabilities, misconfigurations, and outdated components, following the OWASP Web Security Testing Guide (WSTG) for EVO and MASVS for EVO-Sign.

However, automated scanning alone is insufficient for systems of this complexity. Manual verification will be conducted to eliminate false positives and uncover logic flaws that automated tools cannot detect. This includes testing for improper session handling, insecure API endpoints, and privilege escalation paths. For e-KYC, vulnerability testing will extend to biometric workflows, ensuring that data capture and transmission mechanisms are hardened against interception and replay attacks. The outcome will be a comprehensive vulnerability map, classified by severity using CVSS v4.0, forming the basis for subsequent penetration testing

2 **Penetration Testing (Black Box, Gray Box, White Box)**

Penetration testing will follow the NIST SP 800-115 methodology, structured into phases of information gathering, enumeration, exploitation, and post-exploitation. Black Box testing will simulate external attacks without prior knowledge, Gray Box will leverage limited authenticated access, and White Box will involve full source code review and architectural analysis. Techniques will include network mapping, API fuzzing, privilege escalation attempts, and exploitation of business logic flaws, ensuring realistic attack scenarios.

Penetration testing will simulate real-world attack scenarios to validate the resilience of AGE's platforms under adversarial conditions. The methodology will follow NIST SP 800-115, structured into phases of reconnaissance, enumeration, exploitation, and post-exploitation.

- Black Box Testing will replicate external attacks without prior knowledge, focusing on publicly exposed interfaces, APIs, and authentication mechanisms.
- Gray Box Testing will leverage limited authenticated access, simulating insider threats or compromised user accounts to test privilege escalation and lateral movement.
- White Box Testing will involve full access to source code and architectural documentation, enabling deep analysis of logic flaws, cryptographic implementations, and integration points.

The penetration testing exercise is a security exercise using ethical hackers rather than automated processes or real-world hackers who attempt to damage and/or compromise the corporate's information systems. Penetration testing attempts to exploit weaknesses or vulnerabilities in systems, networks, human resources, or physical assets in order to stress test the effectiveness of security controls. A penetration test involves a team of security professionals who actively attempt to break into your company's network by exploiting weaknesses and vulnerabilities in the corporate systems.

To ensure a successful penetration test, there are several activities and processes to be considered beyond the testing itself. This section provides high level methodology for these activities and is organized by the typical phases that occur during a penetration test:

- Pre-engagement,
- Engagement,
- Post-engagement.

Pre-engagement

The objective of this activity is to establish a risk management framework that keeps AGE up to date with our progress and helps both parties to manage the associated risks effectively. Specifically, we would seek to clearly identify what is and isn't being tested, communicate points of contact within the client and Grant Thornton and schedule activities to minimize the risk to the business which includes:

- Scoping,
- Rules of Engagement,
- Success Criteria.

This phase also included establishing an emergency point of contact and escalation paths to inform of any critical high-risk vulnerability that have discovered immediately or to report problems associated with testing e.g., a system going down unexpectedly. The outcome of pre-engagement phase was the signed Rules of Engagement (RoE) with AGE. The penetration testing scope is the agreed definition of what will be tested (and what, explicitly will not) and how those items will be tested.

A penetration testing is an activity in which a test team (Grant Thornton team) attempts to circumvent the security processes and controls of a computer system(s). Posing as either internal or external unauthorized intruders, the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the target system components in unauthorized ways if it had happened outside the scope of the test. Due to the sensitive nature of the penetration testing, specific rules of engagement are necessary to ensure that testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results.

To clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact, the Rules of Engagement (RoE) will be signed between the parties. The purpose of the Rules of Engagement (RoE) is to layout the procedures and establish the rules of engagement for when penetration testing is performed against the AGE's selected system components. As per TOR, the following tests will be performed:

- tests carried out from the external network of the AGE,
- tests carried out from the internal network of the AGE,
- vulnerability assessments,
- Operational resilience tests:
  - simulations on the volume of transactions,
  - simulations of system failures and their recovery,

– simulation of DoS/DDoS attacks.

Prior to commencing the penetration testing engagement, we shall confirm the scope and targets, note any changes and ensure all relevant staff are aware of the process through remote video conferences with the assigned technical staff.

It should be noted that penetration test is not an uncoordinated attempt to access an unauthorized resource. The penetration testing activities should be coordinated and scheduled with AGE staff. At a minimum, some of the requested penetration tests will log alerts in an Intrusion Detection System. Additionally, some tests have the ability to cause an outage of network equipment or systems. For that reason, Company management and staff awareness is required in most cases. Information about the penetration attempts may be found in the targeted systems' logs or on IDS that should be described in RoE document and provided to AGE prior to the penetration test commencing. Steps that will be taken after tester detects a previous or active compromise to systems being tested will be described in incident handling section of RoE document. Classes of issues will be raised with the AGE within which timeframes and the format within which the issues should be raised should be described in incident handling section of RoE document.

One of the most important aspects of penetration test is communication with the customer. How often you interact with the customer, and the manner in which you approach them, can make a huge difference in their feeling of satisfaction. Below is a communication guidelines that will aid in making the AGE feel comfortable about the test activities.

– Any kind communication to other AGE personnel who are not directly involved in test and relates to test data is prohibited, except those will be directly assigned by AGE,
– All Communication related to particular test or test data with Grant Thornton team will be performed electronically, with internal communication methods that support data encryption in transit (e.g. Corporate Email system),
– All points of contact for the Grant Thornton team, appropriate AGE personnel, and the incident response team should be identified and documented in RoE. If applicable, security clearances or comparable background check details should also be provided,
– Details for schedule of testing, hours during which the testing will take place and information such as critical tests and milestones will be described in RoE document,
– Criteria for halting the information security testing should be provided, as should details on the Grant Thornton test team's course of action in the event that a test procedure negatively impacts the network or an adversary attacks the Company while testing is underway,
– AGE's incident response call tree/chain of command should be provided in a quick-reference format,
– A process for reinstating the test team and resuming testing should also be provided in RoE document,
– RoE document will include Information about authorized and unauthorized IP addresses or other distinguishing identifiers, if appropriate, for the system components, and any applications to be tested.

Engagement: Penetration Testing

The time and effort that need to put in for the systems that have vulnerabilities need to be estimated accordingly. After doing the necessary planning and preparation with AGE, the next step is to gather as much information as possible about the targeted systems or system components including any known vulnerabilities. After determining the vulnerabilities that exist in the systems, the next stage is to identify suitable targets for a penetration attempt.

In terms of the attack vectors, the following approached will be used:

– External Testing – targeted at externally visible servers/devices of instant payment solution (e.g. DNS, e-mail, web servers, routers etc.),
– Internal testing - targeted at internally visible servers/devices of instant payment solution,
– Operational resilience tests:

- simulations on the volume of transactions,
- simulations of system failures and their recovery,
- simulation of DoS/DDoS attacks.

During an penetration test the team of pen testers will be given some information regarding the publicly available resources of instant payment system in terms of external penetration testing and some information available internally. The main benefit of this method of testing is to simulate a real-world cyber-attack, whereby the team of pen testers assume the role of an uninformed attacker in and our of AGE premises. For the purpose of internal penetration testing, the secure connection (IPSEC) will be established with AGE's isolated internal network to simulate attack considering that potential attacker has already entered into AGE internal perimeter.

The purpose of the internal and external assessment is to verify the security of the external/internal perimeter and publicly available services of the instant payment system. Tests will reveal if there is a possibility of developing an attack on the available resources.

It should be noted that OSINT (Open-Source Intelligence Gathering) tactics will be employed to extract pertinent information available through sources such as job postings, employee social media profiles, and affiliated third-party associations. Once intelligence was collected, it was used to create a penetration testing tactics for this engagement.

The external/internal attack will be initiated to evaluate AGE perimeter defenses, potential attack vectors, and protection of external-facing assets as well as internal-facing assets. The test will be involved a comprehensive assessment of the external and internal attack surface, including external/internal network infrastructure, web applications, and any publicly accessible services. The primary objectives were to identify potential attack vectors, vulnerabilities, potential entry points, and assess the overall resilience of the instant payment solution's security posture.

All web services and applications will be assessed in accordance with OWASP Testing Guide V4.2 and include following topics:

- Injection,
- Broken Authentication and Session Management,
- Cross-Site Scripting (XSS),
- Broken Access Control,
- Security Misconfiguration,
- Sensitive Data Exposure,
- Insufficient Attack Protection,
- Cross-Site Request Forgery (CSRF),
- Using Components with Known Vulnerabilities,
- Under protected APIs.

We will perform various scanning, enumeration, and attack activities to identify possible weak areas of implementation or application/service itself. By assessing web applications and services for OWASP domains we have performed following OWASP tests.

In terms of infrastructure components, the following testing will be performed:

- **Configuration and Deployment Management Testing**
  - Test Network/Infrastructure Configuration (OTG-CONFIG-001)
  - Test Application Platform Configuration (OTG-CONFIG-002)

  - Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003)
  - Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004)
  - Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005)
  - Test HTTP Methods (OTG-CONFIG-006)
  - Test HTTP Strict Transport Security (OTG-CONFIG-007)
  - Test RIA cross domain policy (OTG-CONFIG-008)
- **Identity Management testing**
  - Test Role Definitions (OTG-IDENT-001)
  - Test User Registration Process (OTG-IDENT-002)
  - Test Account Provisioning Process (OTG-IDENT-003)
  - Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004)
  - Testing for Weak or unenforced username policy (OTG-IDENT-005)
- **Authentication Testing**
  - Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)
  - Testing for default credentials (OTG-AUTHN-002)
  - Testing for Weak lock out mechanism (OTG-AUTHN-003)
  - Testing for bypassing authentication schema (OTG-AUTHN-004)
  - Test remember password functionality (OTG-AUTHN-005)
  - Testing for Browser cache weakness (OTG-AUTHN-006)
  - Testing for Weak password policy (OTG-AUTHN-007)
  - Testing for Weak security question/answer (OTG-AUTHN-008)
  - Testing for weak password change or reset functionalities (OTG-AUTHN-009)
  - Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)
- **Authorization Testing**
  - Testing Directory traversal/file include (OTG-AUTHZ-001)
  - Testing for bypassing authorization schema (OTG-AUTHZ-002)
  - Testing for Privilege Escalation (OTG-AUTHZ-003)
  - Testing for Insecure Direct Object References (OTG-AUTHZ-004)
- **Session Management Testing**
  - Testing for Bypassing Session Management Schema (OTG-SESS-001)
  - Testing for Cookies attributes (OTG-SESS-002)
  - Testing for Session Fixation (OTG-SESS-003)
  - Testing for Exposed Session Variables (OTG-SESS-004)
  - Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)
  - Testing for logout functionality (OTG-SESS-006)

  - Test Session Timeout (OTG-SESS-007)
  - Testing for Session puzzling (OTG-SESS-008)
- **Input Validation Testing**
  - Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)
  - Testing for Stored Cross Site Scripting (OTG-INPVAL-002)
  - Testing for HTTP Verb Tampering (OTG-INPVAL-003)
  - Testing for HTTP Parameter pollution (OTG-INPVAL-004)
- **Testing for SQL Injection (OTG-INPVAL-005)**
  - Oracle Testing
  - MySQL Testing
  - SQL Server Testing
  - Testing PostgreSQL (from OWASP BSP)
  - MS Access Testing
  - Testing for NoSQL injection
  - Testing for LDAP Injection (OTG-INPVAL-006)
  - Testing for ORM Injection (OTG-INPVAL-007)
  - Testing for XML Injection (OTG-INPVAL-008)
  - Testing for SSI Injection (OTG-INPVAL-009)
  - Testing for XPath Injection (OTG-INPVAL-010)
  - IMAP/SMTP Injection (OTG-INPVAL-011)
  - Testing for Code Injection (OTG-INPVAL-012)
  - Testing for Local File Inclusion
  - Testing for Remote File Inclusion
  - Testing for Command Injection (OTG-INPVAL-013)
  - Testing for Buffer overflow (OTG-INPVAL-014)
  - Testing for Heap overflow
  - Testing for Stack overflow
  - Testing for Format string
  - Testing for incubated vulnerabilities (OTG-INPVAL-015)
  - Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016
- **Testing for Error Handling**
  - Analysis of Error Codes (OTG-ERR-001)
  - Analysis of Stack Traces (OTG-ERR-002)
- **Testing for Weak Cryptography**
  - Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001)

- Testing for Padding Oracle (OTG-CRYPST-002)
- Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)

One main advantage of a white box penetration test is that the reporting provides a more focused and efficient assessment of the AGE security posture of selected applications and system components.

In terms operational resilience test, it should be noted that it will be executed within the internal penetration testing engagement.

Post-engagement

After the engagement or testing has been performed, there are activities both parties should carry out.

- Cleaning up the environment,
  - It is important for the tester to document and disclose to AGE any alterations made to the environment (as permitted in the Rules of Engagement) during the test, including but not limited to:
    (1) Accounts that were created as a part of the assessment either by the entity or the tester: the Grant Thornton will then remove these accounts.
    (2) Tools installed by the tester on the AGE's systems (if any): these tools should be removed at the end of the testing.

Removal of accounts and test tools will ensure the accounts or remnant tools could not be exploited or used against AGE.

3 **Security Code Review:**

Static Application Security Testing (SAST) will be performed using tools SonarQube, combined with manual code inspection to identify vulnerabilities that automated tools may miss. The review will focus on insecure coding patterns, improper input validation, and cryptographic implementation flaws, ensuring alignment with OWASP secure coding practices.

Security code review will combine Static Application Security Testing (SAST) with manual inspection to identify vulnerabilities at the source code level. Automated tool SonarQube will be employed to scan for insecure coding patterns, improper input validation, and cryptographic weaknesses. Manual review will complement these tools, focusing on business logic errors, hardcoded credentials, and API security flaws that automated scans often overlook.

For EVO and EVO-Sign, code review will ensure compliance with OWASP secure coding practices, while for e-KYC, special attention will be given to biometric data handling routines, encryption mechanisms, and error-handling logic. This dual approach guarantees both breadth and depth, ensuring that vulnerabilities are detected before they can be exploited.

4 **Security Audit (GAP Assessment):**

The security audit will benchmark AGE's platforms against internationally recognized standards, including eIDAS for trust services, OWASP MASVS for mobile security, and ISO/IEC 30107 for biometric integrity. The audit process will involve detailed configuration reviews, architectural analysis, and compliance mapping, producing a matrix that clearly indicates conformity, partial compliance, or non-compliance for each requirement.

For EVO and EVO-Sign, audits will validate adherence to eIDAS requirements for identity assurance and interoperability, while for e-KYC, compliance with ISO/IEC 30107 will confirm the robustness of presentation attack detection mechanisms. The audit will also incorporate CIS Benchmarks for system hardening and MITRE ATT&CK for threat modeling, ensuring that AGE's platforms are aligned with best practices for resilience against advanced threats.

Specific Approach for e-KYC

The e-KYC platform demands specialized testing due to its reliance on biometric verification and sensitive identity data. Presentation attack detection (PAD) will be assessed using high-resolution photo attacks, 3D mask simulations, and deepfake videos to challenge liveness detection mechanisms. Replay attack scenarios will test session integrity, while document forgery tests will evaluate the system's ability to detect digitally altered identity documents. Biometric bypass attempts will simulate fraudulent enrollment processes using mismatched identity and biometric data, ensuring strict linkage between document and biometric verification.

Summary

This technical approach is comprehensive, combining automated and manual techniques, offensive and defensive strategies, and compliance-driven audits. By leveraging globally recognized frameworks and adapting them to the unique characteristics of EVO, EVO-Sign, and e-KYC, the methodology ensures that vulnerabilities are identified, risks are mitigated, and compliance is achieved without compromising operational continuity. The integration of follow-up testing and bug-tracking ensures accountability and lifecycle security, transforming this engagement into a cornerstone of Moldova's digital resilience.

Project Plan

Effective project management is critical to maintaining control and transparency. Communication with AGE will be governed by a structured protocol, including weekly progress updates and immediate escalation for critical vulnerabilities. In compliance with ToR requirements, any vulnerability classified as Critical will trigger a notification within 24 hours, accompanied by preliminary mitigation guidance.

Risk management procedures will address potential service interruptions during testing. All activities will be scheduled during predefined maintenance windows, and fallback mechanisms will be established to prevent operational disruptions. Quality assurance will be enforced through peer reviews of all deliverables, adherence to standardized templates, and validation against international frameworks before submission.

The successful execution of this assignment requires a structured and disciplined project plan that ensures clarity of objectives, efficient resource allocation, and adherence to international best practices. The plan is organized into three main stages:

1 Planning & Pre-Evaluation,

2 Evaluation & Testing,

3 Analysis & Reporting.

Each of the stages include defined activities, deliverables, and management mechanisms to guarantee quality and timely completion.

Stage I: Planning & Pre-Evaluation

This initial stage establishes the foundation for all subsequent activities. Its primary objective is to define the scope, engagement rules, and methodologies for testing and auditing. Activities will include a formal kick-off meeting with AGE stakeholders to align expectations, confirm objectives, and identify technical and business points of contact. A detailed scoping exercise will follow, mapping all systems within the perimeter: EVO, EVO-Sign, and e-KYC, and determining the depth of testing required for each.

Resources allocated to this stage will include a project manager, responsible for coordination and communication, and lead security consultants, tasked with developing the Test and Audit Plan (Scope of Work). This plan will outline methodologies based on OWASP WSTG/MASVS, NIST SP 800-115, ISO/IEC 30107, and eIDAS compliance requirements. The deliverable for this stage will be a comprehensive Project Plan and Test & Audit Plan, approved by AGE, ensuring that all stakeholders have a clear roadmap before execution begins.

Key Activities

- Organization kick-off with all parties Involved,
- Clear definition a Perimeter (scoping) and Objectives,
- Setting rules of commitment, including of the periods of time for testing and Procedures of Escalation,
- Defining Scenarios Testing and/or Standards that will be used for each of the three Systems,
- Identification of persons of contact technical and Business,
- Obtaining permits Required Writings for Conduct Tests.

Key Deliverables

- Project Plan,
- Test and Audit Plan (Scope of Work – SoW), including scenarios, methodologies and tools), approved by the EGM.

Projected timeline (duration)

Up to 2 (two) weeks.

Stage II: Evaluation & Testing

The second stage represents the core of the engagement, where practical security assessments are conducted. Activities will include vulnerability scanning using automated tools such as Nessus, Burp Suite, and OWASP ZAP, complemented by manual verification to identify logic flaws and eliminate false positives. Penetration testing will follow, structured under NIST SP 800-115 guidelines, and executed in three modes: Black Box, simulating external attacks; Gray Box, leveraging limited authenticated access; and White Box, involving full source code review and architectural analysis.

Security code review will be performed using SonarQube, combined with manual inspection for business logic vulnerabilities. For e-KYC, specialized tests will validate biometric security, including presentation attack detection (PAD), lifecycle security of biometric data, and bypass scenarios. Resources for this stage will include penetration testers, code review specialists, and biometric security experts, supported by a dedicated quality assurance lead to monitor adherence to standards.

Key Activities

Minimum test areas of security testing should cover without being limited to, following areas:

- Configuration and management of the secure deployment,
- Identification and authentication management,
- Access control,
- Validation of input data,
- Error and log management,
- Cryptographic security,
- Testing business logic,
- Customer-level security,
- API testing,
- other areas, according to the established test framework.

In case of the security audit (GAP Assessment), the activity will consist of systematically checking the security controls of the application against the reference standard established at the planning stage. For each requirement of the standard, the architecture, configuration and, where necessary, the source code will be analyzed to determine the degree of compliance.

Key Deliverables

- Interim progress reports (on request), real-time notifications (within 24 hours) for vulnerabilities with Critical severity.

Projected timeline (duration)

Up to 7 (six) weeks.

Stage III: Analysis & Reporting

The final stage focuses on consolidating findings, validating remediation efforts, and transferring knowledge to AGE teams. Activities will include classification of vulnerabilities using CVSS v4.0, development of detailed technical reports, and preparation of executive summaries for decision-makers. Follow-up testing will be conducted after remediation to confirm closure of vulnerabilities. Reports will be structured to provide clarity at both strategic and technical levels, including compliance matrices for audits against eIDAS, MASVS, and ISO/IEC 30107.

Resources allocated to this stage will include reporting specialists, responsible for drafting comprehensive documentation, and technical leads, who will validate findings and provide clarifications during presentation sessions. Integration with AGE's bug-tracking system will ensure traceability and accountability throughout the remediation lifecycle.

Key Activities

- Analyze Referencing and validation of all results obtained,
- Classification of vulnerabilities Identified using a standardized system (CVSS v4.0),
- Development of detailed report,
- Presentation of the results to the Technical Teams and AGE Management,
- Granting Support and Clarifications for a full understanding of the risks and Fix.

Follow-up testing

After the development team of the AGE its suppliers Implements measures remediation, we will perform a follow-up test to validate the correctness and their effectiveness and to confirm closing vulnerabilities.

Key Deliverables

- Test and analysis reports with detailed recommendations,
- Presentation of the results to the Technical Teams and AGE Management,
- Follow-up reports.

Projected timeline (duration)

Up to 3 (three) weeks.

The proposed project plan combines structured methodology, clear communication protocols, and robust risk management to deliver a comprehensive security assurance program. By aligning with international standards and integrating lifecycle security practices, the plan not only addresses immediate vulnerabilities but also establishes a foundation for continuous improvement, reinforcing Moldova's digital resilience.

Implementation Schedule

The implementation schedule will span approximately 12 weeks, distributed across the three stages:

1 Weeks 1–3: Planning & Pre-Evaluation, including kick-off, scoping, and approval of the Test & Audit Plan.

2 Weeks 4–9: Evaluation & Testing, covering vulnerability assessments, penetration testing, code reviews, and biometric-specific tests for e-KYC.

3 Weeks 10–12: Analysis & Reporting, including preparation of final reports, executive summaries, presentations, and follow-up testing.

This timeline ensures that all systems, such as EVO, EVO-Sign, and e-KYC, are assessed thoroughly without compromising operational continuity.