Terms of Reference for an International Cybersecurity Expert
Improving Equitable Access to High Standard Public Services through GovTech in Albania

July 2024

1. BACKGROUND

Over the past 15 years the Government of Albania (GoA) has committed to significant reforms to modernize its public sector through a GovTech approach, combining the adoption of digital technologies with public sector reforms implemented a whole-of-government approach. The aim of these reforms has been to increase the effectiveness of the public administration, and to provide more inclusive access to high quality public services for all Albanians. To this end, in 2008 the National Agency for Information Society (Agjencia Kombëtare e Shoqërisë së Informacionit – AKSHI) was established to lead the digitalization agenda. In 2012 AKSHI launched the e-Albania digital service portal, which currently enables online applications to around 1225 services (95 percent of all central government provided administrative services). As of 2022, e-Albania had around 2.8 million registered users (individuals and businesses).

Albania's notable progress with GovTech reforms has been recognized internationally. The 2022 edition of the WB GovTech Maturity Index (GTMI) categorizes Albania within Group A (the most advanced of four groups), reflecting a positive evolution when compared with the previous edition where the country was positioned in Group B. The Organization for Economic Cooperation and Development (OECD) highlights Albania as a positive model for e-governance in the Western Balkans.

Despite the GoA's progress with the digital transformation, challenges remain, in particular from a user perspective. These relate to the need to upgrade existing systems, apply frontier technologies, improve the quality and delivery time of services and ensure equitable access to digital services to all Albanians, including to vulnerable groups such as the poor, rural communities, the disabled and those with limited digital skills.

In order to make the full transition to a user-centric mode of digital service delivery, and fully harnessed the newest technologies for a tangible impact on user experience in service delivery, the GoA continues to demonstrate a high level of political commitment to the Digital Transformation agenda. This is underpinned by a clearly articulated medium-term vision consisting of the GoA's government's 2030 political vision (2021), the National Strategy for Development and Integration (2022-2030), and the Albania Digital Agenda Strategy and Action Plan 2022-2026.

Given the World Bank's (WB) longstanding support or the GoA in service delivery and digitalization, the GoA requested further Bank support of the implementation of its digital transformation agenda. Building on the results of the WB-financed Citizen-Centric Service Delivery (CCSD) Project (2015-2020), the GoA and WB launched a new Program for Results (PforR), which became effective in July 2023. The Program is called "Improving Equitable Access to High Standard Public Services through GovTech" and its development objective is to increase the equitable access to and quality of selected digital services in Albania. The operation seeks to strengthen national systems to accelerate the transition to a fully user-centric mode of digital service delivery, to enable the Government of Albania (GoA) to harness new digital innovations for tangible impact and to move Albania into the advanced rankings of GovTech.

The Program supports the GoA in achieving selected objectives under its digital transformation agenda in three Results Areas (RAs):

1. **Enhancing E-Service Quality and User Experience**
    1.1. Re-Engineering of E-Albania Portal based on Accessibility and User Experience (UX)
    1.2. Ensuring High Standard, Personalized, and Pro-Active Event-based E-Service Re-organization
    1.3. Upgrading the E-Services Backbone: E-Albania and Government Gateway ICT Infrastructure and Business Continuity
2. **Improving Digital Skills and Digital Inclusion**
    2.1. Improving Digital and Foundational Skills
    2.2. Enhancing Customer Service and Accessibility
3. **Strengthening Priority GovTech Enablers**.
    3.1. Strengthening GovTech Whole-of-Government: Data Governance.
    3.2: Strengthening Whole-of-Government GovTech Institutional Enablers

One of the sub-Results Areas under RA3 is focused on strengthening GovTech Whole-of-Government: Data Governance.

There are selected areas where a "whole-of-government" approach to data governance needs to be further strengthened and further aligned with EU best practices. The GoA could make further progress in its data governance to ensure an even more secure, protected, advanced and personalized digital service delivery. First, key data protection and data security challenges include gaps in the legal framework and gaps in the capacities of public sector institutions to implement all necessary steps for data protection and information security. Second, data interoperability needs strengthening to move towards a genuinely "data-driven public sector" that is also compliant with the latest EU interoperability standards. This includes strengthening both non-digital and digital interoperability layers, such as by establishing Meta-data standards for all digital content. Third, there are weaknesses in service delivery data collection, data analytics and

data usage to improve internal accountability and management decision-making. Finally, data transparency and public usage of data could be increased, there is a limited amount of publicly available data that follows the best practice Open Data (OD) standards, and the OD portal has not been sufficiently designed based on UX.

This RA supports the GoA in its program objectives to: (i) strengthen data governance, data security and transparency; and (ii) adopting enabling digital systems, requirements, and intelligent processes. In addition, aspects of this RA are cross-cutting insofar as they support the broader achievement of results under RAs 1 and 2: for example, pro-active services require robust data governance.

To improve data governance, security and quality, this RA will support various initiatives and assessments on specific data governance topic relevant for the digital transformation agenda under this Program.

2. OBJECTIVE OF THE ASSIGNMENT

These Terms of Reference (ToR) are for an individual consultant (henceforth, the Consultant).

The objective of the consultancy will be to perform an initial assessment on the current cybersecurity status, and to support the AKSHI with day-to-day questions and tasks on cybersecurity and to perform more detailed assessments on the specific cybersecurity topics as requested by the AKSHI.

3. SCOPE OF WORK AND MAIN TASKS

The Consultant's role is to support the AKSHI by performing an initial assessment by reviewing the existing Program documentation: Program Appraisal Document (PAD), Terms of References for the components supported by the program and the coordination plan. Additionally collect cybersecurity input from AKSHI stakeholders in order to identify all entry points for improving the technical cybersecurity in particular and information security in general.

Subsequently supporting AKSHI on any other cybersecurity topics as requested by AKSHI in the form of recommendations (e.g. on staffing, training, software, hardware and policies), analysis and assessments.

The Consultant is expected to work closely with the AKSHI, the Program's Coordination Unit (CU - housed in AKSHI) and will perform the following tasks, during the assignment:

CURRENT SITUATION PHASE

Collect and analyze information on the current cybersecurity status for the components in the Program.

- Reviewing the available cybersecurity documentation for the components covered by the Program.
- Work closely with the beneficiary to collect information on the current cybersecurity status for the components in the Program.
- Consolidate this information in the initial assessment providing a narrative description of the AS-IS cybersecurity situation and potential challenges ahead.

CONSULTANCY PHASE

Analyze information and give recommendations on the actual and perceived cybersecurity requirements for the components included in RA1-3 in the Program for an initial 1-year plan period, with the possibility of extension, as needed. The task list includes, but is not limited to, the following.

- Supporting detection, investigations and mitigating exploits and compromises;
- Assist in developing or improving incident response plans to effectively address and mitigate cybersecurity incidents.
- Support in the development and implementation of cybersecurity policies, procedures, and best practices to strengthen the government's overall security posture.
- Advise on policies, tools and equipment to improve incident prevention, detection, and resolution;
- Monitor emerging cybersecurity threats and trends in the world and provide recommendations for proactive defense measures.
- Consultation on normative-legislative framework on cybersecurity and/or roadmap to become a member of international communities;
- Providing advice and consultation in the field of cyber diplomacy and cooperation;
- Performing training for specific topics of interest, e.g. APT, for AKSHI employees;
- Specific support in the detection and mitigation of APT and state sponsored threat actors;
- Recommendations on cybersecurity staffing.
- Providing just-in-time advice and inputs to the AKSHI on other identified and urgent cybersecurity issues, as needed.

4. DELIVERABLES

The Consultant will be responsible for the following key deliverables:

1. Initial assessment report

Initial assessment to identify current as-is cybersecurity situation for the components in the Program and other areas (as identified by the AKSHI), describing current technical cybersecurity status, challenges, and recommended mitigations.

The initial assessment shall include a gap analysis between the current technical cybersecurity setup and international best practices and a set of recommendations to align with international best practices.

All results will be documented in an informative report.

The Initial assessment report shall be delivered 30 days after contract signing.

2. Consultancy phase

Supporting the above task list by making assessments on cybersecurity, in the form of gap analysis and expert advice, upon request from AKSHI;

Note:

- Any and all copyrights and licenses related to the deliverables will be handed over to the AKSHI;
- The definitive dates for the activities and deliverable will be established in agreement with CU;
- All the written deliverables will be delivered in English language. Additional translation costs, if required, could be provided.

5. REPORTING

The Consultant will report to AKSHI and will closely coordinate its activities with the CU.

All report drafts and deliverables will be reviewed by AKSHI and other relevant stakeholders to ensure that the findings are acceptable, and the deliverables revised accordingly. AKSHI will facilitate the meeting appointments with the target list of interviewees for the current cybersecurity status and the collection of documents needed for the initial assessment report. The consultant will conduct field missions to ensure the successful completion of the assignment (a minimum of 5 missions is anticipated). The consultant is expected to contribute a short report summarizing key activities and results at the end of each mission.

For administrative matters, the consultant shall communicate with the CU case by case.

6. TERMS

The assignment is expected to start in August 2024. The effort level is a maximum of 100 days spread throughout 18 months, with a possibility of extension of the contract beyond the first year, as needed. Out of the 100 days, at least 50 working days will be spent on site at the AKSHI premises.

The Consultant is not required to be located in Albania, though he/she is expected to visit the country as necessary. The timing and frequency of visits will be agreed beforehand with CU. Between missions Consultant should be available for virtual meetings based on agreed schedule with CU.

7. CONSULTANT QUALIFICATIONS

The Consultant retained for the project shall have an international perspective on cybersecurity, cyber incidents, and crisis management (therefore with a keen understanding in cyber threats but also with a strategic outlook, focused on government systems/services protection) and shall have the following expertise and experience:

- At least Master's degree in law, political science, international relations, information and cybersecurity technologies or an equivalent combination of academic qualifications, and work experience in the cybersecurity field;
- Previous experience acting as international cybersecurity expert with a focus on policy analysis, cyber diplomacy, and cyber capacity building. At least ten years of professional experience in cybersecurity, with international expert knowledge in research and policy analysis, cyber crisis management, cyber resilience, and cyber diplomacy.
- At least 3 years of experience with compliance on EU cybersecurity and information security-oriented regulations and directives;
- Demonstrated experience in conducting cybersecurity assessments, and EU compliant.
- Proven experience and expert knowledge on digital risks, cyber resilience to support the improvement of national regulatory framework.
- Experience with different security technologies and products, e.g. Microsoft Azure cloud security is considered a plus;
- Excellent oral and written communication skills in English.

8. IMPLEMENTATION AND ORGANIZATIONAL ARRANGEMENTS

The CU shall provide the Consultant with administrative assistance, meeting space in order to perform her/his functions and responsibilities during her/his missions. CU shall also provide internet access, consumables and stationery goods required to fulfil the contractual obligations. The Consultant is expected to be equipped with her/his own personal computer/laptop.

9. EVALUATION CRITERIA

Applicants that fulfill the qualification requirements will be further evaluated based on the below criteria:

- General Qualification – 30 points
- Adequacy for the assignment – 60 points
- Language – 10 points

10. SELECTION

The service will be selected under the provisions of the World Bank Procurement Regulations for Borrowers under Investment Project Financing" dated July 1, 2016, revised on November 2017, August 2018, November 2020 based on the method of Selection of Individual Consultants, Time-based contract.