Terms of Reference - Short Term Expert - IT Consultant

IT Consultant for Preparation of proposal for Technical and Functional Specification of the Disaster Recovery Data Centre (DRDC)

Background Information

Digital transformation of the national economy and public administration are among the key priorities of Serbian Government. In addition to providing high-level political support and institutional sponsorship, the Government introduced new institutional framework to manage this process and initiate internal changes.

The Government of Serbia, elected in June 2017, has heavily prioritized digital transformation of the national economy and state administration. The Prime Minister's Keynote Address before the Parliament stressed digitalization and education as the most important catalysts of innovations, competitiveness and growth for Serbia in the coming years. It also stressed the need for a rapid digitalization of public administration and provision of integrated, secure and citizen-focused electronic services. This political support has materialized in August 2017, when the new Government formed the Office for IT and eGovernment (OITeG) and appointed the Prime Minister as head of the Council for Innovative Entrepreneurship and Information Technologies (IT Council).

In addition, the Government of Serbia has requested assistance of the World Bank in supporting the reform efforts, through a loan. To this effect, the World Bank has initiated the Enabling Digital Governance Project (EDGE). The objective of the project is to improve access, quality and efficiency of eGovernment in Serbia.

The project, officially started in May 2019, aims at contributing to development of the digitalization in Serbia, through implementation of the following components:

Component 1: Foundations for Digital Service Delivery

The objective of this component is to establish the necessary cross-cutting foundations to support the use of ICTs in the provision of public services to citizens, and businesses, including inter alia, regulations, standards, and digital infrastructure.

Component 2. Transforming Services for Citizens, Business and Government

The objective of this component is to support re-engineering, digitalization, and piloting of selected administrative e-services. It will support improvements in back-office processes to reduce administrative burdens and increase efficiency of administrative service delivery to citizens and businesses.

Component 3. Digital Skills Development, Institutional Strengthening and Change Management

Activities under this component will focus on transforming the provision of administrative services to citizens and businesses, which will result in the change of the way public servants do their work as well as the way citizens and businesses interact with the administration. The key result of this component is enhanced capacity for project management and institutional coordination to achieve project results. This component will include strategic frameworks to help all stakeholders to understand, commit and successfully develop digital skills, implement change and, by promoting digital skills and changes, contribute to further institutional strengthening which will bring major benefits to citizens and business.

For the purposes of effectively managing and coordinating EDGE and future projects with IFI financing, the Project Implementation Unit (PIU) has been founded at the OITeG.

Initial consultations between the key government stakeholders gathered in the Coordination Council for e-Government indicated that the currently available data center facilities will be insufficient or unqualified to provide for the required long-term computing, communication and security infrastructure needs. In accordance with Article 29 of the Law on eGovernment, physical data protection and backup are prescribed. The competent authority provides additional physical protection of the data by forming a secondary database and a secondary computing system to ensure the continued functioning of the eGovernment services. The OITeG conducted a survey with 90 Governmental institutions and, after analyzing all the information received, concluded that a Disaster Recovery Data Centre (in further text: DRDC) is necessary and that the DRDC should host at least four plus two modules in Facility No. 1 (two for government institutions, two for commercial renting and two to be equipped in later stages), with a total of around 800 rack units in full capacity, and one module in Facility No. 2 with total 120 racks Also, "N+1" or better redundancy model is preferred to be achieved at each level of the future facility. The Consultant is expected to further elaborate and confirm or modify these requirements through the process explained further in this ToR.

The DRDC is planned to be built on a plot of 40.000 sq. m area in total and including two facilities. Total flor area of facility No. 1 is 8.398,74 sq. m and total flor area of facility No. 2 is 3.437,71 sq. m.

In response to this need, the Government of Serbia has decided to commence with the construction of a new DRDC. The Government has designated this project as strategically important, and appointed the OITeG as the "Investor", in line with local planning and construction rules and regulations, and a future Manager of the DRDC, on behalf of the Republic of Serbia. Finally, the Government has identified a location in the City of Kragujevac as a suitable for the construction of the Facility.

In order to successfully deliver the results of EDGE under Component 1, the Elaborate for DRDC should be developed and deployed.

Objectives of the Assignment

OITeG is seeking to hire senior short term expert (STE) – IT consultant, hereinafter referred as the Consultant, with data center design and cybersecurity expertise to provide technical guidance to the process of planning and execution of technical solutions (Software and Hardware) for DRDC facility. The Consultant's duty is also to review the current state of the primary data center (in further text: DC), and to prepare recommendations for DRDC development. The Consultant should prepare recommendations for integration of relevant products and services within DRDC itself and also between DC and DRDC, followed by advises on the foundation of cyber security related requirements, operational compliance, development of tools, technology, methods, services and solutions.

The Consultant shall provide guidance to OITeG and PIU on data center infrastructure designs and data security to support of a large scale and complex IT infrastructure, system integrations, and business process for provisioning data center services in support of client requirements. In addition, the Consultant will prepare a roadmap for the future DRDC and DC and infrastructure services, cloud services, and security services domains, provides leadership and effectively communicates with all levels of management - including "C-level" in areas related to data center solution architecture and future technical strategy. The Elaborate should be conducted in three (3) Phases, with the following deliverables:

Phase 1 – Inception Report

The consultant work in this phase will be based on the existing reports and documentation listed below – requirements obtained through surveys already conducted with 90 Governmental institutions and

commercial users (in further text: stakeholders) during the inception phase for the design development of new government DRDC. Also, based on these reports, the Consultant will identify deficiencies of the existing DC, located in Belgrade, in order to be able to synchronize existing DC with the new DRDC in Kragujevac. Based on analyzed documentation, the Consultant should produce the Inception Report for the OITeG, as a high level review of current potential risk and challenges identified in DC and future DRDC.

Phase 2 – High Level DC and DRDC Expansion Assessment Report

Based on the Inception Report (Phase I) and best professional practice, the Consultant will develop a DRDC and DC Expansion Assessment Report for the OITeG, which will include a set of recommendations for hardware (HW) and software (SW) solutions to be implemented in both, DC and DRDC, which will enable them sustainable, smooth and frequent (fast) data synchronization. The areas to be covered, at least, are:

- DRDC Equipment – active equipment (storages, servers, system software etc.)
- Primary Data Centre Central Data Backup
- Active/Active or High Data Availability Solution for Data Centre
- Connectivity for e-Government
- Monitoring of Application (in further text: MoA)
- Network Operations Centre (in further text: NOC)
- Computer Emergency Response Team / Security Operations Centre (in further text: CERT/SOC)

In order to develop the best practice recommendations for NOC and CERT/SOC solutions, the Consultant will be provided the report "Analysis and strategy development of the State Network of the Republic of Serbia and data centers under the jurisdiction of the OITeG".

Phase 3 - Final Report

Based on the results of two previous Phases and subject-matter expertise, the Consultant should prepare and deliver the Final Report, which should include set of high level recommendations for design, implementation, administration and management of DRDC and DC in both locations, as well as recommendations for the future data center and infrastructure services, cloud services, and security services domains

Deliverables, Timelines and Payment schedule

The Consultant shall be responsible for the following deliverables:

No.	***Deliverable***	***Deadline***	***Payment***
1.	Phase 1 – Inspection Report	45 days after contract signing	30%
2.	Phase 2 – High Level DC and DRDC Expansion Assessment Report	75 days after finishing Phase 1	50%
3.	Phase 3 – Final report	30 days after finishing Phase 2	20%

All deliverables and reports must be accepted & approved by the OITeG, PIU and WB responsible person.

All deliverables must be submitted in English and Serbian (upon approval). All deliverables shall be provided in electronic copy format only.

All documentation to be delivered as part as this contract should be in Microsoft Word or Excel 2003 or higher, or in format that can be viewed and edited by open source and free software (e.g. for business process diagrams).

After awarding the contract, the Consultant shall sign the Non-disclosure Agreement (NDA). The following documentation will be delivered to the Consultant after signing the NDA as a basis for work:

- Conclusion of the Government of the Republic of Serbia, 05 No. 351-6365/2018, July 06, 2018.
- Law on e-administration,
- Law on information security,
- Technical requirements for the development of technical documentation for Government Data Centre,
- Analysis and strategy development of the State Network of the Republic of Serbia and data centers under the jurisdiction of the OITeG,
- Building Permit Project,
- List of state institutions software and hardware needs.

Required Qualifications

- Master Degree or four (4) year degree in Information Technology and 15 years of relevant experience to include major cloud service providers
- Must have at least 10 years of recent experience in leading large enterprise and government cloud projects
- Proven experience in development of relevant documentation for implementation of the government's disaster recovery data centers. Strong capability and extensive experience in interpreting datacenter cloud architecture and security requirements and advising on technical solutions in the form of conceptual, logical, and physical designs, including the ability to articulate those concepts both verbally and in writing – Serbian and English preferred
- Have a strong background in both private and public cloud environments, migrations and cloud native development. Being familiar with most major public clouds (e.g. AWS, Azure, GCP) and have experience in setting up everything from single instances to complex managed and distributed services
- Extensive experience with virtualization and software defined datacenters, with virtualization tools from VMware, Openstack and similar
- Have strong interest in Infrastructure-as-a-Code with various cloud frameworks, such as Terraform, CloudFormation and other automation frameworks
- Have experience in design and delivery of systems based on public cloud IaaS, various PaaS, SaaS and CaaS offerings, as well as exposure to different architecture models such as all-in and hybrid cloud

- Experience operating workloads leveraging PaaS, SaaS and CaaS solutions, such as Kubernetes, CloudFoundry and others
- Have experience with continuous integration, continuous deployment, continuous delivery, and automation tools, such as Jenkins, Bamboo, Concourse, Spinnaker, and others
- Must demonstrate strong skills in defining cyber security compliance solution design
- Ability to synthesize solution design information, architectural principles, available technologies, third-party products, and industry standards to advise on a data center architecture that meets client's data requirements
- Extensive experience on a broad spectrum of technology areas, including cloud solution design, cloud migration and operation, IT service management, data center modernization, advanced networking, mobility, cyber security, data classification, compliance implementation, change management, disaster recovery and business continuity, incident response, risk management and security audits
- Strong intellectual curiosity in exploring and learning new technologies, technology trends, forthcoming industry standards, new products, and the latest solution development techniques; ability to leverage this knowledge to formulate technical solution strategy
- Experienced in delivering presentations, leading meeting discussions with customers and team members at all levels (including "C-level")
- Experience working with Oracle, Microsoft 365, Microsoft Azure, Amazon Web Services (AWS), Google Cloud or other cloud providers
- Experience with cyber security strategy and ability to design and architect solutions based on policies and standards such as CSIRT, ENISA, FEDRAMP, NIST, etc.

Preferred Certifications

- **ISC2 - CISSP or CCSP certified**
- **Microsoft certified**
- **Cisco certified**
- **AWS / GCP / Azure certified**
- **CKA/CKAD certified**

Length of assignment

- The Consultant shall be engaged for up to 120 days in the period of one year from the beginning of the assignment. Duration of the assignment may be subject to extension depending on project needs.

Confidentiality

- The Consultant undertakes to maintain confidentiality on all information that is not in the public domain and shall not be involved in another assignment that represents a conflict of interest to the prevailing assignment.

Selection of Consultant

- A Consultant will be selected in accordance with the Open Competitive Selection of Individual Consultants as set out in the Regulations.