Terms of Reference

Support for development of the Calculator

Improving Public Financial Management for the Green Transition Project

Background

Improving Public Finance Management for the Green Transition in the Republic of Serbia is a four-year Operation supported by the World Bank and the Agence française de dévelopement (AFD), which aims to help the Government of the Republic of Serbia in strengthening its capacity to manage public finances and implement green investments. Key implementing institutions besides the Ministry of Finance are the Ministry of Environmental Protection (MoEP), the Republic Property Directorate, the Public Policy Secretariat (PPS), the Public Procurement Office.

The Operation consists of two components:

1) **Program for Results (PforR) component (Program)** comprising two results areas:

- Strengthen fiscal resilience, transparency, and spending effectiveness-focused on further strengthening fiscal resilience, using public expenditure management to enhance efficiency and a result focus, enhancing the ability to link plans and budgets through stronger costing at the planning stage, improving fiscal transparency, and improving the preparation of public investment projects.
- Greening Serbia's expenditure cycle and developing selected other institutions for greater environmental resilience- focused on introducing and utilizing green criteria in Public Finance Management (PFM), Public Investment Management (PIM), and public procurement, and on strengthening systems for monitoring and reporting on Green House Gases (GHGs) emissions from installations.

2) **Investment Project Financing (IPF) component (Project)** consisting of technical assistance to support the implementing entities in delivering expected results. The IPF component will consist of Technical Assistance (TA) - including trainings, capacity building and peer learning, support for stakeholder engagement, and support for managing the Program.

The Operation development objective is to improve core PFM functions and institutional capabilities needed for Serbia's fiscal resilience and Green Transition. The Operation will support the following core PFM functions (i) budgeting and strengthening linkages between plans and budgets, (ii) public investment and asset management, and (iii) fiscal risk management.

Objective of the assignment

The main objective of this assignment is to develop the Calculator as a software solution that aims to improve and digitize the existing Costing table with Instruction and which enables a unified calculation of costs of public policies and regulations. The calculator shall include: front matter, introduction, solutions, further considerations, success evaluation, scope of work, analysis, deliberation, and end matter. The practical recommendations and guidelines provided within amended version of the Costing Manual for the purpose of green and climate aspects integration into PPDs and regulations, the existing costing table, as well as the Methodology for Calculating Standard Costs for the Preparation of Planning Documents and Regulations[1] are intended to be the basis for the development of the software for calculator. These solutions have been further specified within the Technical specification for the Calculator and which has been completed. The PPS intends to engage one firm to develop the software solution for the calculator in order to upgrade and digitalize the current costing table.

[1] https://rsjp.gov.rs/en/calculation-of-costs-for-planning-documents-and-regulations/

Furthermore, PPS aims to ensure a unified calculation of costs of measures and activities during the process of development of planning documents and regulations, including the calculation of costs of green and climate aspects. As a part of this initiative, we are seeking a qualified firm to develop the software solution for calculator in order to enable the unified calculation of the costs during the development of planning documents and regulations. Once the calculator software is being developed, it is intended to be installed on PPS' website for the purpose of use by civil servants at the national level in Serbia.

A part of the proceeds of the IBRD loan will be used for financing the proposed assignment. These Terms of Reference define the scope of activities and responsibilities of the firm.

Scope of Work

The firm's scope of work will include, but not be limited to, the following:

- Develop a preliminary/initial version of a software solution for the calculator in accordance to the Technical specification[2], aiming to digitize and to unify calculation of the costs of public policies and regulations at the national level in Serbia [3];
- Cooperation with the PPS, during the course of development of the preliminary/initial version of software solution for the calculator and programming of software calculator**;**
- Software programming of the calculator which includes: front matter, introduction, solutions, further considerations, success evaluation, scope of work, analysis, deliberation, and end matter;
- Installation of the software for the calculator on the PPS' website and testing of its functionalities;
- Develop upgraded and finalized version of the software for Calculator based on PPS' inputs and testing of software in practice.

Deliverables[4]

1 System Analysis, Requirements Gathering, and Initial Design

- Perform a comprehensive analysis of stakeholders and business requirements to align the platform's design with client and user needs.
- The service provider shall deliver a detailed report covering the system analysis, collected requirements, and outcomes of the initial design phase. This report must be submitted for client review and approval before proceeding to the next phase of implementation.

2 Cost Calculator for Public Policy Documents and Regulations implementation service

- Software Development / Implementation
- Installation and implementation of all Cost Calculator elements
- Upon completion of the implementation, the service provider shall deliver a comprehensive report detailing all performed tasks, which will serve as the basis for the issuance and signing of the acceptance certificate
- The service provider shall deliver a user manual for General Public User in electronic format (PDF or equivalent).

[2] In accordance to the deliverables of *the Terms of Reference for the development of technical specification for the Calculator*.

[3] In line with the solutions stipulated within the amended Costing Manual, which includes green and climate aspects, Methodology for Calculating Standard Costs for the Preparation of Planning Documents and Regulations and existing Costing table.

[4] A detailed explanation of the deliverables can be found in the Technical specification for the Cost Calculator for Public Policy Documents and Regulations, which is Annex 1 of the Terms of Reference (ToR).

- The service provider shall deliver a technical documentation of the Cost Calculator which including:
    - Description of the Cost Calculator's architecture, technologies, and components.
    - Diagrams and other supporting materials that enable understanding and further maintenance of the Cost Calculator.
    - Application source code organized in an appropriate repository or archive.
    - README document with basic instructions for installation, configuration, and testing of the Cost Calculator.
    - API documentation of the Cost Calculator (specification of available routes, methods, and communication formats).

3 Training service for administration of the Cost Calculator for Public Policy Documents and Regulation

- Training of the client's staff for administration of the Cost Calculator, to be conducted in person at PPS's office location
- Prior to the training, the service provider shall deliver training materials and administrative documentation of the Cost Calculator via email, in electronic format (PDF or equivalent). Training materials will include: Instructions for maintenance, administration, and monitoring of the Cost Calculator, Information on accesses, security measures, and procedures related to Cost Calculator. No testing or certification of participants is required.
- The service provider shall also deliver a training report, including signed attendance sheets of all participants. Training report will be delivered upon completion of the training

Warranty

The Service provider must provide the following services under the Contract.

- **Warranty coverage period**: 12 months;
- **Defect Repair Service**: The Service provider is responsible for correcting all defects without any cost to the Purchaser within 30 days from the date of notice by the Purchaser within the warranty period.
- During the warranty period, the Service provider will ensure the normal functioning of the entire System, addressing any arising issues, and offering guidance for smooth operation post-deployment;
- Intervention maintenance will be about solving critical problems;
- The service provider will respond to the request for emergency maintenance when the problem is highly critical, regardless of its working hours and the working hours of the MAFWM, and will engage all possible resources. By signing the work order or minutes by the authorized person of the Purchaser, it will be considered that the intervention is completed.
- Forty-eight hours after receiving an emergency maintenance request will be the deadline for eliminating highly critical problems and ensuring the software's standard functionality

Time schedule

The firm shall prepare and deliver the following in the corresponding stages of the assignment:

Deliverables	Due dates
Deliverable 1: System Analysis, Requirements Gathering, and Initial Design	30 days after signing the

• Detailed report covering the system analysis, collected requirements, and outcomes of the initial design phase	contract
Deliverable 2: Cost Calculator for Public Policy Documents and Regulations implementation service • Software Development / Implementation • Comprehensive report detailing all performed tasks • User manual for General Public User in electronic format • Description of the Cost Calculator's architecture, technologies, and components. • Diagrams and other supporting materials that enable understanding and further maintenance of the Cost Calculator. • Application source code organized in an appropriate repository or archive. • README document with basic instructions for installation, configuration, and testing of the Cost Calculator. • API documentation of the Cost Calculator (specification of available routes, methods, and communication formats)	100 days after signing the contract
Deliverable 3: Training service for administration of the Cost Calculator for Public Policy Documents and Regulation • Signed attendance sheets of all participants, • Training materials and administrative documentation of the Cost Calculator	120 days after signing the contract

The selected firm shall be paid the lump sum contract amount linked to the deliverables.

Reporting obligations

The firm will report to the PPS' Sector for the planning system, coordination, development and improvement of public policies.

The firm should take into consideration all relevant gender related issues in relation to the outputs of the assignment.
The firm will provide hard and electronic copies of any documents and technical materials developed during the Project in their original electronic PDF format. The reports will be provided in English/Serbian language.

Ownership and Intellectual Property Rights

All intellectual property rights for the developed software, including the source code, documentation, and related materials, will be transferred to PPS upon project completion. PPS will have full ownership and rights to use, modify, and distribute the software as needed.

The Consultant/Firm is to meet the following requirements:

Consulting firm:

- Implementation, maintenance, and upgrade of at least 2 (two) projects with cost calculation / expense calculation functionality;

- At least 5 years of general experience in project management and development of public facing web portals / applications for large clients;
- Technical expertise in developing and integrating IT systems within existing client's infrastructures is considered as an advantage
- Experience working with Serbian state authorities is considered as an advantage;

The Consultant/Firm shall provide a team of experts covering the following requirements:

Key Expert 1 - Project Manager:

- MSc degree or equivalent in the field of computer science, informatics, ICT engineering or equivalent technical field;
- At least 10 years of relevant professional experience and strong portfolio showcasing a project management experience. PMP certification is considered an advantage
- Possess project management experience on at least two similar assignments with cost calculation / expense calculation functionality; experience with developing portals / websites of public institutions is considered an advantage
- Excellent knowledge of written and spoken English and Serbian language
- At least 2 years of experience in planning and overseeing user training sessions for implemented IT solutions. Proven skills in organizing and delivering in-person user training sessions. Strong facilitation and communication skills for knowledge transfer and capacity building

Key Expert 2 – Web UI/UX designer

- A bachelor's degree in design, computer science, or a related field
- At least 10 years of relevant professional experience and strong portfolio showcasing a user-centered approach to design and a strong understanding of design principles and techniques.
- Experience in prototyping and wireframing - creating wireframes, high-fidelity mockups, and interactive prototypes of designs. Experience with designing portals and websites of public institutions is considered an advantage
- Excellent knowledge of written and spoken English and Serbian language

Key Expert 3 – Front-end developer

- MSc degree or equivalent in the field of computer science, informatics, ICT engineering or equivalent technical field;
- At least 5 years of relevant experience as developer and in-depth knowledge of relevant programming languages HTML, CSS, JavaScript and JavaScript Frameworks.
- Proven record of implementations of projects with the cost calculator / expense calculator functionality
- Excellent knowledge of written and spoken English and Serbian language
- Preferably has at least three years of experience on development projects in Serbian government administration bodies.

Key Expert 4 – Back-end developer

- MSc degree or equivalent in the field of computer science, informatics, ICT engineering or equivalent technical field;
- At least 5 years of relevant experience as developer and in-depth knowledge of relevant backend technologies matching project technology stack.
- Proven record of implementations of projects with the cost calculator / expense calculator functionality
- Excellent spoken and written English and Serbian language
- Preferably has at least three years of experience on development projects in Serbian government administration bodies.

Length of assignment

The period of contract implementation will be 120 days from the contract signature.

The firm shall deliver all the expected outputs at the daily rate that will be dependent on the qualifications, the market range for similar assignment and previous candidate remuneration for similar services as well as approved project budget.

Input by the PPS

The PPS will provide the firm's access to any documentation and information within the jurisdiction of the PPS necessary for the performance of its tasks.

Confidentiality

The firm 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 firm

The firm will be selected in accordance with Consultant's Qualifications Selection (CQS) method set out in the World Bank's Procurement Regulations for IPF Borrowers (July 2016, revised November 2017, August 2018 and November 2020).

Expressions of interest will be evaluated based on the following criteria:

General experience in the field of assignment	40 points
Specific experience relevant to the assignment	60 points
TOTAL:	**100 POINTS**

Annex 1 –
Technical Requirements

for the Cost Calculator for Public Policy Documents and Regulations

A.1. BUSINESS FUNCTION REQUIREMENTS TO BE MET BY THE COST CALCULATOR (APPLICATION)

#	Name of Related Service	Technical Specifications and Standards
1	**System Analysis, Design**	Web-based cost calculator application that enables users from the general public and government institutions to accurately calculate costs associated with the preparation of planning documents and regulations. The application will strictly adhere to the Costing Manual and the Methodology for Calculating Standard Costs for the Preparation of Planning Documents and Regulations. The application must explicitly identify and highlight activities, categories, and costs that are designated as "green"—representing eco-friendly alternatives to conventional options. These green cost elements will be clearly presented throughout the application.
		The Application shall support the following user roles: • General Public User • Administrator • System(automated functions) The Application shall enforce role-based access control to ensure that users can only access functionalities permitted for their role.
		Cost calculation is the main part of the Application, which is accessible to the general public. There is no need for the users of the calculator to register and login in order to use the calculator. Cost calculation is performed for one activity only. Each calculation session requires a single activity to be set. An activity is set by filling in the fields Activity Number, Activity Title and selecting the Activity Type from a dropdown list. Next to the Activity Type dropdown, a tooltip explaining the field is shown. The tooltip is activated by clicking or hovering the mouse pointer over it, depending on the client device. After an activity is set, a range of years during which the activity will take place is selected, by selecting one or more checkboxes from the respective chechbox list Choose validity period. The years offered are 10 years in the future from the current year (the number of years is a configurable parameter of the Application). For each selected year, the Application shall show a separate tab for

		entry of costs of conducting the activity for the selected year. Cost calculation for the set activity is then continued by selecting a cost subcategory from its respective dropdown list. For each selected cost subcategory, a standard cost is selected from the dropdown Standard Cost Title. Each standarized cost has its own unit of measurement and cost per unit. The standard cost title, unit of measurement and unit cost are managed using the Administrative Module. Costs contributing to achieving the goals of the Green Agenda are marked with a green leaf icon in their respective row of the calculator. Individual rows with standard costs can be added and removed by clicking the corresponding action buttons. The Remove action button will remove a single row with standard cost from the calculation, and the total sum will be automatically recomputed. There are two Add buttons – Add Cost Subcategory and Add Standard Cost within a given subcategory. By clicking the Add Cost Subcategory button, a new row will be added to the calculator containing the dropdown for selection of cost subcategory and standard cost within the selected subcategory. By clicking the Add Standard Cost button, a new row will be added to the calculator, containing the dropdown for selection of standard cost within the same cost subcategory from the previous row. In each calculator row, the user fills in the quantity in which the cost is applied (e.g. Number of experts = 2 or Number of seconds = 30) and the frequency in which the cost is repeated throughout the selected year. As each field is filled in, the Application calculates a subtotal for the given unit cost, based on the following formula: Subtotal = Quantity × Frequency × Unit Cost At the same time, the Application computes the total cost of activity by summing all subtotals for all unit costs entered so far. The Application automatically recomputes and updates subtotals and total cost on each data entry change. The Application shall allow previously entered unit cost rows to be rearranged on the calculator form using “drag and drop” mouse action. Rearranging the rows should be implemented so that the integrity of data is maintained and the calculation result is not affected. A row containing standard cost within a parent cost subcategory can only be moved to a different position within the same parent cost subcategory, whereas rows which contain a parent cost subcategory for one or more standard cost rows can be moved to another position together with all standard cost rows belonging to the respective cost subcategory row.
		The Application shall allow users to generate an export file containing: • A tabular layout of all entered data • Calculation results (subtotals and total costs) The exported file shall closely match the visual representation shown in the Application calculator interface, except for the

		division by years, where it is defined that the calculations per year will be listed one below the other in the same Excel sheet. The Application shall provide the export file as a downloadable resource in Microsoft Excel format. The exported file will be allowed for saving to user's local client device after download.
		The system shall provide an administrative interface for managing the following data entities and codebooks: • Activity types • Cost subcategories • Standard costs •Units of measure and respective labels • Front-end labels •Years (of activity implementation or PPD validity) The Application shall restrict access to administrative functions to users with the Administrator role. The Application shall allow administrators to add, modify, or delete entries in codebooks and data entities.
		The System shall automatically track and store the date and time of the last update to codebooks and data entities done by the Administrator. The Application shall display the last update date and time on the calculator interface for transparency.
		UC 1.1 – Calculate Activity Cost *Actors: General public user* Description: The user selects an activity category and fills in the number and title of activity. The user selects one or more years when activity is planned. For each year, the user calculates individual cost one or more times (UC 1.1.1). The application updates the subtotal and total on every data input and generates the calculation results (UC 1.1.2) **UC 1.1.1 – Calculate Individual Cost** *Actors: General public user* Description: The user fills in an individual cost by selecting cost subcategory and standard cost and fills in the frequency and quantity. The Application calculates the individual cost on entry change and displays it next to the individual cost entry in the same row. **UC 1.1.2 – Generate Calculation Result** *Actors: General public user* Description: On every data change, the Application calculates the subtotals for individual costs by multiplying quantity, frequency and unit cost. All subtotals are added up to calculate the total cost, which represents the calculation result. **UC 1.2 – Export & Download Calculation Result**

		Actors: General public user Description: The user can generate an export file containing a tabular layout of all data entered in the calculator as well as the calculation results (total and subtotals per unit cost), matching as nearly as possible the visual representation shown in the calculator. The export file is offered for download and the user can save it locally on his client device. **UC 1.3 – Administrative Management of Entities and Codebooks** *Actors: Administrator* Description: The administrator manages data entities and codebooks using an administrative interface. The entities and codebooks managed are: activity types, cost subcategories, standard costs, units of measure, labels, years of activity implementation or PPD validity. **UC 1.4 – Track Last Codebook Update** *Actors: System* Description: Each update of data entities and codebooks performed under UC 1.3 is tracked by the system to keep the last date and time of data modification. This date and time is displayed on the calculator.
		The Application UI/UX design must be aligned with the following best practices: • Simplicity and clarity - The UI/UX design should be minimalistic, focusing on core functionality. The input fields should be labeled clearly and placeholder text should be used for guidance. For longer explanations, popup tooltips will be used. Progress indicators and/or processing indication visual aids such as preloaders should be used if any user action can take longer than 3 seconds. • **User-friendly input -** The known data in input fields should be pre-filled and default values in dropdowns pre-selected. All input validation should take place inline in real time before total form submission. Using keyboard to navigate fields and populate them should be supported. • **Accessibility** - Accessibility standard for government websites of the Republic of Serbia should be followed. **Responsive design** - The implementation must ensure that the Application is fully usable on desktop, laptop and tablet devices with no visible loss in functionality and UX. For mobile devices, due to the tabular layout of the wireframe, it is acceptable to use scrollbars if the tabelar layout cannot be replaced with an adequate solution for mobile device screen resolutions.

		The following entities make up the conceptual data model: • Activity type • Cost subcategory • Standard cost • Unit cost The activity type represents the main level of grouping of calculated costs. The user can select only one activity type for one calculation. All cost subcategories which can be used in a single calculation session belong to the same activity type. For each unit cost that makes up the calculation, a cost subcategory is first selected. For a selected cost subcategory, a set of standard costs is offered. Each standard cost belongs to one or more cost subcategories, and each cost subcategory contains one or more standard costs. The standard costs are used as templates to make up unit costs in a single calculation session. A unit cost is entered by selecting a standard cost and applying quantity and frequency of this cost. The same standard cost can be used to instantiate one or more unit costs in a single calculation. A standard cost can be flagged as "green" or "not green" (eco-friendly or not).
		Activity type: - Description: Main level of hierarchy in calculator data. One activity type is selected per calculation session. - Relationships: Contains one or more activity subcategories
		Cost subcategory: - Description: Each row in calculation belongs to one subcategory. Selecting a subcategory allows for selection of standard cost. - Relationships: Belongs to exactly one activity type, contains one or more standard costs
		Standard cost: - Description: Each row in calculation is based on one selected standard cost. A standard cost has a name, unit of measure, default unit price. - Relationships: Belongs to one or more cost

		subcategories, induces creation of unit cost
		Unit cost: - Description: The actual unit of calculation contained in a single row. Can be based on standard cost or custom entered if standardized unit or price are not available. - Relationships: A set of unit costs makes up a calculation.
		The logical data model defines data entities in detail – keys and attributes, and their relationships, based on the relational database paradigm.
		Assumptions <u>User Access & Interaction</u> • Users can access the calculator without logging in or creating an account. • The calculator is used primarily for one-time calculations without saving user inputs. • Users will have access to modern web browsers (Chrome, Firefox, Edge, Safari). • Users are expected to have basic knowledge of cost inputs and calculations. <u>Functionality & Data Handling</u> • The calculator will process numerical inputs and return cost estimates instantly. • Inputs will not be stored persistently (no database storage for user-generated data). • The system will perform calculations based on predefined formulas, which may not cover all possible use cases. <u>Performance & Scalability</u> • The Application is expected to handle high traffic since no authentication bottleneck exists. • The Application should work efficiently on both desktop and mobile devices. <u>Security & Privacy</u> • Since there is no authentication, no personally identifiable information (PII) will be collected. • Any sensitive data should not be stored or logged. • Data entered by users will not be recoverable once they leave or refresh the page.

		Constraints No User Accounts or Data Persistence • Users cannot save, retrieve, or track previous calculations. • Any data entered will be lost upon page refresh or browser closure. Limited Customization • Users cannot personalize the interface or modify underlying data entities and codebooks without administrator intervention. Technology & Compatibility • The Application must be implemented using web technologies (HTML, CSS, JavaScript) and must not require additional installations for frontend users (e.g., no browser plugins). • It must be optimized for performance across mobile, tablet, and desktop screens. Security & Data Protection • Since there is no authentication for the public facing calculator interface, the Application must not expose vulnerabilities like XSS or CSRF that could compromise user inputs. • The administrative interface is protected using at minimum username/password combination of credentials. • The Application must comply with GDPR-like data protection laws, ensuring that no unintended data collection occurs. Limited Offline Functionality • The Application will require an active internet connection.
2.	**Software Development / Implementation**	**Performance and Scalability** •The Application should handle up to 100 concurrent users with no significant loss in performance. •The Application should provide response to simple user actions such as individual calculations within 3 seconds. •The Application should efficiently process large datasets, such as being able to perform a cost calculation with 100 unit costs or returning a list of 100 standardized costs at once.

		Security • All data in transit should be encrypted. • The Application should be protected against common web vulnerabilities. • No personal data should be stored in the Application database.
		Availability and Reliability • The Application should have 99.5% uptime. • The database should be backed up using a regular automated process to minimize data loss in case of system failure.
		Usability • The UI should be responsive, supporting mobile, tablet, laptop and desktop devices. • The interface should support keyboard navigation and screen readers. • Error messages and tooltips should be clear, user-friendly and contextual. • Prefilled values should be used wherever possible.
		Maintainability and Extensibility • The Application should have modular architecture to allow future enhancements. • APIs should be versioned to support backward compatibility.
		The application should follow a three-tier system architecture, comprised of the following layers: •Presentation Layer (Frontend) •Application Layer (Backend APIs) • Data Layer (Relational Database)
		Technology Stack The requirements for the proposal of the technology stack for the Application are the following: • Robust, secure and well-integrated • Based on industry standard client and server platforms • Widely used in web-based software government projects in the Republic of Serbia Both backend and frontend components should meet these overall requirements. Additional requirements for the selection of the technology platform for the specific components are also defined, as follows: <u>Presentation layer:</u>

		• Using Vanilla JS or any well-established modern JS framework such as Angular, React or Vue.Js, providing a dynamic and interactive UI and able to handle client-side state management • Using Ajax or Fetch API calls to exchange data with the application layer •Supporting internationalization (support for Serbian Latin, Serbian Cyrillic and English version) <u>Application layer:</u> •Implemented on an industry standard programming platform • APIs based on REST protocol • Based on an industry standard server platform hosted in VPS or containerized environment, such as Linux VPS server or Linux-based Docker container <u>Data Layer:</u> • Using an industry standard relational database server with no additional licensing costs, such as SQL Server Express, MySQL or PostgreSQL
		Integration Points The Application does not integrate with any external data and functionality providers.
		The administrative part of the Application requires administrative users to be authenticated prior to accessing it. The authentication is done using username and password, where the username is the administrator's email address. The administrative user can also request his password to be reset. The Application will allow multiple administrative users but they will all share the same access level to the administrative part of the Application. There is no need for differentiation of individual user access levels within the administration. The public part of the Application – the calculator – allows unauthenticated access to all users from the public internet.
		The data stored in the Application will not contain any information that can be categorized as personal or sensitive (PII, health or financial data). It is required that the database integrity is maintained at all times and that the Application is protected against any data injection or insertion vulnerabilities.
		All data exchanged between the user and the Application should be encrypted in transit using TLS 1.2 or higher protocol. There is no need to encrypt data at rest, since all data stored in the Application is publicly available and no personal or sensitive data is kept.
		The Application should comply with best practices to prevent

		and mitigate security risks identified in the most current OWASP Top Ten list: 1.Broken Access Control 2.Cryptographic Failures 3.Injection 4.Insecure Design 5.Security Misconfigurations 6.Vulnerable and Outdated Components 7.Identification and Authentication Failures 8.Software and Data Integrity Failures 9.Security Logging & Monitoring Failures 10.Server-Side Request Forgery Special attention should be given to pre-emptive action during software design and implementation phase to comply with the list and care taken to follow the suggested mitigation strategies.
		The APIs exposed internally from application layer toward presentation layer will be based on REST protocol and all communication will take place using secure transport (HTTPS).
		No third-party integrations are present in the Application.
		The format for data exhange between presentation layer and application layer is JSON.
		Error Handling In general, errors and warnings should be displayed to the user without disclosing any technical or sensitive information about internal functioning. The errors should be handled in such a way to allow user to continue operation or re-run the same operation without significant data loss or disruption. Possible errors are categorized as: • User input errors • Business logic errors •Authentication and authorization errors • System errors **Logging and Monitoring** The Application should log information about all critical events. Logging should be done in textual format and verbose enough to allow issue resolution. Logs should be kept at least for three months. A log rotation system should be established. The Application should generate automated email messages in case of critical errors such as system errors and authentication errors and send them to a designated email address for

		monitoring.
		User input errors Example cases are: missing required input field, validation rule broken (text entered where numeric is expected, value exceeds a limit). The error should be handled so that the erroneous field is highlighted and the user is allowed to correct the error and continue operation without data loss.
		Business logic errors Example cases are: a subcategory contains no standardized costs so a unit cost can't be added. The error should be handled so that a clear message is shown and the user is allowed to continue operation by selecting a correct combination of entries.
		Authentication and authorization errors These are only applicable to the administration interface. Example cases are: invalid username or password entered in the administration login form, user is locked, user doesn't have appropriate access level for the selected data entity. The user should be redirected to the login page if he can't authenticate. In case of access level errors, a clear message should be shown instructing the user to contact the administrator for access level setup.
		System errors Example cases are: database connectivity issues, network connectivity issues, server overload, unexpected errors. A generic user-friendly message should be shown, instructing the user to try again later. All errors should be logged based on their assessed severity level for further analysis.
		To meet performance requirements, the Application should be stress-tested with load parameters given as per requirements. The stress test can be run using JMeter or any other applicable load testing tool with the following parametrization: • 100 concurrent users on page load responding within 3 seconds • 100 concurrent unit cost calculations responding within 3 seconds • Loading a list of 100 data entities and displaying it in a dropdown on the calculator form takes place within 3 seconds
		Based on previous data it is estimated that the average load on

		the Application will not surpass 10 users per minute and the peek should not be over 100 users per minute.
		The Application architecture allows vertical scaling by increasing allocated CPU and memory power and Internet bandwidth.
		The Application should adhere to standards and best practices for Serbian government websites in the areas of accessibity, data protection and internationalization.
		The Application should comply with WCAG 2.1 standard.
		Only technical cookies related to user session and calculation data should be used. No marketing or tracking cookies should be used.
		The Application should provide full internationalization in Serbian Latin, Serbian Cyrillic and English alphabet. Internationalization should cover all labels, calculation results and downloadable files. The administrative module does not need to be fully internationalized, however it is favorable if key elements can be displayed in Serbian.
		Security Risks Security risks include common web application vulnerabilities. Mitigation strategies are: • Applying OWASP Top 10 suggestions for prevention of web attacks • Keeping all 3rd party libraries at latest stable updated version • Using secure transport via TLS encryption • Using cookies with HttpOnly and Secure attributes
		Integrity and Accurracy Risks The risks in this category are: • Incorrect calculation due to incorrectly applied formulas • Incorrect standardized costs lead to incorrect unit and overall cost of planning activity • Incorrect rounding applied can lead to errors in total sums and overall cost Mitigation strategies are: • Perform automated and manual testing to ensure all calculations are correct • Use fixed decimal types for numeric values to ensure rounding is applied in a consistent and controlled manner without precision loss

		Performance Risks Mitigation strategies are: • Implement asynchronous requests for calculations that can last longer than expected performance threshold • Use auto-scaling for vertical resource scaling if server environment allows it • Optimize database queries using proper indexing and query optimization strategies • Use caching for large data structures that do not change frequently, such as codebooks
		Compliance and Accessibility Risks Compliance and accessibility risks are constituted in the Application failing to meet the related requirements Mitigation strategies are: •Ensure accessibility compliance by verifying the Serbian government websites guidelines checklist •Implement GDPR-compliant data storage policies – only technical cookies used, user acceptance or rejection is required • Clearly state all possible legal constraints related to the cost calculation results • Clearly display notices and instructions related to calculator operation •Verify that internationalization is diligently applied in all textual displays
		User Experience Risks The UX risks are caused by not meeting the stated requirements: • Poor UI/UX – If the interface is confusing, users may make mistakes or abandon the tool. •Lack of mobile optimization – If the application isn't mobile-friendly, it may alienate a portion of users. The mitigation strategies are based on adhering to UI/UX requirements: • Use intuitive input controls with clear and understandable labels • Use tooltips where ever possible • Implement real-time validation • Use responsive design and test the Application on devices of different resolutions as well as all supported browsers • Show clear error messages