Social Welfare Services Information System
Technical Requirements

The objective of this document is to be used as a technical specification document for Social Welfare Services Information system. This document is a part of a tender dossier for Development and Implementation of the Information system for the Ministry of Labor and Social Policy (Institute for the Social Activities) and the Centers for Social Work.
# Table of Content

List of Abbreviations ................................................................................................................................................. 4  
Terminology used ......................................................................................................................................................... 5  
Referenced Documents ............................................................................................................................................... 6  
Notes ........................................................................................................................................................................... 7  
Objective ...................................................................................................................................................................... 7  
SoWelSIS environment .............................................................................................................................................. 7  
SoWelSIS general requirements ................................................................................................................................. 12  
  Computing Hardware Specifications .......................................................................................................................... 13  
  Software Specifications ........................................................................................................................................... 13  
  System Management, Administration, and Security Specifications .................................................................................. 13  
  Migrating data from existing databases to SoWelSIS .................................................................................................. 14  
User Types ................................................................................................................................................................. 14  
Social Welfare Service Information System Architecture ........................................................................................... 15  
Data Model ................................................................................................................................................................. 25  
Reporting Tools ............................................................................................................................................................ 27  
System Management ..................................................................................................................................................... 29  
  Storage Requirements ............................................................................................................................................... 30  
  Security ..................................................................................................................................................................... 30  
  Data Encryption ....................................................................................................................................................... 32  
  Hardness of Operating system .................................................................................................................................. 32  
  Confidentiality of Communications .......................................................................................................................... 33  
  Network Security ......................................................................................................................................................... 33  
  Backup and Disaster Recovery Strategies .................................................................................................................. 34  
NON –Functional Requirements ........................................................................................................................................ 34  
  Standards and Methodologies ...................................................................................................................................... 34
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>35</td>
</tr>
<tr>
<td>SoWeISIS acceptance procedure</td>
<td>36</td>
</tr>
<tr>
<td>SoWEISIS CBMIS Database Schema</td>
<td>39</td>
</tr>
<tr>
<td>Application Prototypes</td>
<td>40</td>
</tr>
<tr>
<td>SoWeISIS maintenance</td>
<td>41</td>
</tr>
<tr>
<td>Additional Services</td>
<td>46</td>
</tr>
<tr>
<td>Training</td>
<td>46</td>
</tr>
<tr>
<td>Startup Service</td>
<td>46</td>
</tr>
<tr>
<td>Maintenance</td>
<td>47</td>
</tr>
<tr>
<td>SoWeISIS Project Management Requirements</td>
<td>48</td>
</tr>
<tr>
<td>Project Methodology</td>
<td>48</td>
</tr>
<tr>
<td>Security</td>
<td>48</td>
</tr>
<tr>
<td>Project Management Team</td>
<td>48</td>
</tr>
<tr>
<td>Project Management Board</td>
<td>49</td>
</tr>
<tr>
<td>Communication and Reporting</td>
<td>49</td>
</tr>
<tr>
<td>Project Phases</td>
<td>51</td>
</tr>
<tr>
<td>Description of the Information Technologies, Other Goods, and Services</td>
<td>52</td>
</tr>
<tr>
<td>Quality Evaluation Criteria Table</td>
<td>52</td>
</tr>
<tr>
<td>Estimated time needed for the SoWeISIS implementation</td>
<td>53</td>
</tr>
<tr>
<td>SoWeISIS Financial implications</td>
<td>53</td>
</tr>
<tr>
<td>Estimated budget summary</td>
<td>53</td>
</tr>
<tr>
<td>Evaluation criteria</td>
<td>54</td>
</tr>
</tbody>
</table>
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphic User Interface</td>
</tr>
<tr>
<td>HTML</td>
<td>HyperText Markup Language</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MVC</td>
<td>Model View Controller Pattern</td>
</tr>
<tr>
<td>SOA</td>
<td>Service-Oriented Architecture</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>UDDI</td>
<td>Universal Description, Discovery and Integration</td>
</tr>
<tr>
<td>WSDL</td>
<td>Web Services Description Language</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Model Language</td>
</tr>
<tr>
<td>AJAX</td>
<td>Asynchronous JavaScript And XML</td>
</tr>
<tr>
<td>3-4 NF</td>
<td>3rd or 4th Normal form for Relational Database Design</td>
</tr>
</tbody>
</table>
## Terminology used

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.</td>
</tr>
<tr>
<td>System Management</td>
<td>The term system management refers to methods and tools hardware and software aimed at the management and monitoring of the system.</td>
</tr>
<tr>
<td>SOAP</td>
<td>SOAP, originally defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks.</td>
</tr>
<tr>
<td>Model View Controller Pattern</td>
<td>Model–view–controller (MVC) is an architectural pattern used in software engineering. Successful use of the pattern isolates business logic from the user interface, permitting one to be freely modified without affecting the other. The controller collects user input, the model manipulates application data, and the view presents results to the user. Typically, views and controllers come in pairs, each corresponding to a small part of the user interface; an application will likely be built with many pairs.</td>
</tr>
<tr>
<td>Web Services Description Language</td>
<td>The Web Services Description Language (WSDL) is an XML-based language that provides a model for describing Web services.</td>
</tr>
<tr>
<td>XML</td>
<td>XML (Extensible Markup Language) is a general-purpose specification for creating custom markup languages. XML's purpose is to aid information systems in sharing structured data, especially via the Internet, to encode documents, and to serialize data.</td>
</tr>
<tr>
<td>Universal Description, Discovery and Integration</td>
<td>Universal Description, Discovery and Integration (UDDI) is an open industry initiative enabling businesses to publish service listings and discover each other and define how the services or software applications interact over the Internet.</td>
</tr>
<tr>
<td>UNICODE</td>
<td>Unicode is a computing industry standard allowing computers to consistently represent and manipulate text expressed in most of the world's writing systems. For the purpose of this section, systems must be able to receive, store, process and return data containing any character covered by UNICODE UTF-8.</td>
</tr>
<tr>
<td>Service Oriented Architecture</td>
<td>Service Oriented Architecture (SOA) is a business-centric IT architectural approach that supports integrating your business as linked, repeatable business tasks, or services.</td>
</tr>
<tr>
<td>Unified Modeling Language</td>
<td>Unified Modeling Language (UML) is a standardized general-purpose modeling language that can be used to specify, visualize, modify, construct and document the artifacts of an object-oriented software intensive system under development.</td>
</tr>
<tr>
<td>AJAX</td>
<td>Ajax, sometimes written as AJAX (shorthand for asynchronous JavaScript and XML), is a group of interrelated web development techniques used on the client-side to create interactive web applications or rich Internet applications.</td>
</tr>
</tbody>
</table>
## Referenced Documents

<table>
<thead>
<tr>
<th>Reference number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref1</td>
<td>ISO 17799 standard</td>
</tr>
<tr>
<td>Ref2</td>
<td>Information Security Management System and Regulative for technical and organizational means for providing security and confidentiality for personal data manipulation published in official gazette no 7/05 and 103/08</td>
</tr>
<tr>
<td>Ref3</td>
<td>&quot;XML-Signature Syntax and Processing&quot; issued by W3C consortium</td>
</tr>
</tbody>
</table>
Notes

It should be noted that all findings listed below are based on what has been obtained from interviews conducted during June 2009 with social service experts, IT experts and legal experts from institutions involved in the process of providing social welfare service. In some cases findings are quite general and not definitive as a result of a current change of governmental and internal legislative and hence, comprehensive review should be conducted at the time of the detailed system design.

To allow a fair and unbiased decision regarding a successful vendor, no specific platform or software development tools are described by Purchaser in this Bidding Documents. The Purchaser is trying to avoid the fact that, by dictating a particular software development tools, indirectly we would be requiring a particular operating system, DBMS and hardware that is best integrated with the technologies that these tools provide.

Objective

The objective of this document is to be used as a technical specification document for Social Welfare Services Information system (SoWelSIS). This document is a part of a tender dossier for Development and Implementation of SoWelSIS for the Ministry of Labor and Social Policy (Institute for the Social Activities) and the Centres for Social Work.

SoWelSIS environment

At the moment, there is no unique IT management system for evidence of social services beneficiaries and social services. It should be noted, that although, they are very similar, there is also no standardized procedure or organizational hierarchy that can be find among the Social Work Centers (SWCs). SWCs currently use simplified desktop based system for keeping analytical records needed by the Institute for social activities. The operational work is mainly managed by hand or via standard
office application tools. None of these databases are connected across SWCs or with the Institute for social activities in Skopje.

The lack of a centralized database creates many operational problems. Most significant operational problems are:

- Lack of validation on offered services allows for the possibility of multiple requests for services in behalf of recipients in multiple locations around the country.
- Lack of high-level security measurements on local databases allows for illegal database modifications without the possibility for tracing these changes.
- Current database structure does not allow any data queries for analytical, budgeting and forecasting reporting.
- The need for a common repository for Business rules is needed to control indiscriminately approvals/denials of services and easy system maintenance and system updates with new policies and procedures.

Figure 1. The Social Welfare System Organization

The Social Welfare Service Information System (SoWelSIS) is working in environment which is represented on figure 1. The boundaries of the environment can be spread to all governmental institutions in the country, but at the moment, the SoWelSIS will be installed at the following entities: Social welfare centres, and Institute for social activities. It has to be mentioned that the Ministry of labour and social policy will determine premise where the data server of the SoWelSIS will be kept.
The Centres for Social Work will use the SoWelSIS for their everyday work. They will be mainly concerned with the input of operational and analytical data regarding the social welfare service beneficiaries. Since they operate with private and sensible data, the need for the security policies and user roles for accessing and manipulation with that data is obvious.

The number of expected user of the SoWelSIS is given with the following figures: The Institute for Social activities will have 20 users, the Centre for Social Work in Skopje approx 120 users, while all the other 30 centres will have up to 40 users or approx 1340 users in total.

The Centres for Social Work have workstations working mainly under MS Windows XP, although some of the workstations are working under MS Windows 98 and MS Windows 2000. Some of them are organized and managed in workgroups. Generally the equipment can be qualified as low to mid class PC equipment.

The communication infrastructure within the SoWelSIS will be based on IP protocol, and on the basis of that choice all sites nationwide will be supported by appropriate TCP / IP connection. The network infrastructure will ensure the connection between the components provided in the various domains and the other systems that need to interface to the SoWelSIS. The following table present the network traffic that will be provided to different Centres for Social Work.

Table 1: Centres for Social Work planned internet traffic

<table>
<thead>
<tr>
<th>Social Welfare Centre</th>
<th>Cite Code</th>
<th>Required traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Berovo</td>
<td>BE</td>
<td>Un</td>
</tr>
<tr>
<td>Bitola</td>
<td>BT</td>
<td>Un</td>
</tr>
<tr>
<td>Debar</td>
<td>DE</td>
<td>Un</td>
</tr>
<tr>
<td>Deltchevo</td>
<td>DE</td>
<td>Un</td>
</tr>
<tr>
<td>Deltchevo - rt.</td>
<td>DE-RT</td>
<td>50</td>
</tr>
<tr>
<td>Demir Hisar</td>
<td>DH</td>
<td>25</td>
</tr>
<tr>
<td>Gevgelija</td>
<td>GE</td>
<td>Un</td>
</tr>
<tr>
<td>Gostivar</td>
<td>GO</td>
<td>Un</td>
</tr>
<tr>
<td>Gostivar - rt.</td>
<td>GO-RT</td>
<td>25</td>
</tr>
<tr>
<td>Kavadarec</td>
<td>KA</td>
<td>Un</td>
</tr>
<tr>
<td>Kavadarec - rt.</td>
<td>KA-RT</td>
<td>50</td>
</tr>
<tr>
<td>Kitchevo</td>
<td>KI</td>
<td>Un</td>
</tr>
<tr>
<td>Kitchevo - rt.</td>
<td>KI-RT</td>
<td>25</td>
</tr>
<tr>
<td>Kotchani</td>
<td>KO</td>
<td>Un</td>
</tr>
<tr>
<td>Kratovo</td>
<td>KT</td>
<td>50</td>
</tr>
<tr>
<td>Kriva Palanka</td>
<td>KP</td>
<td>Un</td>
</tr>
<tr>
<td>Krushev</td>
<td>KR</td>
<td>50</td>
</tr>
<tr>
<td>Kumanovo</td>
<td>KU</td>
<td>Un</td>
</tr>
<tr>
<td>Makedonski Brod</td>
<td>MB</td>
<td>50</td>
</tr>
<tr>
<td>M. Brod - remote</td>
<td>MB-RT</td>
<td>25</td>
</tr>
<tr>
<td>Negotino</td>
<td>NE</td>
<td>Un</td>
</tr>
<tr>
<td>Negotino - rt.</td>
<td>NE-RT</td>
<td>25</td>
</tr>
<tr>
<td>Ohrid</td>
<td>OH</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>
### Social Welfare Centre

<table>
<thead>
<tr>
<th>Social Welfare Centre</th>
<th>Cite Code</th>
<th>Required traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prilep</td>
<td>PR</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Probishtip</td>
<td>PO</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Radovish</td>
<td>RA</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Resen</td>
<td>RE</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Shtip</td>
<td>ST</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Skopje</td>
<td>SK</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Skopje-Center</td>
<td>SK-CE</td>
<td>50</td>
</tr>
<tr>
<td>Skopje-Gazi Baba</td>
<td>SK-GZ</td>
<td>50</td>
</tr>
<tr>
<td>Skopje-Karposh</td>
<td>SK-KA</td>
<td>50</td>
</tr>
<tr>
<td>Skopje-Kisela Voda</td>
<td>SK-KV</td>
<td>50</td>
</tr>
<tr>
<td>Skopje-Shuto O.</td>
<td>SK-SO</td>
<td>50</td>
</tr>
<tr>
<td>Skopje-Tchair</td>
<td>SK-TC</td>
<td>50</td>
</tr>
<tr>
<td>Skopje-MLSP</td>
<td>SK-ML</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Skopje-SPIL</td>
<td>SK-SP</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Struga</td>
<td>SG</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Struga - rt.</td>
<td>SG-RT</td>
<td>50</td>
</tr>
<tr>
<td>Sveti Nikole</td>
<td>SN</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Tetovo</td>
<td>TE</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Valandovo</td>
<td>VA</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Veles</td>
<td>VE</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Veles – remote</td>
<td>VE-RT</td>
<td>50</td>
</tr>
<tr>
<td>Vinica</td>
<td>VI</td>
<td>50</td>
</tr>
<tr>
<td>Institute for social activities</td>
<td>SK-DZ</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

**Total access points unlimited traffic**: 28

**Total access points limited traffic 25 GB**: 5

**Total access points limited traffic 50 GB**: 14

**Total access points**: 47

At the time this specification is written, the required traffic is in the process of purchasing. The table 1 describes traffic that will be available to the different entities in the SWCs. The solution providers will have the information about the access bandwidth at the time they sign the contract.

Database Server of the SoWelSIS will be placed at the premises of the Ministry of the labour and social policy, while the back-up and data warehousing system will be placed at the premises of the institute for the social activities. The bidders should clearly state the needed bandwidth to those two institutions in their offer.

The SoWelSIS should define the services that under regulation would be able to other governmental institutions in the forms of web services. At this time, only the connection to the SPIIL information system under the control of the Ministry of labour and social policies should be provided.

The information needed from this system is:
The type of financial benefit used by the beneficiary, if any, determined by beneficiary’s personal id (in Macedonian language: maticen broj) and his/her name. This is an exchange of information that must be provided.

The scanned documents that have been processed by the SPIL system, if any, determined by the beneficiary’s personal id and his/her name. This is an exchange of information that should be provided if feasible and supported by corresponding security policy determined by the SPIL system.

The general data for the social service beneficiary’s already processed by the SPIL system, if any, determined by the beneficiary’s personal id and his/her name. This is an exchange of information that should be provided if supported by corresponding security policy determined by the SPIL system.

The information that should be made accessible to the SPIL system is:

The type of social service used by the social beneficiary, if any, determined by beneficiary’s personal id (in Macedonian language: maticen broj) and his/her name. This is an exchange of information that must be provided.

The scanned documents that have been processed by the SoWeLSIS system, if any, determined by the beneficiary’s personal id and his/her name. This is an exchange of information that should be provided if feasible and supported by corresponding security policy determined by the SoWeLSIS system.

The general data for the social service beneficiary already processed by the SoWeLSIS system, if any, determined by the beneficiary’s personal ID and his/her name. This is an exchange of information that should be provided if supported by corresponding security policy determined by the SoWeLSIS system.
SoWelSIS general requirements

According to SoWelSIS environment, SoWelSIS should:

- allow optimization of the costs of operational management of the system:
  - basic operating costs such as hardware, software licenses, personnel management system;
  - costs related to the management of access systems at the national level;
  - costs related to managing the single space administration of the system
  - maintenance costs and/or replacement of hardware components;
  - costs required for the development of new functionality.

- alignment of the solution to the current state of technology

- possibility to integrate and manage new types of data such as images, photographs, fingerprints and, more generally, biometric information.

In order to achieve these objectives the SoWelSIS must meet the following general requirements listed below:

FR1: The SoWelSIS must be based on the Web based System Architecture. This approach typically include -

1. Web Server – for rendering the client presentation.
2. Application Server – for support the service logic.
3. Database Server – for supporting data management.
4. Security and/or user domain server – for integration of various security policies

The solution provider is free to change this application roles distribution according to the recommendation of specific development and deployment environment he is offering for the solution.
Computing Hardware Specifications

FR2: Within SoWelSS project, Database, Application and Web servers will also be procured. Bids must clearly state offers for this hardware equipment.

Software Specifications

FR3: Application should use XML as a data interchange methodology

The SoWelSIS should implement XML as a data interchange process. The use of XML would provide the following advantages:

- A standard means to exchange information between different systems
- A standard way to query data from different systems

The solution provider must state the standards and protocols deployed for the purpose of electronic data exchange,

FR4: SoWeLSIS must provide a website

The SoWelSIS needs to incorporate informative website to the citizens of this country explaining the available Social Services and documents they need in order to apply. The web site should enable single sign on for all functionalities of the system.

System Management, Administration, and Security Specifications

The Security module must cover all functionality required for the System Management, Administration, and Security of the SoWeLSIS.

Security and Identification Requirements follows:

FR5: The application systems must log all transactions performed.

FR6: Transaction log information must provide date, user and module information.

FR7: User and support staff access to the application must be password protected.

FR8: The application must require user and password identification to be accessed, as well as digital software signature signed internally.

FR9: Use of encrypted data must be implemented through standard specifications (SSL, TLS)

FR10: System Security policies must be implemented on a role-based methodology
FR11: Central database system and a national level access interface. The client access systems should have features uniform for all administrations. The system should have single point administration;

FR12: the system must ensure the security, availability, integrity and the constant updating of data in the database;

FR13: the system must provide a backup database system located in a different place in order to ensure an adequate level of availability and disaster recovery, at the same time optimizing the system response time by routing of data traffic between the two sites; both sites are able to perform all the functions in charge of the central system ensuring high reliability as each site plays Disaster Recovery feature.

FR14: The system should provide some kind of data warehousing capability enabling fact access to the data and generation to different reports from multidimensional tables.

FR15: The system must be able to receive and store data in either format (UNICODE Unicode and transliterated) and be able to handle queries using the transliteration rules in both directions. This means that a query received as “ß” must be able to match “ß” (original spelling) and “S?” (Transliterated spelling) and a query received as “S?” must be able to match “ß” and “S?” Data must always be returned to Users in the way it has been originally entered by its owner.

*Migrating data from existing databases to SoWelSIS*

FR16: Those who respond to tender have to indicate appropriate and feasible scenario of migration of existing databases into the new system. The existing system is presented in a form of Fox-Pro application.

**User Types**

The SoWelSIS have the following users:

Internal users will access the system from within the premises of the Centers for Social Work. There are three sub-categories of these users: social specialist, social specialist from another center, and manager. The first internal user sub-category (social specialist) fulfills operational and analytical data for the social welfare beneficiary. Those users can be grouped depending whether they work together on the social benefited dossier, and can retrieve, and manipulate data from the groups they belong to. The second internal user sub-category is social specialist from another center. He/Her can request data from beneficiary dossier belonging to another welfare center. The last internal user sub-category of this group is manager, which can access all dossiers from the centre he is managing, and give permissions for access requested from another centers or external users.

The external users are defined as such from the point of view of the SoWelSIS. This category of users can be also divided in three sub-categories. First external user sub-category is general public users that can only access information approved by “public access” policy, which, at this moment is only
static information about the social welfare services and corresponding documents needed for the potential users of those services. Second external user sub-category is the members of governmental institutions (e.g. Ministry of interior, Ministry of labor and social policies, and Institute for the social activities). They should have polices that allow access to the cumulative data, but as well personal dossier after the approval of the social center manager. The only user of this sub-category that has to be implemented at this time is the “institute for social activities” user. Third user sub-category are the users of the SPIl system which can access certain information based on the security policies implemented in SoWelSIS in a form of web services offered to them. All access to the information for the external users must also be logged in the system logs.

The third user type is system admin. The system administration users, can create users, define user roles, define new security polices; create access rights to the data and e-forms, etc. The sub category of these users (if needed) can dial with different system logs (access to the log activities, system logs, exceptions logs, system error logs).

FR17: The solution must integrate previously described user types, the possibility for their grouping together with corresponding roles as minimum requirement. If needed, the solution provider can further detail this list.

Social Welfare Service Information System Architecture

At access level SoWelSIS will have two possibilities: external users using web based access over https enabled internet connection, and internal users using web based access over intranet. It should be noted that there might be more than one system that will be access using the same client machines (at least SPIl system and some back office systems). Thus, the security enabled web based access is recommended for the intranet users as well.

FR18: There are three important processes that must be considered within SoWelSIS: e-request processing for external users, e-forms processing (both subject of SoWelSIS) and communication with SPIl system. The solution provider must describe in the bid in detail how it will implement these processes in terms of technology, and developing environment used.

The SoWelSIS processes should communicate among themselves and with the end users (both internal and external) by establishing service modules. Service modules group common activities from the SoWelSIS software perspective. Service modules can be invoked by other service modules, by end users, or by SoWelSIS system itself. The following services modules can be identified, but the solutions provider can further detail or accommodate this list to the specific solution feature set:

- Filling request forms,
- Filling operational forms,
- History tracing,
- Notification,
• Identifications,
• Validations,
• Determination of the access level
• Status check,

FR18: The service modules must be implemented as minimum service modules for solution provider. Each of these service modules can be further subdivided according to the nature of its usage.

All service modules communicate with the SoWelSIS data centers, which are responsible for availability and integrity of all SoWelSIS data.

The minimum service modules are elaborated in detail in the following text.

Filling external forms is represented by a standard web interface that enables multiple dimensions queries over SoWelSIS data. The solution provider should consider accessing replicated database for the purpose of those queries enabling Centres for Social Work more bandwidth to operational data from the central database.

Filing e-forms can be divided in two general categories: filling analytical forms, and filling operational forms. Both of these form types share same data regarding the social welfare service beneficiary. They are also further divided according the specialization of the social service they support.

FR 19: The solution providers are encouraged to use Model–View–Controller (MVC) architectural pattern in order to separate business logic from user interface considerations, resulting in an application where it is easier to modify either the visual appearance of the application or the underlying process rules without affecting the other. This will be helpful since the end user interface should look exactly as the paper form documents provided as annex to this dossier.

History tracking deals with access to the previous versions of the SoWelSIS social welfare beneficiary data, or SoWelSIS system log, enabling information, what has been changed, and by whom.

Notification is a short message that is produced as a result of the system setting, or fulfilling some action from the different SoWelSIS users. Examples of such notification include but are not limited to: notification for not verified social welfare service beneficiary identification number, notification for the request for social welfare service beneficiary data(that needs to be approved in order to be processed), notification that access to information is approved or rejected, and so on. More details on these notification messages is given in section explaining the use case scenarios of the SoWelSIS.

Identifications is a service that identifies system users, external and internal SoWelSIS users, social welfare service benefiters, for the purposes of access control, verifying data, etc.

A validation complements identification service when needed. It is used to approve access to certain information. The typical scenario can be user account validation.

Determination of the access level should be used for deployment of security standards as a part of identification/validation process.
Status check service is used for internal SoWeISIS system control in order to provide integrity, persistence and availability of the SoWeISIS data.

Figure 2 represents logical architecture of Social Welfare Service Information System.

Figure 2. Logical architecture of the Social Welfare Service Information System

Figure 3 explains the proposed physical architecture of the SoWeISIS.

FR20: The external users should be separated from the internal users with the help of firewall. The solution providers can offer another solution as long as that solution provides the same level of security protection for data access.
Presentation level for all users should be implemented with the set of standard web enabled technologies. The integration of different services offered to the SoWeiSIS users is established via integration level that deals with register of services offered to internal and external users, transactions, message format validations and EDI standards deployed as well as log tracking and security policies. The services can be made available to different categories of internal and external users by make it accessible via set of service registers. One possible solution for such scenario is presented on figure 4.

According to this scenario, we propose the SOA (service oriented architecture) to be deployed for implementation of the end SoWeiSIS services. The SOA is implemented as a set of orchestrated web services. All services available to all users are described in UDDI register. The internal services are published in internal UDDI register, while external services are published in external UDDI register. This approach gives flexibility and easy maintenance to the service offered to different parties which is very important taking in mind constant need for improvement in the field of legislative dealing with social welfare services.
Figure 4. SoWeISIS Service modules provider scheme on integration level

When the service is approved as available, its description can be found in the form of WSDL protocol using SOAP messages. This protocol is used to generate notifications and model user interaction using MVC enabled e-forms to the end user.

FR21: The bid must deploy orchestrated web service at integration level. The bidders are free to accommodate the standards and protocols that best match the platform of integration they choose.

FR22: The bid must explain how the integration level will be deployed in the SoWeISIS.
FR23: The bid must elaborate in detail, how, with the help of web services, the needed information will be available to external users.

The service modules are grouped according to their functionality in the SoWellSIS into application modules. The proposed application modules of the SoWellSIS are e-forms module, management module, security module and DB connection module. More details on the interconnection of those application modules are given on Fig 5- Proposed application infrastructure of the SoWellSIS.

Fig 5. Proposed application infrastructure of the SoWellSIS.

The application modules are e-form (portal) modules, security modules, management module and DB connection module.
Fig 6. Elementary use case step for internal user.

The application module is responsible for generation of user interfaces and user interaction. It has to check the user roles, and active security policies in order to deny or approve user access to requested data, and generate the needed user interface. The system management module can change default settings of those interfaces in order to add new fields in certain form, change form
header and footer, or established simplified workflow if needed (by establishing no more than two steps approval procedures – which are not needed at this moment). Management module also deals with new users, user groups and their roles. Security model defines and controls all system and user logs, and generate new security policies. DB connection module determines which data request to be forward to which Database. It is recommended that report generation module (especially for external users) should access replicated data and/or data warehouse. The DB connection module might also be responsible for implementing DB replication and disaster recovery policies (if that is not offered by database management system on system level).

FR24: The solution providers can change the application infrastructure (number, organization and interchange of information among the modules) according to the specific software features they will offer, but must explained the application infrastructure in detail in their offer.

If the proposed design is accommodated by the solution provider, all user scenarios for internal, external and administrative users, can be represented as a consecutive repetitive steps that fully or partially implement the elementary step.

**Use case scenario: elementary internal user step**

The use case scenario for the external user is given on Figure 6.

Internal users model all the interaction with system as a result of certain event (new social beneficiary has entered the room, the system has generated certain approval or denial, the specialist has to perform analyses of his/her group dossiers, etc.). He has to request access to certain data from certain dossier in order to perform his intent. Once this request is logged in the system, if the user role is validated by certain user policy, the corresponding e-form is invoked and fulfilled with the data from database. If the security module deny the request on the basis of privilege to access the information, the external request to the system is generated (this transform the internal user to external and is covered in different elementary step). If the certain dossier is entered for the first time, internal users become the responsible for this dossier.

In the case of the need for additional form to be invoked (special social welfare service to be added to the social beneficiary), it triggers the new event and the whole process is reputed. If for example, in that case the beneficiary has to show some documents, the user can check whether such document already have been brought (and possibly scanned) in the SoWelSIS or SPIL system (in the second case it triggers external user scenario).

**USE CASE Scenario for the external user**

The use case scenario for the external user is given on Figure 7. It principal, it is similar to the previous user scenario, with the addition that the data flow is done according different security polices, and the services are registered in different registers. It can be easily checked that the external user use case scenario covers at least two important scenarios:

- External user needs some summary data
• External system has provided requested data (e.g. financial social service type)

Fig 7. Elementary use case step for external user.

Use case step for administrative user
Fig 8. Elementary use case step for administrative user.

The use case scenario for the external user is given on Figure 8. It implements simple, one–step authority approval process. In this case the authority decision is also logged in the system. It also integrates the modification, and addition of the new security policies (or users, user roles, etc…)

FR25: The bid must explain how it plans to implement basic user scenarios explained in the technical specification in terms of deployed security, policies, logging of the activities, technology used and protocols deployed, and discuss why they differ from the explained ones, if that is a case.
Data Model

The Social Work Centers (SWCs) in the country currently administrates number of different social services beneficiaries and social services offered to them. The documents given in attachment to this document are document templates used for operative and statistical work for the SWCs and they list all services and data that need to be kept for all of them, which give an insight of the scope and volume of data for the SoWelSIS.

FR26: Document templates used by the social service specialist should be used as a UI design for the specialist – end user of the SoWelSIS.

FR27: In addition, the information whether certain activities within the service has been applied as a directive from the Institute for the social activities must be kept. The activity of giving directives can be treated as given from the external user that works at the Institute for Social Activities. It is then approved by the corresponding social center manager, and shows as notification to the social center specialist (internal user), who then applies it to the social welfare beneficery.

This information can be later used for generation of different reports as well.

FR28: The information structure should follow one dossier principle. Each social service beneficiary must have one dossier. Different social welfare services can be added to that dossier.

FR29: It must be enabled that many internal users can have access to the same dossier, thus forming a group working with that dossier.

FR30: It must be enabled that social services beneficiary can be group in beneficiary groups (family, children, marriage, etc.). In this case, for analytical purposes, group can be treated as one dossier or set of individual dossiers (depending on the needed report)

The nature of the reports and the treatment of social beneficiary groups depends on the social welfare service types: There are five general service types groups:

- marriage and family related services
- children and youth related services
- custody of children without parents and parental care services
- adult welfare services
- social Inclusion services
- people with disabilities in physical or physical development services

The groups of service types are not strict and they can be further divided or expanded with new groups. For each of those groups there are operational and analytical information that has to be kept. Sometimes, the operational operation might include documents issued from different governmental institutions (domestic and foreign).

FR31: The SoWelSIS must be designed in such way that it can keep and manipulate scanned documents related to certain dossier and/or social service type.
The information related to general social welfare type is added to the general information of the social welfare beneficiary.

The general data base model is represented on fig 9.

![Diagram of General SoWelSIS data model](image)

**Figure 9. The General SoWelSIS data model.**

**FR32:** The social welfare beneficiary dossier should be identified by personal ID number. However, in the case, the social beneficiary is not able to provide information about its personal number, the system must crate temporal identifier to be use as a unique ID of the social beneficiary and create notification, which will remind internal users to provide official personal ID. Once the personal ID is requested it triggers external event in order to check whether the social beneficiary has already benefited from different social center, or SPIL system.

**FR33:** The solution providers must propose unique ID system that will enable social specialist (internal users) to work with persons depending on the emergency of situation, and not availability of documentation they have. These include not only persons that not have valid identification documents, but foreign citizens, etc..
FR34: The code tables should be used whenever possible. The solution provider must explain which code tables it will be used, what will they enable, and how they can be modified. (e.g. The code tables of towns related to the social welfare centers)

Reporting Tools
FR35: SoWeISIS reporting module must be able to handle the following constraints:

- **Date of Birth**
  A query can be a year, a month and year or an exact date. Where the date of birth is not known exactly, it is often replaced by the presumed year of birth.

- **Range of Serial Numbers**
  Data is sometimes stored as a range, e.g. AW900-AZ1000. The system should be able to find an item within the range based on a specific number, e.g. AX050.

- **Near-Match and Misspellings**
  The systems must be tolerant of misspellings and be able to match misspelled names, names spelled according to different conventions or names entered only in part (e.g. ‘Aleks’ matching ‘Aleksandar’).

- **‘Name’ Convention**
  The reporting and query tools offered must have the Flexibility to handle among others the following common types of issues:
    - Some cultures will place the surname first while others place the surname last so that the surname/name order can be confused.
    - Some cultures have compounded surnames, which may be used in full or in part.
    - Conflicts between current name and name at birth

- **Free text searches**

FR36: A searching may result in a large list of possible “Hits”. Both systems must be able to handle the following issues (amongst others) that often result in long lists:

- **Common names**
  Name searches can result in a large number of Hits. Additional discriminators may need to be added to refine the results, without increasing the risk of a false Hit or a false no-Hit.

- **If the Near-Match algorithm is too broad**, a pruning process can be implemented to restrict the number of Hits returned to the User.
FR37: The bidder must describe the searching tools and how these tools will meet the requirements in terms of functionalities, performance and scalability. In addition, the solution must offer the Users the possibility of customizing ranking rules and defining cut-off points.

FR38: Platform independence is an important requirement.

FR39: The reporting tool should provide OLAP or OLAP like functionality

- Easy management and distribution of reports
- Easy integration with data sources, portals, and applications using open standards
- Multi dimensional expression language that provides a rich and powerful syntax for querying and manipulating the multidimensional data stored.
- High performance, interactive analysis of large or small volumes of information
- "Dimensional" exploration of data, for example
  - For each general service type summary report that groups the social beneficiaries by sex, age interval, education type, region they have current address, region they have original address (region can be postal code, municipality), employment status, nationality or any other general information
  - These reports can be calculated on basis of social welfare centers, group of Centres for Social Work or national level
  - The cumulative numbers on national level has to calculate one beneficiary as one beneficiary, regardless to the number of centers that have served him (due to the change of his/her current address). On the other hand, that person should be calculated in each of the centers that gave him/her any kind of social service
  - The social activities given by the directive from the Social Activities institute has to be used as a filter to all queries.
  - The non validated social beneficiaries (problems with personal ID must be used as a filter to any query)
- High-speed queries through the use of aggregate tables
- Possibility for Integrated scheduling and authentication
- Advanced calculations using the calculation expressions
- Extensive customization capabilities using APIs, web services, or modification of templates, business rules,
• Integrated audit logging to track user activity, performance, and content access

System Management

FR40: SoWeISIS should integrate the tools necessary for the system management, exiting as market standards, in order to allow remote management of each component of the system. The bid must contain the description of the set of tools that will be used in the SoWeISIS and their features.

The set of system management tools should be:

• open to the collection of any information relating to the monitoring of the system; configurable through setting standards to determine which events and system components manage and monitor;
• uniform, to allow inspection of every component of the system regardless of its basic technology;
• integrated, in order to allow the interchange of information between different tools and to allow management through common interfaces.

The system management tools will be used by different categories of users with different access permissions. Among the categories are:

• Administrator (with the property set configurations, and access permissions);
• Manager (with read-only access to information on auditing).

FR41: The procedures for system management must include:

• Capturing of system activities and time;
• Capturing of internal system events (including reports of planned operating systems, any type of application messages, fault of the hardware and software provided);

FR42: The System Management information must be stored in a uniform, centralized way, and must be maintained on-line for at least two years and then off-line. The information stored off-line should have the possibility of being restored in a quick and efficient if necessary.

FR43: The system management tool should be able to perform:

• consultation and analysis of information collected;
• producing reports on the monitoring system on the basis of monthly and annual information;
• generate statistics for the comparison of information collected during a period equal to 5 years;
• relate each user to every single event registered;
• verifying the state of communication between each component of the system

Storage Requirements
The architecture of the SoWelSIS includes the need for use of a storage for storing databases.

FR44: The solution provider must take into account the following considerations:
• it is currently anticipated that the SoWelSIS will permanently store the multimedia data (scanned versions of the Social welfare service beneficiary documents);
• databases will have to provide the storage needed for auditing logs.

Security
The characteristics of high criticality and confidentiality of SoWelSIS data require a high level of safety. It is essential that all aspects of security are considered, evaluated and integrated in the provided solution.

The requirements stated in this dossier are based on the ISO 17799 standard, Information Security Management System and Regulative for technical and organizational means for providing security and confidentiality for personal data manipulation published in Official Gazette no 7/05 and 103/08.

The functional requirements of safety are:

FR45: The bidder must describe the Security Model he plans to deploy. User roles and responsibilities must be clearly defined, identified and periodically subjected to inspection.

FR46: The bidder must be provide periodic review procedures for monitoring including alarm management, escalation procedures and archiving for all logged data

FR47: The confidential or sensitive data in the database should be stored as encrypted data.
Areas that need to provide adequate levels of safety are:

1. Policies and Operating Procedures
2. Applications
3. DataBase
4. Server
5. Infrastructure Network

The main security policy rule is that information that the person that has created the social beneficiary dossier is the responsible for the dossier. However, since in the process of determining what kind of services will be offered to the beneficiary, and the follow up process, more specialists from the social welfare services might be included, they all should have the access to the dossier. In that way, the team related to the dossier is created.

Sometimes the beneficiary might change the location of residence (not necessary his/her address) and in that case, he/her can be under jurisdiction of different social welfare centre. It that case, the dossier up to certain date can be accessed, after the prior approval of the social welfare centre manager from the other specialist from the other social welfare centres.

The request for service might also be permanent, in which case the approval confirms the transfer of the dossier owner to different centre. In that case, the prior social welfare center has right to access the beneficiary information by the time the beneficiary was under the jurisdiction of the centre, but for the period after the transfer of jurisdiction, the approval has the required.

FR 48: The bidder must explain the procedures and policies for encryption. It must be clearly defined: where, what data or components, and should be used when encryption, how the system will manage encryption keys and how will the system react in case of problems on the data encrypted or in the event of loss by certificate or encryption keys.

**Authentication**

FR 49: All operators, administrators and managers must be authenticated to systems and applications. In order to minimize the risk of unauthorized access is required to implement an authentication system strong "two factor authentication based on verification at two levels:" something "that you own and" something "that the user knows.

The possible ways for this implementation might be hardware token or software based private key. The authentication should be done by cross-checking two codes typed and addressed by the authentication server.

**Access Control - Management Roles and Profiles**
FR 50: The rights of access for all users must be configured based on roles and profiles managed centrally.

The SoWelSIS should be based on centralized authorization system that will be responsible for management and maintenance of roles and profiles. Any other systems that were interfacing SoWelSIS should have its own mechanism of authentication and authorization, which must notify the SoWelSIS-profile role in the use of applications.

FR51: The procedures for interfacing (trust procedures) are support for the definition and verification of actions to maintain the proper level of security while avoiding compromises related to deficiencies of external systems. The solution provider must provide an adequate and detailed service reporting for monitoring and review of access to SoWelSIS.

Data Encryption

FR52: The appropriate levels of security and data integrity can be obtained by providing encryption and signing of messages exchanged to external applications. The recommendation "XML-Signature Syntax and Processing", issued by W3C, can be taken as a reference point in defining the mechanisms signature message applications. The similar mechanism might be used for storing sensitive Social welfare beneficiary private data in the database system.

Hardness of Operating system

In order to prevent exposure to known or vulnerability to exploitation of default configuration settings, it is essential that DataBase Server systems undergo following activity:

FR53: Depending on the type of operating system must be checked at least the following:

- removal of the default profiles for authentication;
- changing the default settings of the manufacturer for standard passwords;
- disabling of unnecessary services on the server;
- network access allowed only to authorized users;
- use of safe administrative tools (eg ssh to Unix or Linux);
- activation of the tracking systems, and storage of logs on different machines;
- removing or disabling sample script provided by the manufacturer.

FR54: With regard to database systems should be checked (and prevent from):

- use of generic profiles from the DB;
- for use of network ports dedicated and non-standard connection to the DB;
• unauthorized access from external applications that exceed the security application (eg through ODBC or call direct SQL queries);

FR55: Common to all systems must be verification and implementation of upgrades and new versions by the manufacturer (update, service packs and patches) with periodic inspections.

FR56: A system protection is required for the introduction of additional tools for the control of vulnerability (eg: Automatic Vulnerability Assessment), intrusion detection and host-based type firewall.

FR57: The workstations using SoWelSIS must be configured according to the operating levels and security provided by the policies of "interfacing safe" (trust security). In particular, a centrally managed system with antiviral systems properly configured and maintained with the latest patches and SW versions must be installed.

Confidentiality of Communications

All communications between the SoWelSIS to the end user workstations and other systems (SPIL system) will be confidential and protected. It is therefore necessary that this traffic is encrypted so that, even if intercepted messages, which can not be accurately interpreted.

FR58: In order to ensure confidentiality of communication, the system must implement mechanisms such as SSL encryption application, or TLS-based products (eg RSA, PGP) implemented specific protocols based on the TCP port communication.

It is assumed that the provider of external connectivity ensures protection of communications.

Network Security

FR59: The control of passwords and installation and management of firewall systems should be provided. It is also recommendable to provide a complement to traditional firewall protection, in form of mechanisms to detect attacks, intrusion and strong authentication.

Logging and Monitoring

FR60: Actions that has to be logged are:

• All database modification requests (Creation/Update/Deletion);
• All queries;
• All answers to queries, including no-Hits;
• Data dumps, database restorations and repairs;
• All communications between the SoWelSIS and the other systems;
• All User and logons and performed actions, as well as failed or unauthorized logons.

FR61: The central logs must allow administrators to trace actions in time, and identify the Users who performed each action, and if necessary help this Users to identify the End-Users.

FR62: Because no action can be performed if it cannot be logged, the Logging system must be permanently available and a secondary/backup Logging repository must be foreseen.

FR63: Access to the Logging data must be restricted to administrators and log accesses will also be logged. No Logging data can be modified. No logging data can be deleted before its legal expiry date.

FR64: Each User must be able to review the logs of all actions performed by themselves or actions performed on their data. Logs of User transactions may need to be returned to the User and provision should be made to make this task simple.

FR65: Logs can also be used for statistics purposes. Reporting and analysis functionalities or tools must be developed to provide the reviewer(s) with usage exceptions and workable information.

Tenderers must describe in their tender offer how they intend to implement all Logging requirements.

Backup and Disaster Recovery Strategies

FR66: Solution providers must provide backup procedures to ensure the restoration of unity (natural or individual partitions) if necessary. These backups must be performed each time a change is made at the operating system or application.

FR67: Solution providers must define and generate test procedures involving applicants to restore, that will cover all areas subject to backup. Each of these tests will produce a report and, if it fails, will be made all the corrective actions provided for in the shortest time possible.

NON – Functional Requirments

Standards and Methodologies

NFR1: Industry Open standards and methodologies should be used rather than company-specific methods. The use of standards and methodologies is relevant for all areas of the project such as: Project management methodology, Solution analysis and design, Development, Security.
Documentation

Solution providers should produce detailed documentation for all project deliverables. The documents must be properly organized and indexed, and include the following types of file:

NFR2: Technical and functional specifications: every component part of the system must be accompanied by technical and operating specifications. In particular, communication interfaces between the various components, the data model, and standards used, should be described;

NFR3: Hardware: hardware equipment that comprise the system must be accompanied by appropriate documentation describing the procedures for installation, configuration, usage and troubleshooting;

NFR4: Software: For software, both commercial and custom, which contribute to the realization of the system, solution provider must provide documents that describe the procedures for installation, configuration, usage and troubleshooting. For the various software components specially designed for the project solution provider must supply detailed technical documentation describing the various modules;

NFR5: User Manuals: the system must have user manuals that explain the use of the system and cover the following profiles of use: Systems Administrators and Different Users who access the services;

Below is a description of each stage in the SoWelSIS development process as a reference to which stages on the SoWelSIS need to be documented. Vendor compliance is required in terms of documenting each step of the process.

NFR6: Any additional requirements that are further requested, must be documented using UML (Unified Model Language).

NFR7: This conceptual design must provide us with a formal model of the database table structure of the SoWelSIS.

NFR8: This phase involves determining which kinds of data and operations will be accessible to which user groups, and designing the appropriate human-computer interfaces for these groups. (e.g. access rights tables constructed for different user types and the decision to support different screen forms) has to be documented.

NFR9: Prototyping aim to cover the major functions in the requirements specifications, but will omit mostly the error checking and finer details required for the final version, using a small set of sample data. A prototype document should define a graphical implementation (screens) of the proposed system, without business logic implementation.
NFR10: Once the Purchaser’s Management has accepted the application prototype, the final application design will be completed including all validations and other details not included on the prototype version. In this phase, the actual code for the production version should be created.

NFR11: Testing and validation document should describe data and procedures used for testing and validation

Number of Copies - Six(6) sets of the entire documentation (including one paper copy of each type of document) must be provided at no cost to the vendor

Distribution - All documentation must be revised by Purchaser and approved prior to be printed in a hard-copy form and release to the users.

Copyrights - Purchaser must keep the rights to reproduce parts or the whole documentation in any form. In addition, Purchaser also keeps the right to release the documentation, including source code and other system information to any third party.

Electronic Document Support - All documentation must be produced on MS-Word running windows operating system.

**SoWelSIS acceptance procedure**

**Application performance indicators**

A well-designed database and a thin client implementation are important factors in the evaluation of the performance of a web application. In addition validations and error checking, as well as other techniques (e.g. AJAX) when possible, must be deployed at the client-side thus minimizing network traffic.

Below are described the minimum performance requirements of the acceptance tests

- The interactive queries of application systems end users must processed within 5 seconds.
- All on-line reports must be generated within 2 minutes. Otherwise, the system must recommend generating a report in batch processing mode.

**Operational Acceptance Tests**

Successful completion of the contract will be measured through a series of formal test performed on all modules to be delivered by the vendor.

The acceptance test will demonstrate that the supplier has met each and every requirement specified and agreed within the contract and has delivered all required reports and documentation and an effective operational system.
Acceptance test will be carried out at three different levels:

1. **Unit Test**

   For each module and sub module described under the business modules, users would provide a test scenario to the vendor so it can be used to guarantee the acceptance test. For each user interface, the vendor would need to provide a list of process and function that involves the test.

   For each event, the following information must be provided -
   - Precondition requirements
   - Expected results
   - Obtained result
   - Acceptance of the test
   - Identifications of errors presented during the test
   - Observation of the person performing the test

2. **Integration test**

   At the completion of the entire system, the Integration tests will be conducted under a series of expected workloads.

3. **System Qualification test**

   This test will be performed on completion of the integration tests and involves end-to-end testing of all elements of the system in a simulated system.

   Test Conditions: A test environment requires a separate machine with same operating system as the production environment and database instance.

   Unit test for operational forms
   - Easy friendly interface
   - Optimal time to perform processes and database retrieval
   - Verify GUI (Graphical User Interface) like combo boxes, content and operation.
   - Confirm required fields
   - Check validation of data fields formats
• Confirm agile navigation
• Verify the existence and operation of help, cancel and retrieve buttons
• Check the operation of the open and close button
• Verify format of database records
• Check that all required fields are present on the form
• Validate the service process
• Confirm the printing Overview Document process

Statistics Module Unit test
• Check validation of data fields formats
• Confirm required fields
• Verify GUI (Graphical User Interface) like combo boxes, content and operation.
• Optimal time to perform processes and database retrieval
• Easy friendly interface
• Check the operation of the open and close button
• Verify the existence and operation of help, cancel and retrieve buttons
• Confirm agile navigation
• Verify format of database records
• Check the existence of all required reports
• Validate the data of all required reports

Security Module Unit test
• Verify GUI (Graphical User Interface) like combo boxes, content and operation.
• Verify the existence and operation of help, cancel and retrieve buttons
• Confirm agile navigation
• Optimal time to perform processes and database retrieval
• Easy friendly interface
• Check the operation of the open and close button
• Check validation of data fields formats
• Confirm required fields
• Check the existence of the required menu options for Person, Position, User, Profile, Module, Profile, Application log and System
• Validate that the security module is implemented under a Role-based methodology
• Validate the ability of adding code tables to the system
• Check the application sign-on process
• Check the security to access unavailable modules for a defined security role
• Validate Database and non-database error handling
• Verify the existence of error handling procedure for application generated errors
• Perform audits on transaction log
• Perform checks on how vulnerable security mechanisms are in placed

SoWElSIS CBMIS Database Schema
Based on described processes and data fields requirements, the following checks and validations will be performed.

• Verify that all supporting database tables that are required are implemented following standard database principles (3-4 Normal Forms when possible)
• Check the existence of necessary indexes
• Check for existence of data corruption while interrupting transactions to the database
• Check of validity of data
• Check for the necessity of triggers
• Check performance of data retrieval
• Check performance of transactions to the database
Application Prototypes

- Peer review and user evaluation will be conducted for the evaluation of the screen and interfaces with the system.

- Application Prototypes will be reviewed and compared to up-to-date screen designed.

Integration Tests

The objective of the Integration test is focused on times response for processes, primarily on retrieval and insertion to the database and for reporting.

Benefit Module Integration test

The following table describes the required load testing

Table 2: load testing parameters

<table>
<thead>
<tr>
<th>Type of Load</th>
<th>Interactive Load</th>
<th>Congruent Load</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single</td>
<td>1 e-form submission (repeated 10 times in intervals of 5 seconds)</td>
<td>None</td>
</tr>
<tr>
<td>Light</td>
<td>1 e-form submission (repeated 30 times in intervals of 3 seconds)</td>
<td>None</td>
</tr>
<tr>
<td>Medium</td>
<td>100 applicants submissions activated at intervals of 1 second (repeated 30 times after intervals of 5 seconds)</td>
<td>5 - 15 workstations</td>
</tr>
<tr>
<td>Heavy</td>
<td>200 applicants submissions activated at intervals of 1 second (repeated 30 times after intervals of 5 seconds)</td>
<td>15 - 25 workstations</td>
</tr>
</tbody>
</table>

The following table describes the required load testing for all reports

Table 3: Load testing parameters for reporting issues

<table>
<thead>
<tr>
<th>Type of Report</th>
<th>Amount of Records</th>
<th>Congruent Load</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single</td>
<td>500 records search on a 2 database table relationship</td>
<td>None</td>
</tr>
<tr>
<td>Level</td>
<td>Records Search</td>
<td>Relationship</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Light</td>
<td>500 records search on a 5 database table relationship</td>
<td>None</td>
</tr>
<tr>
<td>Medium</td>
<td>3000 records search on a 2 database table relationship</td>
<td>5 - 15 workstations</td>
</tr>
<tr>
<td>Heavy</td>
<td>3000 records search on a 5 database table relationship</td>
<td>15 - 25 workstations</td>
</tr>
</tbody>
</table>

**SoWelSIS maintenance**

The Supplier will be expected to provide a long-term support capability covering:

- Provision of direct support of the system - under warranty, at no additional cost to the Purchaser - for one year after obtaining Operational Acceptance. In this period the Supplier must handle all reported errors, bugs and change management. Should it be required for any part of the system to be modified during the warranty period, all modifications must be implemented by the Supplier free of additional charge.

- System maintenance capability for a minimum of 48 months after the warranty period expires.

- Any updating and further development of the application software that may be required to meet evolving business requirements.

- Ongoing advice and guidance in the use of the system

- The Supplier must provide a HELP DESK to be available for the Purchaser at least during its working hours, that is from 8am until 5pm each working day determined as such by the Government

- This should cover both application functionality and IT technical support as appropriate.

**Warranty Service and Post Warranty Service:**

- Warranty Period: twelve month after the Operation Acceptance

- Post Warranty Period: twelve month after the Warranty Period
• During the warranty and post warranty period, the SoWellSIS most certainly would experience software problems.

(a) All problems that will occur during the Warranty period will be handled by the Supplier free of charge, and all problems that will occur during the Post Warranty period will be charged according to prices calculated in the Supplier’s Bid - Recurrent Cost Form.

Below is a description of the possible scenarios that the vendor must contemplate and be able to address regarding changes on the application.

**Types of problem requests:**

- Requests due to situations on which the system is malfunctioning or seriously decreased its performance.
- Requests due to bug/errors in the Information System
- Requests for adjustments of the Information System due to changes in the legislation;
- Requests for adjustment of the Information System due to the facilitation of the operation;
- Requests for supplementing the functionality which does not change the basic technology. These requests include minor changes of final facilities, which do not require additional project designing.

**Classification of system errors**

Fatal Errors - These are described as errors which disable the operation of all or most of the processes of the system.

Serious Errors - These are described as disabled functionality required to perform processes with initial performance requirements.

Minor Errors - Errors which interrupt certain activities no critical to processes.

**Types of Maintenance**

Warranty (in warranty and post warranty period) covering maintenance due to any errors/bugs/malfunctions on any part of the system.
During the warranty period (1 year) and the post warranty period (1 year) the vendor must warranty the system of any errors classified above.

**Services provisions under warranty and post warranty**

Below is described the different types of services expected from the vendor regarding warranty.

- Installation of mandatory patches or upgrades to third-party or COTS software provided by the vendor
- Correction, if applicable, to data lost or changed, due to malfunction components of the system
- Installation of changes, upgrades or any other modifications to the system following change management processes, which includes version control, test environment and retrofitting modifications (perform by the vendor) to the existing software version.

**Information contents of the request**

A change request form, provided by Purchasers or the vendor, should be used to keep track of the software requests. Below is a description of the information this request should include

1. Specification of the window screen, menu option or process that identifies the problem.
2. Description of the error, including a short description of the event, data or behavior.
3. Date of the software change request
4. Name of the user requesting the software change request
5. Name of the Manager approving the change
6. Name of the Vendor Software engineer assign to work on the change
7. Time of receipt of the software change request
8. Classification of the Software change (Urgent/non-urgent)

**Classification of Software Change request**

Urgent change -

This problem is considered urgent if it disrupts the operation of the system in such a way that can be considered 'down-time' (no processing). This type of a change must be
commenced within a period of three hours with notification to the Purchaser within 6 hours to report the progress and status of the problem.

Non-urgent change -

This problem is considered non-urgent if it does not disrupts the operation of the system in such a way that can be considered 'down-time' (no processing), allowing processing to continue. This type of a change must be commenced during an 8 hours period following a notification to the Purchaser when the changes would be completed.

Distribution of changes

Test

The supplier shall, prior to the delivery and distribution of the Software change, test all modifications and upon a successfully test procedure; issue a quality certificate, containing name of the Software Engineer that participated in the test and a description of the test environment.

Distribution

Changes could be delivered electronically or using any type of media, but must be first deployed on the testing environment to allow for proper Purchasers testing. Upon Purchasers testing, the Software change request would be consider accepted and by consequence closed, or not accepted and therefore outstanding.

Consultations

The vendor must allow for user support or consultations related to the software solutions by phone, email or at the vendor premises.

User support:

It is acceptable that a problem resolution person be available during working hours to report any problems with the system. The coverage of the Help Desk provided by the vendor must be the same as the Warranty and Post Warranty periods - 1 year. In the case
that nobody is available to answer the call, a problem call need to be returned back to the vendor in no more than 24 hrs.

Technical Assistance:

Technical Assistance is required from the Supplier during the Warranty and Post Warranty periods.

Technical Assistance must be provided on site using Supplier’s personnel. The assistance given on site by the Supplier’s personnel should include fault finding, fault-fixing, adjustments, monitoring of the proper operation of the system, implementation of improvements, on the job training of Purchasers staff, software support and familiarization with the use of documentation.
Additional Services

Training

The solution provider must include following training in the offer:

- system administration training for two persons;
- administration of application training for two persons;
- Use of the system training for ten persons.

These training services should be provided by qualified instructors with hands on experience on the subject of training.

The courses relating to the administration of the system will be aimed at training of the technical personnel who will be responsible for the management of infrastructure hardware and basic software and administering the system.

The courses relating to the application will be aimed at training of the personnel who will be responsible for the management of application processes and support for end users of the system.

The courses on the use of the system will be aimed at training the focal point which in turn will train end users (according to any different categories / types) of the system.

The training must also include the drafting of the plan on organizing (rent, infrastructure requirements, number of sessions planned duration of individual sessions)

Startup Service

The support services relating to starting up the new system should include:

- Support activities in system Administration, in order to minimize impacts on the use of the new system;
- Monitoring components of the system activity through the use of system management tools provided in architecture
- Support services should cover the period from the start of operation of the new system to one year of usage.
**Maintenance**

This service is related to hardware and software on site that needs corrective maintenance. The initial maintenance should cover period of two years beginning from the operational start of the system.

The maintenance includes:

- hardware / software support on site
- all the activities to be undertaken during the partial or total withdrawal of all equipment under maintenance
- diagnostic of equipment/application through appropriate tools in case of malfunctions
- removing the cause of the failure and restore normal function of systems

Responsive time for the maintenance should be indicated in the offer. The maximum responsive time should be no longer than 5 hours. The solution provider support must be available during the working hours of the end users.
SoWelSiS Project Management Requirements

The following subsections provide a list of requirements related to project management, methodology, documentation and other procedures.

**Project Methodology**

A Solution provider has to provide a detailed project methodology that covers:

- Project management;
- Design and analysis methodologies;
- Software development;

The methodology must be professional, widely used and based as far as possible on standard methodologies for carrying out mid-scale IT projects.

**Security**

**Assessment of Personnel**

All personnel who will be involved in the project must hold a positive security clearance for working with sensitive data prior to working in the project.

**Communication**

All exchanges of information by email (i.e. documents, Deliverables) shall be made in a secure way (e.g. encrypted) if not otherwise agreed with the contract.

**Storage of Documents**

Storage of documents on premises/equipment must be secure and will be liable to a security Audit.

**Project Management Team**

At contract signature, the successful tenderer will confirm the composition of the Project Management Team. For any clearly identified role within the team, there must be a replacement indicated. The following team positions must be identified in the tender offer It is expected that at least the following roles are required from the successful tenderer:

- A Project Manager;
- A deputy Project Manager

Deputy Project Managers must be able to assume the responsibilities of the Project Managers in their absence and the Project Manager and deputy Project Manager of a project can never take a leave of absence from work simultaneously.
At contract signature, the successful tenderer will confirm the composition of the whole project team and other key actors. All project team members are expected to be involved for the whole duration of the project. It is expected that at least the following roles will be dedicated to a person(s) from project team:

- A Chief Architect;
- A Security Manager;
- A Quality Manager.

The project manager will act as the contact point between the successful tenderer and the UNICEF office.

The tasks that must be performed by the project team include:

- To deliver, within 30 days from the signature of the contract, a Project Master Plan;
- To produce and maintain the Project Quality Plan;
- To produce Monthly Progress Reports;
- To produce and maintain Risk Management Plan;
- To participate in various meetings;

**Project Management Board**

The Project Management Board (PMB) will be chaired by the UNICEF Project Officer and will consist of at least the following persons:

- The UNICEF project team and other representatives of the Commission’s Services, if required.
- The successful tenderer’s project Manager.
- Representatives from the Participating Administrations.

The PMB will hold its first meeting around the time of the delivery of the draft Project Management Plan. It is expected that PMB will meet once a month, though the meeting frequency may increase or decrease depending on the needs of the project. Other members of the successful tenderer’s project team may be required to attend as needed.

PMB meetings will normally be held in the premises of UNICEF.

**Communication and Reporting**

The spoken and written language of all communication will be English and/or Macedonian. All Deliverables, reports, drafts etc. must be delivered in English unless otherwise agreed. Daily contact per telephone or e-mail must be possible between the teams of the UNICEF and of the successful tenderer.

**E-mail Communication**

In order to facilitate communication between the Project teams, the successful tenderer must provide a functional e-mail address. The successful tenderer must guarantee that any
incoming mail is either fully answered within 2 working days or answered with a holding reply indicating when an answer might be expected.

Communication and Co-ordination with Third Parties

Due to the complexity of the project it could be necessary for the successful tenderer to contact and collaborate with third parties, after prior Authorisation by the UNICEF Project Officer.

In such case, a copy of any relevant communication between the successful tenderer and the third parties must be sent to the relevant Project Manager or Project Officer at the UNICEF.

Monthly Progress Reports

At the beginning of each month, a monthly progress report must be sent to the UNICEF with details of the work carried out in the previous month. The report must also contain a description of the work to be performed in the next month, clearly mentioning the milestones. The Monthly Progress Report must report at least:

1. List of the tasks originally planned during the reported month;
2. Progress during the month: for each task mentioned in the list of planned tasks, a short description of the contribution to the progress is given:
   - Description of the activities carried out;
   - Description of the results achieved;
   - Comments on ongoing tasks when appropriate;
   - Justification of any deviation from the originally planned tasks.
3. The Deliverable Tracking Matrix showing the:
   - Planned delivery dates;
   - Foreseen delivery dates;
   - Actual delivery dates for review and for acceptance;
   - Along with justification of any differences between planned and actual dates;
   - Provisional budget provision’s consumption for non-fixed price tasks;
4. Problem and issues: problems and/or issues met during the execution of the tasks. Overruns of tasks and/or difficulties for meeting agreed target end-date must be explained here.
5. Task planned for the next month: an extract of the project time plan, listing all the tasks that are planned to start or to be continued during next month.
6. Request for action: the requests for action must be listed with their reference number and title, to which short comments can be added as relevant.

**Project Phases**

The Project Phases are different from the Contract Phases and are not related to the Acceptance Procedures and payment terms.

The exact schedules of work on these phases should be specified in the tender offer. The initial project implementation can be been divided into three main project phases:

- **Project Phase I - Detailed analysis and technical Design**, resulting in full system specifications. The results of this phase must include a full set of interface specifications defining the communication processes

- **Project Phase II - Development, testing and deployment** of the systems (development/training/testing/pre-production/production environments).
  - Prototype application must be accepted in Skopje and one additional site. The prototype application has all the functionalities of the SoWellSIS that work on just two locations.
  - The interoperability with other systems must be accepted

- **Project Phase III - Migration, Integration and Support to Users**
**Description of the Information Technologies, Other Goods, and Services**

The Bidder must provide detailed descriptions of the essential technical, performance, or other relevant characteristics of all key Information Technologies, Materials, other Goods, and Services offered in the bid (e.g., version, release, and model numbers). Without providing sufficient clear detail, Bidders run the risk of their bids being declared non-responsive.

To assist in the bid evaluation, the detailed descriptions must be organized and cross referenced in the same manner as the Bidder’s item-by-item commentary on the Technical Requirements. All information provided by cross reference must, at a minimum, include clear titles and page numbers.

The Bidder must provide an item-by-item commentary on the Purchaser’s Technical Requirements, demonstrating the substantial responsiveness of the overall design of the System and the individual Information Technologies, Goods, and Services offered to those Requirements.

The following table (Quality Evaluation Criteria Table) is provided to help the Bidder organize and consistently present its Technical Bid. For each of the following Technical Requirements, the Bidder must describe how its Technical Bid responds to each Requirement. In addition, the Bidder must provide cross references to the relevant supporting information, if any, included in the bid. The cross reference must identify the relevant document(s), page number(s), and paragraph(s). The Quality Evaluation Criteria Table does not supersede the rest of the Technical Requirements (or any other part of the Bidding Documents).

**Quality Evaluation Criteria Table**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bidder’s technical reasons supporting compliance:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bidder’s cross references to supporting information in Technical Bid:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Estimated time needed for the SoWelSIS implementation**

The Bidder must provide an estimated time frame for every foreseen activity and/or phase.

<table>
<thead>
<tr>
<th>Time slot</th>
<th>Activity</th>
</tr>
</thead>
</table>

**SoWelSIS Financial implications**

**Estimated budget summary**

The Bidder must provide an estimated budget.

Table 4: estimated budget summary

<table>
<thead>
<tr>
<th>Information system components</th>
<th>estimated budget in USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database, application and web server</td>
<td></td>
</tr>
<tr>
<td>Backup server, data-warehouse server</td>
<td></td>
</tr>
<tr>
<td>Administration server, software farewell server, Access control server</td>
<td></td>
</tr>
<tr>
<td>Software licenses, operating systems costs</td>
<td></td>
</tr>
<tr>
<td>Software development</td>
<td></td>
</tr>
<tr>
<td>Data Migration</td>
<td></td>
</tr>
<tr>
<td>Server System Software Maintenance (two years period)</td>
<td></td>
</tr>
<tr>
<td>Application Software maintenance (two years period)</td>
<td></td>
</tr>
<tr>
<td>System Administration Training for two persons</td>
<td></td>
</tr>
<tr>
<td>Administration of application Training for two persons</td>
<td></td>
</tr>
<tr>
<td>Application Software Training for 10 persons (Trainers)</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
</tr>
</tbody>
</table>
Evaluation criteria

The following criteria will be used to evaluate all bidders.

Table 5: Evaluation Criteria

<table>
<thead>
<tr>
<th>Component</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price</td>
<td>20%</td>
</tr>
<tr>
<td>Quality</td>
<td>50%</td>
</tr>
<tr>
<td>References for similar projects</td>
<td>20%</td>
</tr>
<tr>
<td>Delivery period</td>
<td>10%</td>
</tr>
</tbody>
</table>

ANNEX to this document are 29 groups of forms that are filled out by the Centers for Social Work. These forms will represent the core of the E-forms Module (operational data). The forms are related to various social beneficiaries and services that are provided to them.