EVALUATION FRAMEWORK OF A SECURE COLLABORATIVE PLATFORM FOR THE JUDICIAL CO-OPERATION ENVIRONMENT

ROBERTA RAIMONDI  
Information Systems Dept  
SDA Bocconi 
Via Bocconi n. 8, 20136  
Milan – Italy  
Ph: +39.02.5836.6301, Fax: +39.02.5836.6893  
roberta.raimondi@sdabocconi.it

LEONARDO CAPORARELLO  
Institute of Organization and Information Systems  
Bocconi University  
Viale Isonzo n. 23, 20136  
Milan – Italy  
Ph: +39.02.5836.2619, Fax: +39.02.5836.2634  
leonardo.caporarello@unibocconi.it
ABSTRACT

This paper refers to a real case (Security E-justice European project) in which the authors proposed a framework to evaluate an innovative web based collaborative platform. It concerns the judicial process environment and relative information that flows between different actors and at different levels.

The evaluation of such collaborative platform represents a very critical factor to allow its own success and to obtain the commitment of the targeted users.

We considered the analysis of two relevant dimensions that derive from the following areas:

1. process and organizational aspects,
2. functional and technical aspects.

Considering the strong connection of the paper with a real case, the authors allocate this paper in the Section 01 – “Paper relevant for practice”.

INTRODUCTION

The SecurE-Justice platform, proposed in the SecurE-justice European Project¹ provides a solution that assists the people involved in the judicial system to achieve their work faster, using state-of-the-art technological solution to manage the flow and exchange of information between different actors, at different levels, in a secure and reliable way, to support the judicial process, starting from the investigation phase and ending with the final judgment of the trial phase without modifying the normal course of the process as specified by the law. The communication used during the ‘investigation phase’ will be achieved in an asynchronous way (not-real time communication) because of the nature of the investigation that will be executed at different stages, locations, times and involves different people not necessarily connected online always at the same time to achieve results. While the communication used during the ‘trial phase’ is achieved in a synchronous way (real time communication) to allow the actors during the debate of a trial to exchange

information immediately without the need to be located in the same place (delocalized trial).

The proposed solution is a *collaborative workspace* to organize the work of involved people in dedicated online judicial *workgroup(s)* and to allows them to work in a collaborative manner, exchanging content (documents), ideas and experiences online.

The solution offers a *collaboration centric workflow driven working space*, following particular standards and state-of-the-art technologies and it is a standard Web based solution.

Authors are involving in the task of evaluation of the project, with the following objectives:

- the development of an agreed evaluation plan across the demonstration sites, and which fully meets the requirements of determining the European added value of the project;
- the evaluation of the demonstrated products from a technical and operational perspective.

**METHODOLOGY OF THE WORK AND FRAMEWORK PROPOSED**

The overall evaluation comes from three main categories of assessment, defined as the following:

- functional coherence of the system (that may be viewed as a Collaborative Portal, running in a protected and secure context): this means that the system functions are useful to answer at the process requirements and the user needs,
- user acceptance,
- adherence to the main and more applied technological standards (in terms of architecture, operating systems, security….).

We evaluate also the security environment in terms of existence of security functionalities, the respect both the technical security standards and the national security and privacy normative and the existence of a security atmosphere.

Our framework considers the analysis of that aspects from the following aspects:
- organizational, including the evaluation of the user perception and the process impact;
- technical, that – from a generical to a specifical approach – aims to evaluate the coherence and the effectiveness of the system (from a user and process perspective) both by a security and functional view.

Besides specifying objectives, the evaluation plan also describes how the team will organize the evaluation flow, who the subjects of evaluation are, and what kind of tools (and indicators) will be used in the several steps of analysis.

Consequently, this document makes an overall view of the testing methods, necessary for obtaining valuable indicator values, that are to be used by the demonstration sites. In addition to these common testing methods, each site may undertake additional tests based on specific local needs or services.

Our framework takes into account that this activity can be used as a real and pragmatic tool to design or modify or improve new functions of the system (i.e. more personalized and more useful): evaluation would improve both in its effectiveness (with more specific indicator and tools) and its direction of growth (from the prototype level to a complete system).

This decision is consequence of the observation and rationalization of user reactions in case of introduction of a new information system: very high and more stressed in presence of an interactive interface.

For a system with a great interaction between users on an electronic interface, the common and more used flow for a project design and development has little differences if compared to the classic waterfall methodology proposed by Royce in 1987. Moreover, in the design of the evaluation process we considered the following critical aspects:

1. there is a wide variety of very different communities of users, with related different needs and requirements;
2. for some of these communities this is probably the first experience with a technological system to support their specific processes.

For these reasons, our evaluation is “transparent” in order to consider the different knowledge and ability of the user using a new technological system, “trans-european”
to save the specific context and organization of the Countries and also is “coherent” with the contextual ability of users: this ability rises with experience in using the system. Consequently, like in a project flow, our process of evaluation is structured and planned as showed in the Figure 1.

![Reiteration with a more complex framework](image)

**Figure 1: The methodology proposed**

### EVALUATION OF ORGANIZATIONAL ASPECT

**Evaluation of user perception**

This part aimed to evaluate the user “feeling” (user friendliness or usability) in the use of the system. The user perception given by a new information system may be influenced by ones knowledge, competence and familiarity with this one. Two factors have influence on this perception: education (and/or training) and experience. For this reasons, the user perception is evaluated, firstly, immediately after the training process and, secondly, after a brief period of use.

In this evaluation we have also included some generally considerations regarding system context and external interface features.
From our point of view both these areas are connected to the presentation tier of system architecture. In this specific area, we will consider also the ability of the system to be multi-channel and multi-devices, personalized and contextualized.

We use some technical measurements (especially for the multi-channel and multi-devices requirements, in the section dedicated to the technical evaluation) and a checklist for the users, inspired by a specific approach named “user centered design”, created by Jacob Nielsen. The relevance of interface in a design of a web system (like our SecurE-Justice system) has inspired in the last few years a lot of standards ISO.

The latest ISO standard is the ISO 13407 (1999) that came directly from the Nielsen’s framework and is called “Human centred design processes for interactive system”. This standard inspired part of our evaluation and the definition of our user questionnaire, that will include some questions related to this standard; we would like to note that this is only an indicative reference.

The questionnaire dedicated is structured in three logical sections:

- the first presents a general overview of the usability inspired from the ISO standard;
- the second presents specific questions aimed to evaluate the friendliness of the system: to appreciate the real feeling of the user;
- the third presents some questions personalized and contextualized at the specific situation of the site.

The first and the second sections are sintetized in a checklist adapted from the one developed by Lewis in 1995. Questions may have a scale graduating from 1 (low satisfaction or user-friendliness of the system) to 7 (high satisfaction).

**Process impact**

A detailed description of *roles, people involved, activities and processes* by use of Rational Unified Process (RUP) helped us to define a specific user context, useful to describe and evaluate in each step of the judicial process the system performances. Methodology is described in others deliverables of the project.

The evaluation (that will start with a generic view and proceed with a more specific measure on each functional group) aims to appreciate if the use of the system (or some of its specific features):
from a user point of view (user involved (owner) in a specific step of the process) represents a duplication of time or resource or is (for instance) time consuming or resource consuming;

from an organizational point of view (may organize focus group with all those involved in a process) is more or less difficult to coordinate or “confuse” o more or less quick to perform;

from a contextual point of view, in the specific test site (for instance from an analysis of the specific context – Country…) is a real alternative to the previous system (manual or electronic).

These factors are collected in a checklist, useful to support several Focus Group, in which there will be the participation of all the main groups of users, like police and judicial actors.

In this area we will produce a matrix with the activities in the different phases of process in which we will “capture” the level of improvement during the testing phases with the new system.

EVALUATION OF TECHNICAL ASPECTS

This dimension of evaluation is composed by two parts: “Functional” and “Security”. Functional evaluation is about matching between desired features and functionalities and what is developed. Security evaluation considers the matching between the aimed level of security and the security of the software. Some principles of evaluation are suggested and should be respected: appropriateness, impartiality, objectivity, repeatability and reproducibility, soundness of results.

Functional evaluation
The mainstream of software evaluation usually concerns the fit between software quality and user needs. This fit concerns both explicit and implicit needs about the product, often referred to as software product quality. Quality characteristics are used as attributes to describe a software product. During the history of software engineering several quality models have been developed. In particular, we refer to the ISO 9126 quality model, because it is an international standard that addresses user-
needs of a product explicitly. ISO 9126 (ISO 9126, 1991) distinguishes six quality characteristics:

- Functionality, the capability of the software to provide functions which meet stated and implied needs when the software is used under specified conditions.
  - Suitability - the capability of the software to provide an appropriate set of functions for specified tasks and user objectives;
  - Accuracy - the capability of the software to provide right or agreed results or effects;
  - Interoperability - the capability of the software to interact with one or more specified systems;
  - Security - the capability of the software to prevent unintended access and resist deliberate attacks intended to gain unauthorised access to confidential information, or to make unauthorized modifications to information or to the program so as to provide the attacker with some advantage or so as to deny service to legitimate users.
- Reliability, the capability of the software to maintain the level of performance of the system when used under specified conditions.
  - Maturity - the capability of the software to avoid failure as a result of faults in the software;
  - Fault tolerance - the capability of the software to maintain a specified level of performance in cases of software faults or of infringement of its specified interface;
  - Recoverability - the capability of the software to re-establish its level of performance and recover the data directly affected in the case of a failure.
- Usability, the capability of the software to be understood, learned, used and liked by the user, when used under specified conditions.
  - Understandability - the capability of the software to enable the user to understand whether the software is suitable, and how it can be used for particular tasks and conditions of use;
Learn ability - the capability of the software to enable the user to learn its application;

Operability - the capability of the software to enable the user to operate and control it;

Attractiveness - the capability of the software to be liked by the user.

Efficiency, the capability of the software to provide the required performance, relative to the amount of resources used, under stated conditions.

Time behaviour - the capability of the software to provide appropriate response and processing times and throughput rates when performing its function, under stated conditions;

Resource utilisation - the capability of the software to use appropriate resources in an appropriate time when the software performs its function under stated conditions.

Maintainability, the capability of the software to be modified.

Analysability - the capability of the software to be diagnosed for deficiencies or causes of failures in the software, or for the parts to be modified to be identified;

Changeability - the capability of the software to enable a specified modification to be implemented;

Stability - the capability of the software to minimise unexpected effects from modifications of the software;

Testability - the capability of the software to enable modified software to be validated.

Portability, the capability of software to be transferred from one environment to another.

Adaptability - the capability of the software to be modified for different specified environments without applying actions or means other than those provided for this purpose for the software considered;

Install ability - the capability of the software to be installed in a specified environment;
Co-existence - the capability of the software to co-exist with other independent software in a common environment sharing common resources;

Replace ability - the capability of the software to be used in place of other specified software in the environment of that software.

Each of these quality characteristics is composed by several sub characteristics.

Security evaluation

It is important, firstly, to perform a security risk analysis and identify security issues and requirements. Secondly, it is possible to use a Software Security Checklist (SSC) tool for all phases of the life cycle. The risk analysis and requirements should then drive the rest of the life cycle with traceable and verifiable security requirements throughout.

Moreover the software should have a risk level rating. This rating will provide those using it an awareness of the overall security of the software. This is a critical issue when integrating software with other software and system components, especially in mission and safety critical systems. A security risk rating is a particularly useful item for re-usable code.

We can identify four phases for a SSC:

1. the first phase addresses the software development life cycle,
2. the second phase addresses the external release of software,
3. the third phase addresses tools to assess security during the life cycle process,
4. the forth phase addresses maintenance and decommissioning issues.

Some general information about the Common Criteria (CC) will help understand how to apply its concepts. The CC's official name is "The Common Criteria for Information Technology Security Evaluation", though it's normally just called the Common Criteria.

For the CC, we identify the functional and assurance requirements that would be met by the Target Of Evaluation (TOE). Following there are the major classes of CC security requirements: Communication/Non-repudiation, Cryptographic Support, User Data Protection, Identification and authentication, Security Management, Privacy,

As noted above, the CC has a set of possible assurance requirements that can be selected, and several predefined sets of assurance requirements. Following there are some assurance measures that can increase the confidence others have in our software: Configuration management, Delivery and operation, Development, Guidance documents, Life-cycle support, Tests, Vulnerability Assessment, Maintenance of assurance.

EVALUATION MODEL

We suggest a technical evaluation based on various tools, models and theories. The different instruments are categorized in the following groups:

- Checklists,
- Guidelines,
- ISO documents,
- Scoring evaluation model (matching objectives).

Checklists

The checklists proposed are ISO or de-facto checklist about software security:

- OWASP (Open Web Application Security Project) Testing Project,
- OWASP Penetration test checklist,
- SAC - Security Assessment Checklist.

The checklist contains nine elements. Each element addresses a different aspect of computer security, and each aspect is important for protecting department and university data and computing resources.

After reviewing the detail page for an element, the initial assessment is recorded by checking the appropriate box on the checklist:

- OK - the element has been addressed by department action or policy. All the detailed questions can be answered affirmatively;
- Review - The basic issue has been addressed, but further review is warranted. Not all the detailed questions can be answered affirmatively;

- Requires Immediate Attention - The element has not been addressed or recently reviewed. Few, if any, of the detailed questions can be answered affirmatively.

<table>
<thead>
<tr>
<th>Security Element</th>
<th>OK</th>
<th>Review</th>
<th>R.I.A.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Physical Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Account &amp; Password Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Virus Protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Data Backup and Restoration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Operating Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. Application Software</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g. Confidentiality of Sensitive Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h. Disaster Recovery</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. Security Awareness and Education</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Guidelines and ISO documents
We have selected various guidelines from ISO standards, quality and security projects and market standards:

- ISO 9126 - Software Product Evaluation,
- ISO 14598 - Software Product Evaluation,
- ISO 15408 - Security techniques,
- ISO 17799 - Code of Practice for Information Security Management,
- OWASP Secure programming guidelines.

Scoring evaluation model (matching objectives).
The evaluation model is based on the quantitative evaluation (scoring model) of the achievement of the objectives defined in the previous documents.

Objectives that concern functionality and security issues are provided for each module of the system (User management, Workflow management…).

A set of questions are assigned to each objective (as described in the next chapter). The questions allow verifying and measuring the achievement of the objective to which are assigned. Besides the requirements pointed out in phase of analysis (i.e. document management, user management, workflow management and notification mechanism, full text indexing and search tool, forum/discussion/meeting/chat,
calendar and schedule, messaging facilities, administrative services, system even logging services, remote communication and exchange data services, data storage management, e-folder management, video conference, online help) some qualitative and quantitative metrics are defined to better evaluate each module.

A weight is assigned to each module, so to know its relative importance with respect to the others modules.

The evaluation of each module is based on three/four main factors that will be measured through scales and/or quantitative formulas. Processing the values of these factors allow to determine a synthetic evaluation for each module.

The evaluation model is based on a set of questions that are assigned to each objective of evaluation. The questions allow the validation and measurement of the achievement of the objectives to which are assigned.

We propose an ‘Objective-Questions’ matrix that can be used by testers to evaluate all the objectives. The evaluation can be done on a Boolean scale or a quantitative (10 based) scale.

The questions are divided in three main groups:

- General functionality questions,
- General security questions,
- Objectives-related questions,

the matching between questions and objectives will, then, help to identify which areas need further review or development.

An example of general functionality questions.

<table>
<thead>
<tr>
<th>Quest. ID</th>
<th>AREA: GENERAL FUNCTIONALITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>FUN_001</td>
<td>The interface is i18n (multi language)</td>
</tr>
<tr>
<td>FUN_002</td>
<td>The user interface is usable and intuitive</td>
</tr>
<tr>
<td>FUN_003</td>
<td>The interface allows a simple access to all the features</td>
</tr>
<tr>
<td>FUN_004</td>
<td>The interface includes the access and management of groups</td>
</tr>
<tr>
<td>FUN_005</td>
<td>The system allows to generate a notification for every status change of a content (creation, modify, delete)</td>
</tr>
<tr>
<td>FUN_006</td>
<td>The system indexes text documents</td>
</tr>
<tr>
<td>FUN_007</td>
<td>The system indexes documents meta data</td>
</tr>
<tr>
<td>FUN_008</td>
<td>The system includes a full text search engine</td>
</tr>
<tr>
<td>FUN_009</td>
<td>The data entry system require meta data to users for indexing activity</td>
</tr>
<tr>
<td>FUN_010</td>
<td>Threads and messages in the forum are organized in hierarchical way</td>
</tr>
</tbody>
</table>
An example of general security questions.

<table>
<thead>
<tr>
<th>Quest. ID</th>
<th>AREA: GENERAL SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC_001</td>
<td>The software is installed in a disaster proof data centre</td>
</tr>
<tr>
<td>SEC_002</td>
<td>The system has a dedicated UPS</td>
</tr>
<tr>
<td>SEC_003</td>
<td>The system is configured in high availability mode</td>
</tr>
<tr>
<td>SEC_004</td>
<td>The system includes an IDS (Intrusion Detection System)</td>
</tr>
<tr>
<td>SEC_005</td>
<td>An IRT (Incident response team) is available</td>
</tr>
<tr>
<td>SEC_006</td>
<td>Development and production environment are separated</td>
</tr>
<tr>
<td>SEC_007</td>
<td>The system will be upgraded with security patches and hardening procedures</td>
</tr>
<tr>
<td>SEC_008</td>
<td>The system uses a SSL (Secure socket layer)</td>
</tr>
<tr>
<td>SEC_009</td>
<td>The communication between system components is cryptic</td>
</tr>
<tr>
<td>SEC_010</td>
<td>The system stores only the password hashes</td>
</tr>
</tbody>
</table>

An example of objectives-related questions.

<table>
<thead>
<tr>
<th>Areas and Objectives</th>
<th>Objective is met?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Management</td>
<td></td>
</tr>
<tr>
<td>Document approval: To approve judicial documents and allow sharing with other users involved in a legal process;</td>
<td>YES</td>
</tr>
<tr>
<td>Digital signature: To digitally sign documents stored in the system repository;</td>
<td>NO</td>
</tr>
<tr>
<td>Document encryption: To encrypts documents stored in the system repository;</td>
<td>NEED REVIEW</td>
</tr>
<tr>
<td>Time-stamping: To mark documents with timestamps to specify the original time of the operation (important for non-repudiation);</td>
<td></td>
</tr>
<tr>
<td>Support for multilingual files upload;</td>
<td></td>
</tr>
<tr>
<td>Assigning metadata to different content uploaded.</td>
<td></td>
</tr>
</tbody>
</table>

Finally, we propose a ‘Functions–Objectives’ matrix. It presents for each system function some related questions that can be used to evaluate it.

<table>
<thead>
<tr>
<th>Areas and Objectives</th>
<th>Related Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Management</td>
<td></td>
</tr>
<tr>
<td>Adding, modifying and deleting user;</td>
<td>FUN_002</td>
</tr>
<tr>
<td>Modifying user account and preferences;</td>
<td>FUN_003</td>
</tr>
<tr>
<td>Implementing access rights, providing a flexible mechanism to manage and monitor access rights within a group;</td>
<td>FUN_003 - FUN_004</td>
</tr>
<tr>
<td>Smart Card identification to access the system. Administrative (supportive) services</td>
<td>FUN_003</td>
</tr>
<tr>
<td>Judicial workgroup customization: authorized users may customize various properties of a judicial workgroup (i.e. title, description, contact information etc.);</td>
<td>FUN_023</td>
</tr>
<tr>
<td>User profiles administration: authorized users may modify the existing user profiles defined in the system or create new ones;</td>
<td>FUN_024</td>
</tr>
<tr>
<td>Services administration: authorized users may enable or disable specific services of a judicial workgroup;</td>
<td>FUN_025</td>
</tr>
</tbody>
</table>

**FINAL CONSIDERATIONS**

The collaborative platform was designed for support a process characterized by a substantial flow of structured and unstructured information, shared between several heterogeneous actors, operating into a mutually dependent international juridical regulations and practices.

Our challenge was to maintain the coherence between these followings critical factors:

- the opportunity to introduce innovative technology in a sector characterized by a low predisposition to introduce innovation;
- the high organizational risk connected in some complex environment, like the judicial one.

We used a reiterative methodology, typical of a web based project, and we focused the evaluation on the usability of the platform, especially in the case of the security infrastructure, to allow the maximum effectiveness of the platform proposed in the European project.

Since the project is still in progress, further work is needed in order to expand and complete the set of questions and the matrix presented above (General functionality questions, General security questions, Objectives-related questions, Functions–Objectives matrix).
REFERENCES


