



2004

4th Working seminar on Performance auditing

Lead paper
On

Risk assessment of e-service projects

Marjan Podgoršek, CISA
The Court of Audit of Republic of Slovenia

Content

- 1 Introduction3
- 2 Risk Management approach - framework.....4
 - 2.1 Recommended time frames for performance of the steps in risk management framework.....5
 - 2.2 Inherent risks5
 - 2.3 Risk Categories Assessed6
 - 2.4 Methods for testing control objectives.....6
- 3 Control Objectives7
- 4 Output of the Risk Assessments /Action plans12

1 Introduction

In previous years we have seen fast development of internet related services. From the point of the SAI's process become especially important with the appearance of different kind of e-Government solutions. Such solutions are usually built through projects that in many cases last for years and are joint efforts of numerous institutions and external vendors. The implementation itself usually also involves significant changes in technology, processes and the role that people play. In the end of the day established e-government service has important consequence on life of many if not all citizens.

As such this projects present risk which should be tackled through audit process of SAI's, primarily to achieve early detection of risks and successfully communicate and mitigate them. Beside financial indicators which are usually audited through classical financial audit approach there are also performance dimensions of projects/implementations and connected risks of e-governance solution project which should be assessed in planning, implementation and post implementation phases of the project.

The presented white paper has the ambition to provide base for approaching risk assessments of e-government projects through:

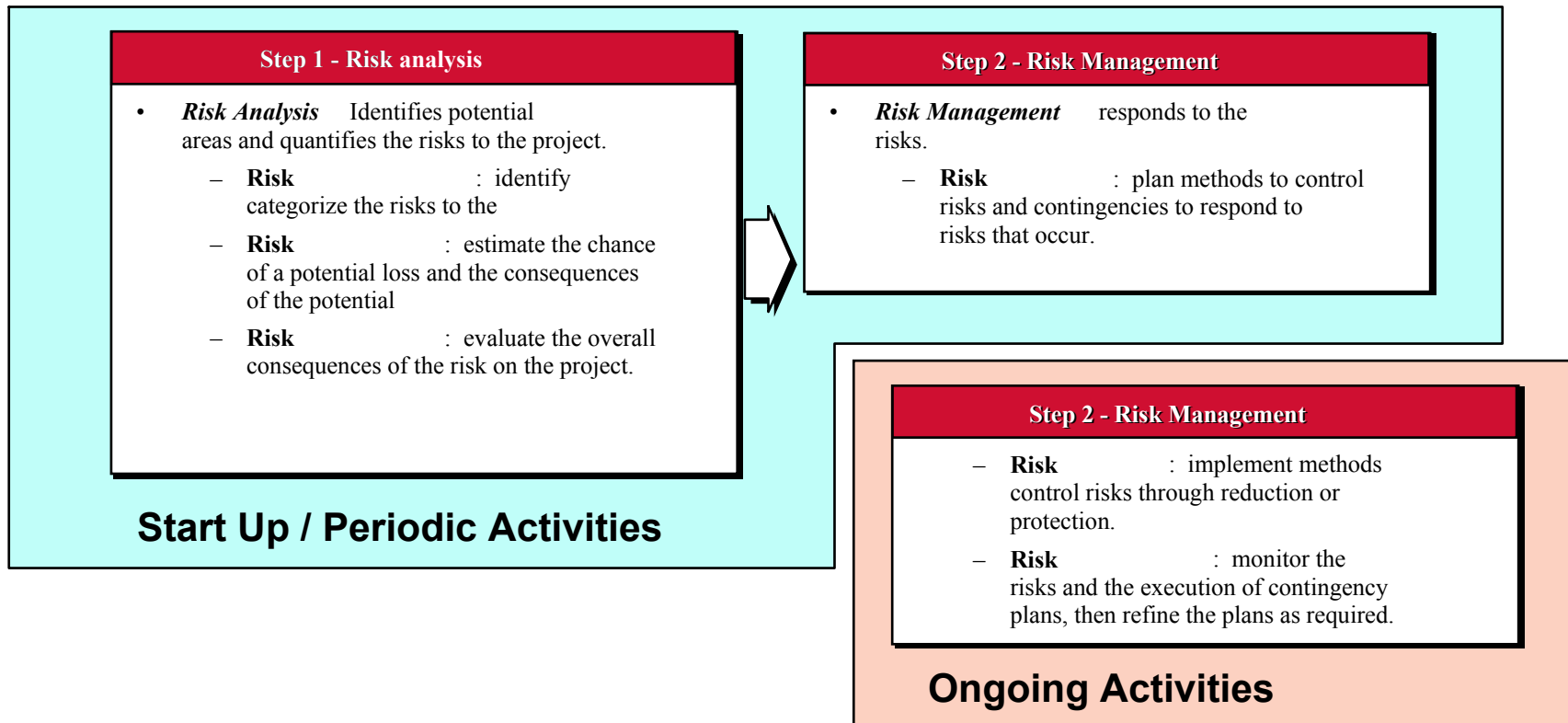
- Definition of the place of risk assessments in risk management approach of e-government projects;
- Definition of basic structure of risk assessment programs;

Additionally this could provide help for the rest of working group to better integrate their papers regarding risk assessment in one consistent group of papers.

2 Risk Management approach - framework

From the point of view of risk management process we can divide activities in two basic steps of activities which relate to each other and should be performed consequently. Steps are interrelated and connected as is seen from the bottom diagram. Despite the fact that in e-government projects we dealing with modern approach to run the citizen services, the approach to risk management of such projects is quite standard one. Major difference to standard life of risk management process is in strong need for formal definition of theoretical and methodical bases for running risk management processes in e-government projects.

That could be best achieved through explicit definition both in budget process requirements as well in specific regulation regarding services that will be supported with e-government systems.



2.1 Recommended time frames for performance of the steps in risk management framework

- A Risk Analysis (i.e. Step 1) should be completed shortly after the project is initiated as well as at regular intervals to account for new situations (every 8 to 10 weeks)
- For each significant risk, the implementation team completes the Risk Planning component of Risk Management (Step 2)
- Risk Control and Risk Monitoring then become ongoing project management activities.

2.2 Inherent risks

For the purpose of relevant scope and objectives of latter risk assessment activities, we should perform the task of risk evaluation through their context and regarding the rank of inherent risk.

For this purpose we should establish in planning phase clear picture about context/environment of the planned e-government system and classify the project regarding the inherent risk of the systems/applications that are involved. As basic guidance for classification/level definition of inherent risk we could use following guidance:

High risk – Systems/applications that:

- Involve large money or significantly important transactions, such that business or government processes would be hindered or an impact on public health or safety would occur if the transactions were not processed timely and accurately,
- Contain highly confidential or sensitive data such that release cause real damage to the parties involved,
- Impact high percentage of the population,
- Are multi-organizational because they can impact the risks to interconnected systems.

Medium risk – Systems/applications that

- Transact or control a moderate or low money value,
- Data items that could potentially embarrass or create problems for the parties involved if released,
- Impact a moderate proportion of the involved information databases.

Low risks – Systems/applications that:

- Are stand-alone,
- Publish generally available public information,
- Result in a relatively small impact on the population.

In the case that specific system falls in more than one of upper categories the classification should be done on regard of highest risk.

2.3 Risk Categories Assessed

There could be many different approaches for dividing the risks. However in proposing the way we followed our previous experience from similar projects and chose to divide the world of risks (and controls) in following five groups/categories:

- **Business Imperative / Motivation to Change**
- **Project Structure & Approach**
- **Technology**
- **People**
- **Project Management & Control**

Actual assessment of the risks related to those groups could be based on testing of control objectives (or part of them). In section 3 we provided the list of control objectives that could be used as base for assessment process and evaluation of the level of risks.

2.4 Methods for performing the risk assessment - testing control objectives

The answer about quality of controls should be collected through examining the documentation, interviews with key project persons, observation of the systems and every day activities. The following scale could be used as base for decision about level of control implementation:

- 1 - Not considered
- 2 - Considered but no action taken
- 3 - Basic action started
- 4 - Partially implemented but not complete
- 5 – Fully implemented

On base of information about control design/implementation the test of control should be undertaken to provide us with sufficient assurance. The extent and deepness of such testing of control performance should take in consideration the context of the environment and the level of inherited risk of the assessed systems/applications.

Through the process special care should be given to the efforts to optimize the usage of resources needed for performance of Risk assessment activities. However, in spite of eventual resource constraints for every control objective we should as minimum get answer about level of control implementation (as base for further decision about testing).

In e-government projects, which usually dealing with significant public funds and sensitive data, legal support through clear and formal definition of minimal requirements regarding risk management (scope, type of reporting, ownership, etc.) in regulation would help in assuring quality of the risk management process.

3 Control Objectives

Following part is intended as base/guidance for designing the scope/objective of risk assessment in e-Government projects. Note that many of these control objectives are also in other type of IT and/or BPR projects. However there are also some that are very specific for e-Government projects (for example subgroup 1.6, 1.7) and therefore should be treated with additional respect.

Risk Category I: Business Imperative / Motivation to Change

Control objectives
<p>1.1 Competitive Service Need</p> <ul style="list-style-type: none"> - Organizational and information technology strategy exists, and Software application fit with the strategy has been established at a high-level - Organizational model has been developed - Position of the organization will be enhanced by the software application - The organization's preparedness for change has been assessed
<p>1.2 Clearly Articulated Vision of the Future Under the System</p> <ul style="list-style-type: none"> - Funding for the cost of initial development and continued operation of established e-government solutions are provided - Organization and IT leadership are fully aligned on priorities and expected outcomes of the project - Priorities and expected outcomes of the project have been communicated across all parts of the organization affected by the system - Enterprise-wide consensus and commitment exists
<p>1.3 Management Commitment</p> <ul style="list-style-type: none"> - Management has active leadership in chartering the project - Management has personal commitment to, and responsibility for project results - Management is committed to allocate superior resources to the project team - Management has an active interest in project progress - An enterprise-wide communications plan is in place and being executed (ongoing) - Ongoing execution of project outcomes
<p>1.4 Costs and Benefits</p> <ul style="list-style-type: none"> - A compelling service case demonstrates costs and benefits - Soft benefits have been conservatively estimated
<p>1.5 User Ownership</p> <ul style="list-style-type: none"> - A project execution plan has been created, and is owned, by users
<p>1.6 Legal Readiness</p> <ul style="list-style-type: none"> - Privacy policies that are consistent and legal is established and disclosed - A method for classifying information and for protecting sensitive information is established to prevent its unauthorized disclosure or access, both internally and externally - Systems involved in E-government comply with legal requirements and ensure the legal standing of transactions - Management established the proper use and enforceability of E-government transactions - Non-repudiation of the parties involved in e-Government transactions is ensured - Legal liability is defined and its definition is available to all parties involved in e-Government applications and/or systems - Proper jurisdiction for e-Government systems is established and the methods and legal remedies to resolve disputes or misunderstandings are stated
<p>1.7 Customer/citizens Readiness and Accessibility</p> <ul style="list-style-type: none"> - E-government systems are made available to the largest degree practicable to all parties expected to be served - Sensitive and confidential data are transmitted only by secure methods when submitted through public facilities - E-government systems provide accessibility for parties with unique requirements based on barriers caused by disability, language or literacy - Fees charged to parties are evaluated for user acceptance - E-government systems and applications provide user assistance and problem resolution

Risk Category II: Project Structure & Approach

Control objectives
<p>2.1 Definition of Scope</p> <ul style="list-style-type: none"> - The scope of service functions and organizational boundaries which will be affected have been clearly defined and agreed to - Approach to reengineering is clearly defined and agreed to - Estimates of impact on the organization, existing systems, and customers/citizens have been developed and incorporated in scope boundaries
<p>2.2 Scope Containment Methods</p> <ul style="list-style-type: none"> - A project progress measurement process is in place - Procedures to identify new issues and resulting "scope creep" are in place
<p>2.3 Mix of Team Member Skills and Authority Levels</p> <ul style="list-style-type: none"> - Teams are comprised of both decision makers and "doers" - Members follow new processes and cross organizational and functional boundaries (users and IT) - Roles and responsibilities of team members have been defined and communicated (including post implementation) - Roles of program management/program leadership are clearly defined
<p>2.4 Full Time Commitment of Team Members</p> <ul style="list-style-type: none"> - Teams are comprised of full-time / fully-committed members
<p>2.5 Effective / Efficient project organization in place</p> <ul style="list-style-type: none"> - One physical team - Service/IT/consulting (including facilities) - Service process focused
<p>2.6 Proven Methodology</p> <ul style="list-style-type: none"> - Methodology is understood and used by all team leaders - Methodology was used to prepare plan
<p>2.7 Issues Management Processes</p> <ul style="list-style-type: none"> - Interdependencies and integration issues across development teams are managed through a formal communication framework - An issues management process is in place, including escalation process - An appropriate Quality Assurance process is in place
<p>2.8 Customization / Gap Closure Strategy</p> <ul style="list-style-type: none"> - Previously proven gap identification process exists - Gap resolution alternatives have been communicated - Gap cost / benefit analysis has been defined and used - Gap approval process has been defined - Development standards have been defined - Resources have been defined
<p>2.9 Approach for Training</p> <ul style="list-style-type: none"> - Processes for training team members have been defined and are in place (including facilities, timing and instructors) - End user documentation and training are derived from To-Be processes

Risk Category III: Technology

Control objectives
<p>3.1 Proposed Hardware, Software, & Communication Hardware Selected and In Place</p> <ul style="list-style-type: none"> - Technology architecture plan - Servers - Applications / Databases - Networks - Desktop - CRP environment - Production environment
<p>3.2 Production Transaction Volumes & Response Times Estimated & Reasonable</p>
<p>3.3 Interfaces Strategy</p> <ul style="list-style-type: none"> - Interfaces have been defined - Interface standards/methodology have been defined - Work standards and schedule with milestone
<p>3.4 Conversion Strategy</p> <ul style="list-style-type: none"> - Previously proven conversion capabilities are available to the teams - Magnitude of conversion effort has been estimated and incorporated into plans - Conversion standards have been defined - Resources have been defined
<p>3.5 Testing Strategy</p> <ul style="list-style-type: none"> - Integration testing - Stress testing - Unit Test
<p>3.6 Ability to Support and Maintain Technology Infrastructure Identified</p> <ul style="list-style-type: none"> - Back-up and recovery - Disaster recovery - Contingency - Help desk
<p>3.7 Global support requirements are addressed</p>
<p>3.8 Process and Systems Integrity</p> <ul style="list-style-type: none"> - Control implications of new systems and process have been considered - Application security strategy has been addressed and designed
<p>3.9 Clear application release strategy is established</p> <ul style="list-style-type: none"> - Clearly defined approach to software modification and software change control process - Vendor relationships for H/W and S/W are stable

Risk Category IV: People

Control objectives
4.1 Knowledge of Business/Industry <ul style="list-style-type: none">- There is a clear understanding among the team members of the service needs driving the project- There is a clear understanding of the As-Is and To-Be processes among each process team
4.2 Knowledge of Software Application <ul style="list-style-type: none">- Teams have an understanding of the functionality of the application- Team members, especially client team members, have been exposed to the type of system being implemented- If reengineering is taking place, reengineering professionals have a good understanding of software capabilities
4.5 Knowledge & Experience in Directing & Controlling Projects <ul style="list-style-type: none">- Project manager(s) have a comprehensive understanding of project management disciplines- Project Management is adequately experienced with implementation projects for the specific application
4.6 Knowledge of New Technical Environment:
4.7 Project Team Integration with Organization <ul style="list-style-type: none">- Team members are highly respected by their peers- End users are connected to, and have buy in to the project- Members are enthusiastic and positive about being part of the teams
4.8 New HR model defined and agreed to <ul style="list-style-type: none">- New organization structure defined and agreed to- New roles and support requirements have been identified- Transition plans are in place and agreed to
4.9 Organization Change Management Methods & Techniques <ul style="list-style-type: none">- Project team members have an understanding of the methods and techniques of change management (people management skills)- Organization transformation plan and process for business and IT are defined

Risk Category V: Project Management & Control

Control objectives
5.1 Valid, Reasonable Planning & Estimating Methods <ul style="list-style-type: none">- A logical, orderly method of estimating workload by activity and task has been used to develop the project workplan- Estimates of workplan loading and time have been compared to other experiences and appear reasonable- To what extent is the plan used to manage the project
5.2 Clearly Defined Activities <ul style="list-style-type: none">- On the project workplan, tasks have been defined in uniform and reasonably concise increments- Task interdependencies are defined and valid
5.3 Clearly Defined End Products <ul style="list-style-type: none">- End products have been defined as tangible, measurable work products which can be clearly demonstrated as being complete- Quality of deliverables
5.4 Clearly Assigned Responsibilities <ul style="list-style-type: none">- Responsibilities for completion of end products have been assigned
5.5 Change Control Mechanisms <ul style="list-style-type: none">- Processes are in place to ensure that changes in scope are reflected in the project control tools
5.6 Risk Assessment Method <ul style="list-style-type: none">- A method for periodically re-assessing the risks of the project has been defined and is being utilized
5.7 IS Project on schedule according to original plan <ul style="list-style-type: none">- Budget vs. actual - people and money- Deliverables
5.8 Clearly defined project standards <ul style="list-style-type: none">- Support tools- Document management control- Data management

4 Output of the Risk Assessments /Action plans

From the previous steps that covered inherited risks and detection/tests of controls on place we should get the answer - list of residual risk areas. Output and real added value of every such process should also **action plan** for minimizing residual risks. For this purpose, risks should be evaluated and arranged regarding the consequences (Impact level/probability of occurrence).

