RISK MANAGEMENT FOR MOBILE SERVICES

Dimitar Kolev

Abstract: This article is dedicated to risk management for mobile internet services. A theoretical framework has been done in order to define risk factors, their evaluation and disposition or impact minimization. On that basis, some key conclusions are drawn and risk management strategy guidelines are presented.

Keywords: Risk management, factors, mobile internet service.

ITHEA Keywords: C.2 Computer-Communication Networks; C.2.0 General - Security and Protection

Introduction

Modern dynamics in the field of economics implies that any business venture is associated with a certain risk. The essence of risk can also be sought through an etymological analysis of the word: "riscio", it has a Latin origin and means danger, uncertainty with a solution whose outcome is unknown. It is often associated with the possibility of failure or loss, and this determines the negative side of the risk, while its positive side is related to the expected profit or dividend for the investors and entrepreneurs. In recent years, organizations have been looking for more opportunities to anticipate and control the negative risk associated with their business in order to secure long run sustainment. Proper risk assessment and management provides an opportunity to respond adequately and minimize possible losses for both the organization itself and all stakeholders.

The main objectives of this research is:

➢ To build a theoretical framework for risk management;
➢ To give examples of risk factors for mobile services and possible solutions.

Theoretical framework for risk management

Risk management is the ability to anticipate threats from the internal and external environment of the organization and minimize their adverse effects. The process is interactive and runs throughout the organizations' lifespan. It starts by identifying the possible risks, going through risk analysis and
planning their management, and then begins a process of monitoring and a regular return to the analysis stage.

The risk management process is standardized in **BDS ISO 31000** “Risk Management”. It recommends that the risk management process should be integrated into the organization’s management processes, in its strategy and planning, management, reporting, as well as in the organization’s policies, values and culture [BIS, 2016].

In the first stage, the organization must **identify** sources of risk, possible events (including changes in circumstances) as well as their causes and potential consequences. This stage aims at compiling a list of risks that can provoke, induce, accelerate, or delay the achievement of management goals.

The **analysis** stage provides input data for risk assessment and decision-making for reactions and allows selection of the most appropriate methods. It takes into account the causes and sources of risk, their positive and negative consequences and the probability rate.

The risk evaluation, according to some researchers [Tomov, K., 2014] is “a systematic process for identifying and evaluating events (possible risks and threats) that could negatively impact on corporate goals. Such events can be identified in the business environment (for example, economic trends, regulatory requirements, competition, etc.) and within the organization's internal environment (e.g., people, processes, infrastructure, etc.).” This process has three basics:

1. Risk evaluation should be clearly regulated and documented. Essential, here is the provision of the necessary resources, the good management and monitoring of the risk evaluation system.

2. These evaluations should be tied to the specific objectives of the organization and are measurable in order to make it easier to allocate the necessary resources both to them and to the associated risks.

3. Quantifying and / or qualifying risk ratings. Risks are usually measured in terms of their impact and probability. Quantitative rating scales allow a greater degree of accuracy for the risk evaluation process. However, they need a qualitative point of view that can be used when the risks are not quantifiable, with no reliable data available or when the analysis of data is not cost-efficient. One of the most common practices is the use of 5-ranked scales according to the probability of occurrence and degree of impact of the risk (see Table 1).
Table 1. Risk evaluation scale

<table>
<thead>
<tr>
<th>Evaluation</th>
<th>Probability</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Impossible</td>
<td>Very low</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>Probable</td>
<td>Moderate</td>
</tr>
<tr>
<td>4</td>
<td>Very probable</td>
<td>High</td>
</tr>
<tr>
<td>5</td>
<td>Certain</td>
<td>Very high</td>
</tr>
</tbody>
</table>

To clarify the qualitative evaluation process an example of risks and their probability and impact is presented in table 2. It is evident that the risk with the highest influence for the implementation of the project is the underestimated development time. In this case, this will lead to non-compliance with deadlines, which is probably linked to serious material sanctions for the organization. Similarly, the impact of an inappropriate assessment of the necessary resources is likely to result in a reduction of project profit or even temporary losses.

Table 2. Types of project risks and their evaluation

<table>
<thead>
<tr>
<th>Risks</th>
<th>Type of risk</th>
<th>Probability</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>The technology does not meet the expectations</td>
<td>Technological</td>
<td>Unlikely</td>
<td>Very high</td>
</tr>
<tr>
<td>Underestimation of the necessary resources</td>
<td>Project risk</td>
<td>Very probable</td>
<td>High</td>
</tr>
<tr>
<td>A large number of newcomers/staff resignations</td>
<td>Size and experience of the team</td>
<td>Probable</td>
<td>High</td>
</tr>
<tr>
<td>Underestimated development time</td>
<td>Project risk</td>
<td>Certain</td>
<td>Very high</td>
</tr>
</tbody>
</table>
Next stage is **risk management planning**; it involves selecting, and implementing one or more tools for affecting it. Once implemented, the risk management method can generate or change the means for managing it. The impact on risk is a recurring process for:

- assessment of the impact on risk;
- determining whether residual risk levels are acceptable when they are not - a new risk management method should be implied with a subsequent assessment of its effectiveness on the risk.

On this stage, the aforementioned scales for risk evaluation are used with calculated rating value by the following formula:

\[ risk\ rating = \text{probability} \times \text{impact} \]  

(1)

Once the risk rating has been determined, a risk management plan is drawn up (see Table 3).

### Table 3. Possible risk ratings and management plan

<table>
<thead>
<tr>
<th>Possible risks</th>
<th>Probability</th>
<th>Impact</th>
<th>Rating</th>
<th>Risk management plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no network coverage</td>
<td>3</td>
<td>5</td>
<td>15</td>
<td>Building more base stations for access, network expansion</td>
</tr>
<tr>
<td>Low speed for mobile data</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>Upgrading the network with higher capabilities components</td>
</tr>
<tr>
<td>Network support issues</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>Checking the network configuration</td>
</tr>
<tr>
<td>Underestimation of operating expenses</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>Make an unexpected costs fund</td>
</tr>
<tr>
<td>New government requirements to evolve to 5G networks</td>
<td>4</td>
<td>5</td>
<td>20</td>
<td>Allocation of more funds for capital investment</td>
</tr>
<tr>
<td>Technical support issues correlated to upgrading to 5G networks</td>
<td>3</td>
<td>4</td>
<td>12</td>
<td>Temporary employment of technicians to help the support team.</td>
</tr>
</tbody>
</table>
As evident from the table, the highest risk for a telecommunication operator is the requirement for mobile network upgrade to 5G, which involves serious capital investment. Next possible risk is no network coverage and its solution is the building of more base stations for access network.

Another risk management option is the so-called “risk transfer” [Zafirova, Tz., 2008] - it aims to minimize the risk in the existing business and transfer it to another organization where the losses would not have a significant impact. Here the mainframe is on various forms of insurance of the activity and / or the property of the organization, additional clauses for forfeit in the contracts and so on.

In order to determine properly the rate of the risks and the management plan, it is necessary to gather relevant information, as follows [BIS, 2016]:

- the reasons for choosing a specific risk management plan, including the expected benefits;
- the person or persons responsible for approving the plan and those responsible for its implementation;
- current actions;
- resource requirements, including those for unexpected costs;
- the criteria for success and limitations;
- control and monitoring requirements.

The last two stages of the risk management process include regular monitoring and control. It is important that risks be reviewed and reassessed on a regular basis, as there is a possibility of some risks to disappear, add new or change their ratings. This also implies a regular return to the risk analysis stage. Here the following main objectives are achieved:

- risk occurrence confirmation;
- insurance that risk management activities are implemented;
- determine which risk, what problems has caused;
- documentation of information for subsequent risk analysis.

At this stage, it is very important that all the results are recorded in order for the risk management activities to be traceable. These records provide a database to improve the methodology, as well as the risk management process as a whole.

**Conclusion**

The integration and proper implementation of a risk management enables each organization to minimize the risks that arise during its market development. This leads to more adequate management decisions, minimizing losses and greater flexibility in response to changes in its internal and external environment, which is crucial for today's business dynamics.
Bibliography

[BIS, 2016] Bulgarian Institute for Standardization. Risk management. BDS Compass, issue 4, 2016, Sofia, pp. 5-9, ISSN 1314-3611.


Authors' Information

Dimitar Kolev – University of telecommunications and post – Sofia;, Sofia-1700, Bulgaria; e-mail: dimitarkolev84@gmail.com

Major Fields of Scientific Research: Economics, Marketing, Management.