Comparative Analysis of Modern Methods of Software Risk Management for IT/IS Projects

Bakhrom Shamuratov[1], and Mohamed A. Hamada[1]

[1] *International Information Technology University, Manas St. 34/1, Almaty, 050000, Kazakhstan*

Abstract

In this research the essential meaning of Risks and Risk Management models are investigated toanalyze the main risk management models of software projects by developing an analytical comparison of modern Risk Management models to recommend the best model, which is more suitable for nowadays challenges and obstacles in the field of software projects development andagile project management.

Keywords

Risk, Risk Management models, software projects, ISO 31000

1. Introduction

In the field of world crisis (financial and economic), the most common issue of Kazakh industrial organizations is Risk Management. Nowadays, the globalization process is another source of economic risks. Therefore, knowing the general concept of the Risk Management algorithm in development will increase the success rate of goals and targets of IT companies, although, of course, it will not reduce the possibility of various kinds of risks to zero [1].

Actually, applying the essential concepts of Risk Management model to develop software projects allows to:

1. Identify risks at any stage of projects; predict, compare, and analyze risks.
2. Create the needed project strategy to mitigate or eliminate identified risks.
3. Implement previous developed strategy.
4. Monitoring the behavior of applied Risk Management model.5.Monitor and control the project deliverables.

Risk Management consists of the following features:

- the need of the company's management for forward-thinking, intuition, and situation foresight; formalizing the Risk Management system as a possibility;
- the ability to respond quickly and recognize ways to improve the functioning of the organization, and minimize the possibility of an undesirable course of events.

It is not news that complex Risk Management systems are widely used in advanced countries such as the USA. Because owners of large organizations are already made sure that old Risk Management methods do not correspond to the modern project requirements and not sure about the high success rate of project completion [2].

A clear division of authority and responsibility among all structure entities is implied by the implementation of Risk Management. The appointment of personnel in charge of carrying out the essential Risk Management procedures at all levels is one of top management's duties.

The company's strategic aims and objectives should be supported by such decisions, and they should not contravene the laws in effect. Additionally, it is crucial to properly distribute among the executors

Proceedings of the 7th International Conference on Digital Technologies in Education, Science and Industry (DTESI 2022), October 20–21, 2022, Almaty, Kazakhstan

EMAIL: 33097@iitu.edu.kz (Bakhrom Shamuratov); m.hamada@iitu.edu.kz (Mohamed A. Hamada)
ORCID: 0000-0002-0442-3663 (Mohamed A. Hamada)

the functions of risk identification and risk situation control.

2. The aim and objectives of the research

Aim: This research aims to demonstrate the importance of Risk Management in the organization, compare the methods of Risk Management models and make a suggestion on the best risk management model (identify the most effective method of Risk Management) for software projects.

Tasks:

- To determine the existing methods of Risk Management;
- To analyze and compare determined methods of Risk Management;
- To identify which method of Risk Management is most effective for an organization.

3. Research methods

In this research, examples of Risk Management methods were considered using the example of various types of scientific research on this topic, as well as by making a survey (interviewing employee of Big 4 Companies that works in the Risk Management area). Methods of empirical research are used as the main methods by using quantitative analysis.

The process of Risk Management evaluation and the suggestion of the suitable model to construct the Risk Management methodology was described according to the guidelines of PMBOK. It is also worth noting that all the proposed models described in the article, according to the authors classification, models have a primitive appearance, which still needs to be finalized. The authors also mentioned which functions should be improved in this model, which played an important role in assessment process.

The recommended risk management model for nowadays organizations was considering the recommendations of the authors and the modern challenges and problems of Risk Management such as system automation, minimum consumption and maximum efficiency.

4. Related works (literature review)

Alexsandro S.F., 2021 in his work represented a risk prediction model (software) called “Atropos” for project management according to the project similarity by it in the context of history. The proposedmodel consists of 6 main components (stages): (1) inserting data about the current project; (2) analyzing the likeness of the project with historical context; (3) storing the information about the current project during the whole project management; (4) comparing each step of the current project with captured projects from a historical database; (5) identification of possible recommendations based on comparisonof the previous stage; (6) building risk management approach to the current project. In a nutshell, the author represented an automated risk management model that builds an accurate risk management planwith described details (risks, recommendations and etc.) [3].

The study by Li G. 2021 represents the risk management model called “Monte Carlo”, which acts as a decision-support system to predict possible risks and risks that may be caused by previous risks (interdependencies network). This model is consisting of 3 main components: (1) development of risk interdependencies network for possible risks identification; (2) development of “Monte Carlo” simulation for assessment of risks; (3) further planning to risk mitigation plans. Also, the author provedof importance oh his model by examining two cases of risk assessment in project management [4].

Syrine Ch., 2020 in his study represents an improved risk management model in Scrum methodology to increase the success rate. This model is created by making a survey, taking the main parts from PMBOK. The peculiarity of this model is that it contains all required phases from planning to risk mitigation stages. This model is described in 6 stages: (1) risk management planning; (2) risk assessment; (3) analysis performing; (4) risk response plan; (5) implementation previous stage; (6) riskmonitoring [5].

The work of Béatrix Baraforta, 2019 presents the result of the development of a new Risk Management assessment algorithm called “Integrated Risk Management process model for IT

Organizations (IRMIS)”. This algorithm differs from others in that in this model each process is divided into more small business processes, which provides an opportunity for a more in-depth study of the risk. It is also worth noting that this algorithm is developed based on the guidelines recommended by international standard ISO 31000 in the context of multi-standards of ISO series [6].

In the work of Varlamova D., 2020, was proposed implementation of an automated Risk Management algorithm in the organization. The author suggests automating Risk Management with software-based solutions.

More precisely:

- building a process model of Risk Management with the help of Workflow task support systems;
- data streams will be in the data storage;
- the data will be processed and analyzed automatically using machine learning techniques with the ability to build models and predictions;
- use of dashboards for reporting and visualization of operational, analytical, and statistical data;
- automated document management systems will ensure the integration of normative documents from different management systems [7].

4.1. What is the risk and risk management?

Formal articulation of the concept of risk is essential and allows organizations to refer to and apply consistent definitions and develop a similar understanding of terminology. While a similar understanding of risk is important, the word “risk” has many different meanings. Similarly, in everyday discourse, "risk" can mean danger, likelihood, consequence, potential adverse factors or threats, and sometimes opportunities [8].

All of these factors, including probability, consequence, danger, etc., characterize risks. Risk is often defined as "the influence of uncertainty on the achievement of objectives" in the context of the ISO 31000 standard. As a result of this description, Risk Management cannot be a procedure that is added on top of existing managerial decision-making systems. On the other hand, risk management is an integral part of all operations and procedures.

Additionally, according to ISO 31000, "goals might have diverse elements (financial, health, safety, or environment) and can be applied at different levels (strategic, organization, project, product, and process)". This variation from what is intended can be both beneficial and harmful.

Furthermore, according to ISO 31000, risk is defined as "the mix of an event's consequences and its associated likelihood" and is frequently characterized by a "connection between prospective events and consequences, or a combination of both". As a result, the probability and sources of the risk's inception are also risk components. Thus, risk can be described as a combination of the following elements shown in Figure 1 [9].

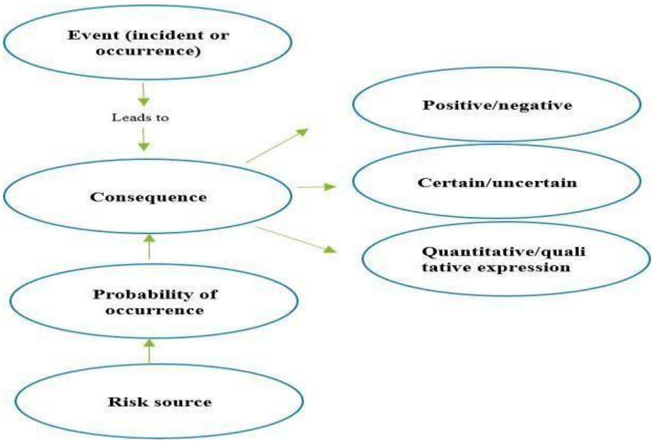

Event (incident or occurrence)
Leads to
Consequence
Positive/negative
Certain/uncertain
Quantitative/qualitative expression
Probability of occurrence
Risk source

Figure 1: Risk and its elements

In other words, in order to identify risk, one must take into account an event that is probable to occur owing to the presence of risk sources, as well as estimate its potential outcomes (the level of uncertainty is defined by the likelihood of occurrence). These effects will have an impact on both individual and corporate objectives.

The source of risk is described in the standard as an element “which, by itself or in combination with others, has the intrinsic potential to generate a risk”. The most elusive risk factor, probability, can be simply defined as "the likelihood that something will occur." This "something" in the context of Risk Management refers to a risk-related event.

As we've already established, risk management is essential for achieving both individual and corporate goals, but it's not the only one. This necessitates the careful application of the steps mentionedin the sentences below.

4.2. What does good Risk Management mean?

The following standards must be applied in order to evaluate the effectiveness of risk management:

- The prompt identification of risks;
- Risks are thoroughly examined, and the most significant ones are given increased importance;
- Balanced risk treatment is carried out;
- Risk treatment is carried out effectively;
- The resources required to implement contingency plans are available, and they have been designed, tested, and are still feasible.

Compliance with these criteria requires systematic Risk Management based on the following actions:

- Establishing a context or understanding of what we are “protecting” (our strategy or assets, health, market performance, etc.) and who the stakeholders are;
- Identifying risks (what events may occur, why they may occur, how likely they are to occur, and what impact they may have on us) and becoming familiar with as many of them as possible;
- Understanding the risks that are most significant to us helps us assess and evaluate them;
- Starting with the risks that are most significant to us, we can choose how to address them (we can keep the risk, share it with another party, mitigate it, or prevent it by removing its source);
- Execution of the choice made in direct response to the Risk Management procedure;
- Creation of a crisis management strategy for risks that have been taken on or reduced. A strategy for managing the risk should it materialize is the end result of this. Since Risk Management is a mechanism for providing sufficient, but not absolute, security, this conceptual step of the process is crucial.

4.3. Main Functions of the Risk Management process

4.3.1. Context establishing

Information is both produced and consumed during the risk management process. The quality of the raw material determines the quality of the final result, just like it does in any other process. The following is a list of the most crucial inputs to the risk management process [10]:

- Goals. One essential component of the risk management approach is clearly defined objectives. Remember that risk is defined as "the influence of uncertainty on goals." It will be highly challenging to recognize, comprehend, and address the associated risks if the goals are not clearly defined. The Center for Strategic and International Studies (CSIS) recommends "identifying and evaluating risk, taking into account the strategy and mission of the organization" as the most effective strategy;
- Assets. Risk Management also requires knowledge of assets - the value of the organization, what it is trying to protect, and potential sources of additional direct or opportunity costs. The key assets of an organization are physical assets, technology, internal infrastructure, capital, finance, and information systems. These assets can be ranked according to the degree of criticality and combined into various categories;
- Information about stakeholders and their needs. According to ISO 31000, a stakeholder is "a person or organization that has the potential to affect (or is already being impacted by, or may become influenced by) a decision or activity." It is critical to understand stakeholders' demands in

order to predict their behavior, as their wants can be a source of various dangers for a business.

4.3.2. Risk identification

A thorough and current awareness of the hazards an organization faces is what risk identification is meant to give it. A risk registry contains a list of all known dangers. It is created by making a list of all pertinent risks' incidences, root causes, likelihoods, and effects [11].

The risk register is constructed via a number of techniques. An essential method for identifying hazards is past risk analysis, which can also serve as the foundation for internal classification. The organization compiles databases of internal losses and obtains data from outside sources to better understand historical hazards.

As shown in Figure 2 below, some of the risks are internal. They originate from business processes and are determined by the nature of the organization's activities. Often referred to as "operational risks", such risks arise from poorly tuned business processes, human error, or system failure. They usually include professional risks, personnel risks, and information and infrastructure risks.

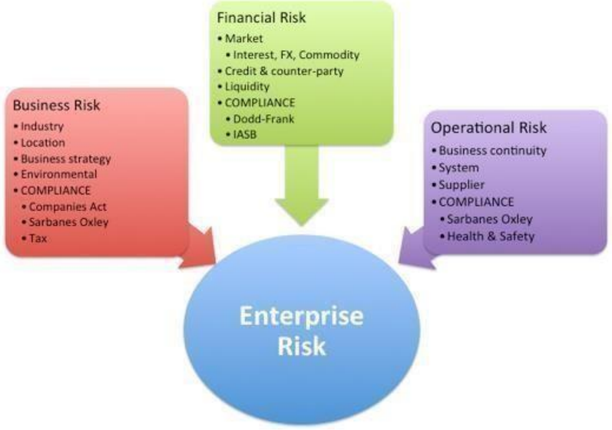


Figure 2: Various types of risks

From a regulator's point of view, risks can be classified by the ability of the regulatory parties to manage risks themselves (as opposed to the need to coordinate actions) and by their impact on other parties (as opposed to risks affecting only one organization or regulatory area).

Other risks originate in the external environment. They come from markets, partners, consumers, regulatory actions and the natural environment. Business risk combines all events related to changes inthe demand for products and services of the organization, changes in the price of these products, and other relevant factors.

Risk classification helps to comprehensively identify the risk. To develop a risk register, you can analyze all existing types of risks to understand what each of them means to the organization.

Risks can be identified through brainstorming using simple checklists where the discussion can be based on risk classification. It is also possible to conduct a series of interviews during which risk classifications can help identify the most suitable respondents and shape the design of the questionnaires. Another useful risk identification tool is the Delphi method, which helps to reach a compromise and conduct a preliminary safety analysis. The idea of the latter is to compile a list of threats and risks by taking into account such characteristics as materials and equipment used or produced in a given process or industry, operating conditions, and the relationship between the components of the system.

Another risk identification tool is a structured "*what-if*" analysis. It implies a systematic study carried out in a group, using the standard phrase of the subjunctive "what if" in combination with indications of the study of how a system, organization, or process will be affected by deviations from normal business and behavior. The discussion is conducted by wording questions containing the phrase "*what- if*": "*what if* ...", "*what would happen if* ..." or "*whether happened to someone or something* ...". The purpose of the analysis is to stimulate the analysis team to explore potential scenarios, their causes, consequences, and impacts on a large scale.

4.3.3. Risk analysis and assessment

The purpose of the risk analysis and assessment step of the risk management process is to prioritize previously detected issues, ensuring that the most severe risks are handled first. Various threats are contrasted to achieve this [12].

Risk analysis is characterized as "the creation of an understanding of risk... by assessing the implications and likelihood of their occurrence, as well as other risk parameters," according to ISO 31000. In order to decide if risk treatment is necessary, risk assessment compares the amount of risk discovered throughout the analysis process to the risk criteria clarifying within the context under discussion.

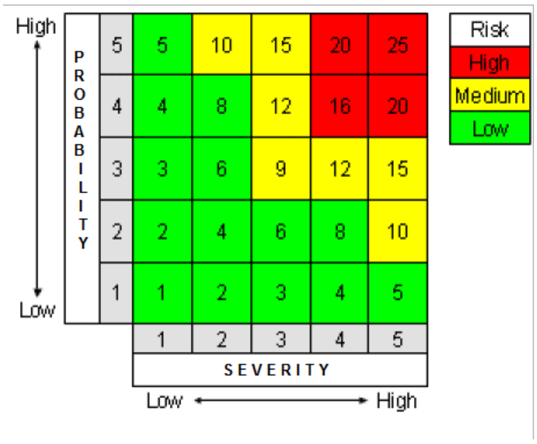
Probability and repercussions, two components of the idea of risk, are used as performance metrics. For a corporation, the effects of likelihood are frequently represented in terms of financial or time losses, whereas for a regulator, the effects may include economic losses, environmental harm, or worsening inpublic health. If decision-makers use these indicators, they can multiply the opportunity by the repercussions to determine the potential cost of risk. You can decide which dangers are more or less important by repeating this action with all of them.

However, risks cannot always be quantified. In such cases, the construction of a matrix of consequences and opportunities is the simplest and most often used tool for prioritizing risks. It allows for a combination of qualitative and semi-qualitative impact ratings and opportunities to obtain an objective and reasonable risk rating. According to ISO 31010, it is "often used as a screening tool when multiple risks have been identified, for example, to identify risks that require further or more detailed investigation".

Probability and repercussions, two components of the idea of risk, are used as performance metrics. For a corporation, the effects of likelihood are frequently represented in terms of financial or time losses, whereas for a regulator, the effects may include economic losses, environmental harm, or worsening inpublic health. If decision-makers use these indicators, they can multiply the opportunity by the repercussions to determine the potential cost of risk. You can decide which dangers are more or less important by repeating this action with all of them. Those risks, whose costs are the biggest, will be themost significant for the organization.

Similarly, the full range of impacts can be broken down into "*very low*", "*low*", "*medium*", "*high*", and "*very high*" impacts. This spectrum usually includes financial loss, professional safety, customer safety, environmental damage, reputation, and other parameters.

The impact of a single risk, for instance, may be "low" in terms of finances, "mid" in terms of workplace safety, and "very high" in terms of reputation. The same risk event may have an impact on each of these categories to differing degrees. It is simpler to assign a risk category in the overall rating linked with the highest score awarded to any of the consequences when these criteria are organized into a matrix.



PROBABILITY	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Risk
High
Medium
Low

High
Low
SEVERITY
Low
High

Figure 3: Probability Matrix

A significant advantage of this tool is that it does not allow users to calculate the cost of a risk that cannot actually be calculated, such as loss of life or health. It also helps policy makers compare risks across a wide range of areas and develop Risk Management at the government level.

Once a risk rating has been developed in context of probability and influence, the organization needs to assign each combination of probability and influence level of severity (for example, "high impact and high probability of influence" - critical risk). This will create a matrix like the one shown in Figure 3. The organization can then use this matrix to prioritize all previously identified risks.

4.3.4. Selection and implementation of risk treatment strategies

Once the risks have been prioritized, the organization can decide how to respond to each risk, starting with the most pressing. Key inputs at this phase include the organization's tolerance level for risk, often known as risk appetite or risk acceptance requirements.

Next, we will look at four main risk treatment strategies:

- Tolerating or accepting risk;
- Transfer or sharing of risk;
- Risk mitigation;
- Risk avoidance.

Due to ISO 31000, selecting the best risk management approach depends on striking a balance between the implementation's effort and expense and the rewards realized while also taking into account statutory, regulatory, and other criteria including social responsibility and environmental protection. In order to choose the best or most profitable alternative, cost-benefit analysis is frequently used to choose a risk management plan. It compares the whole projected expenses to the total expected benefits.

When choosing a risk treatment strategy, it is important to take into account the risk's magnitude, the value that will come from the risk-related activity (which can be stated through targeting), and the cost of risk management.

Tolerating or accepting a risk is the value that will result from the risk-related activity (which canbe expressed through targeting), and the cost of risk management when selecting a risk treatment method.

1. Where "*the stakes are high*", i.e. the expected benefit from risk-taking is extremely high.
2. When the cost of treating risk is greater than the cost of possible damage if the risk event occurs(example, it makes no sense to spend $100 on risk mitigation if it entails a loss of $50).
3. When something is beyond personal or organizational control and there is no other choice but totake the risk.
4. When the decision maker is willing to take the risk (and all legal and regulatory requirementshave been met).

Taking the risk does not mean that the risk is forgotten. This means that whoever takes a risk knows why they are doing it, that the risk is entered into the risk register, and that all risks taken are taken intoaccount when developing contingency plans.

Transferring risk means sharing risk with another party or parties. One of the possible strategies in this case is outsourcing, when one company transfers to another part of the functions and the risks associated with them. Another well-known risk transfer strategy is insurance.

Sharing risk with another person or parties is referred to as risk transfer. Outsourcing, where one organization passes some of the functions and risks associated with them to another, is one of the conceivable methods in this situation. Insurance is a well-known method of risk transmission.

The process of **risk mitigation** entails making an effort to reduce the effects and/or likelihood of a risk event happening. This might be accomplished by removing risk factors, altering the probability of an event occurring, or altering its effects.

Risk avoidance means stopping or avoiding activities that may increase the likelihood of a risk occurring. It also implies the waiver of all benefits associated with it, including some benefits that cannot be foreseen. For example, banning certain manufacturing processes can hinder the development of potentially beneficial technologies. Risk avoidance is generally preferred when the expected benefit does not exceed the cost of risk mitigation and when the risk cannot be accepted.

The ISO 31000 standard advises that when choosing risk treatment methods, an organization take into account the values and vision of its stakeholders as well as the best channel for communication with them. It is also advised to consider the possibility of additional hazards associated with the implementation of new regulations. Even if it doesn't, the failure or ineffectiveness of risk management strategies could still result in a severe risk.

Once a risk's method of action has been established, a risk treatment plan that outlines the approaches an organization will use to handle each risk included in the identified risks and specifies the order in which each risk must be treated must be developed. According to the guideline, the risk treatment approach should include the following:

- Reasons for choosing a particular processing method, including a description of the expected benefits;
- List of persons responsible for the approval and implementation of the plan;
- Proposed actions (which may include the development of regulations);
- Necessary resources.

The risk treatment plan is the first tangible result of the risk management process, and it serves as the foundation for further decisions and the appropriate prevention of risks that may jeopardize the attainment of organizational goals.

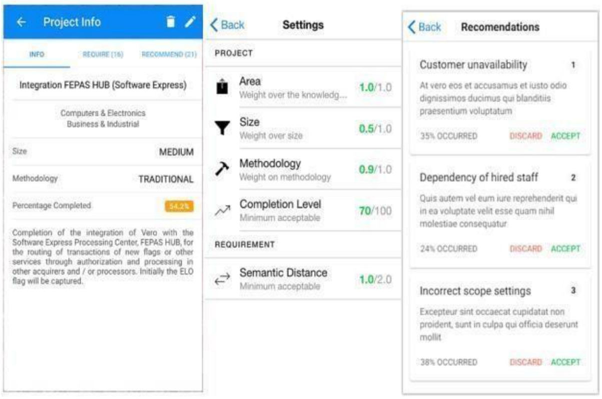
5. Comparing and suggesting the most suitable model for the organization

In this research, the first three Risk Management models, described in the paragraph above (literature review), were compared to determine the most suitable Risk Management model for present organizations.

5.1. “Atropos” Risk Management model, presented by Alexsandro S.F.

In comparison with other suggested models, the “Atropos” model has a more complex structure. Firstly, the structure of “Atropos” consists of the following six main components that allow to users interact with this Risk Management model:

- **Interface**: due to these component users can access the project input and output. In other words, this component allows to users’ up-to-date project details and get back project recommendations;
- **System view and API (Application Programming Interface)**: this is one of the main components since they are used to integrate the application layer with other model components;
- **Database**: this component helps to store whole project information as well as information about previous projects that are used for Risk Management recommendations;
- **Configuration**: to generate recommendations, the Risk Management model has to be configured via these components to set project similarities;



Integration FEPAS HUB (Software Express)

Computers & Electronics
Business & Industrial

Size MEDIUM

Methodology TRADITIONAL

Percentage Completed 54.2%

Completion of the integration of Vero with the Software Express Processing Center, FEPAS HUB, for the routing of transactions of new flags or other services through authorization and processing in other acquirers and / or processors. Initially the ELO flag will be captured.

Area 1.0/1.0
Weight over the knowledg...

Size 0.5/1.0
Weight over size

Methodology 0.9/1.0
Weight on methodology

Completion Level 70/100
Minimum acceptable

Semantic Distance 1.0/2.0
Minimum acceptable

Customer unavailability 1
At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum
35% OCCURRED

Dependency of hired staff 2
Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur
24% OCCURRED

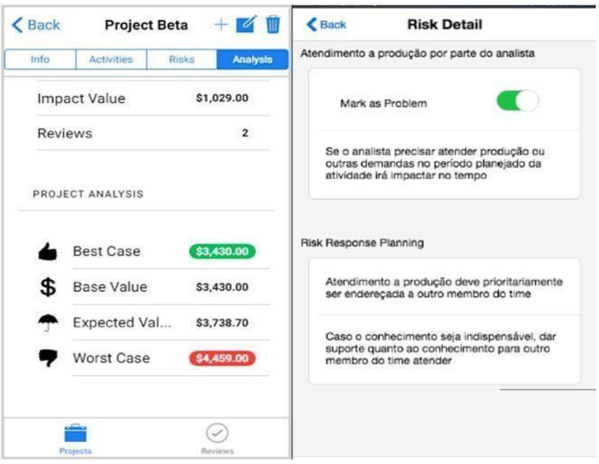
Incorrect scope settings 3
Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit
38% OCCURRED

(a) (b) (c)

Figure 4a: “Atropos” interface (a – project details, b – setting, c – risk recommendation)

- **Risks and Recommendations generator**: this component uses Bots for constant monitoring of project events and comparing them with previous projects from the database. In case of event matching - Bots generate risks with their recommendations.

Secondly, one of the biggest advantages of “Atropos” Risk Management model over other models is the user-friendly interface, showed in Figure 4a and Figure 4b, which is easy to use even for a specialist who is not good at Risk Management.



Impact Value	$1,029.00
Reviews	2

PROJECT ANALYSIS

Best Case	$3,430.00
Base Value	$3,430.00
Expected Val...	$3,738.70
Worst Case	$4,459.00

Atendimento a produção por parte do analista

Mark as Problem

Se o analista precisar atender produção ou outras demandas no período planejado da atividade irá impactar no tempo

Risk Response Planning

Atendimento a produção deve prioritariamente ser endereçada a outro membro do time

Caso o conhecimento seja indispensável, dar suporte quanto ao conhecimento para outro membro do time atender

(a) (b)

Figure 4b: “Atropos” interface (a – project expectation in cost, b - risk details)

After establishing the concept of “Atropos” Risk Management (Figure 5), we can figure out the main advantages and disadvantages of this model by its functionality:

Advantages:

- User–friendly interface;
- Risks are detected by the model itself;
- Recommendations generated by the model itself;
- The minimum human involvement;
- Many steps described in Basic Risk Management are automated.

Disadvantages:

- The database must be filled by users;
- Risks with recommendations must be filed into a database before projects started;
- The model can give incorrect recommendations in case of absence the of similarities in the database.

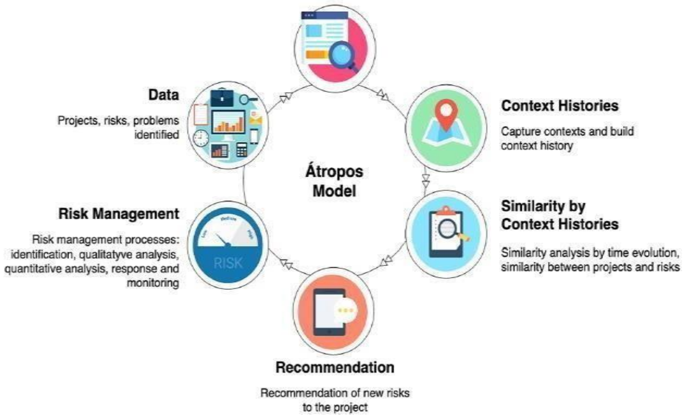

Data
Projects, risks, problems identified
Context Histories
Capture contexts and build context history
Átropos Model
Risk Management
Risk management processes: identification, qualitatyve analysis, quantitative analysis, response and monitoring
RISK
Similarity by Context Histories
Similarity analysis by time evolution, similarity between projects and risks
Recommendation
Recommendation of new risks to the project

Figure 5: The main concept of “Atropos” model

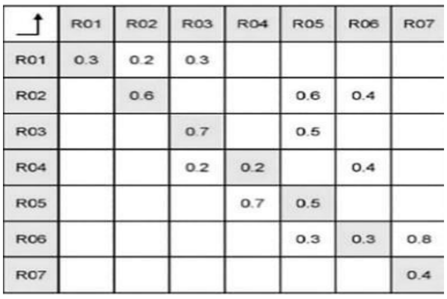
5.2. “Monte Carlo” Risk Management model, proposed by Li G.

The main difference of the “Monte Carlo” model from others is that this model considers not only identified risks but also covers risks that may entail identified risk [13].

Like the previous “Atropos” Risk Management model, “Monte Carlo” model uses previous experiences (projects histories) to predict risks more accurately and possibly their cause.

“Monte Carlo” Risk Management model consists of three main stages with their components.

The first stage is “Risk identification”. The input for this stage is information about previous similar projects to identify current project risks and build interdependencies with other risks. As output, from this stage, we will get possible project risks in relation to other risks, which can be realized in case the previous risk is not mitigated. Knowing all possible risks – allows for building cause-effect relationships. In addition, in this step, each risk’s spontaneous probability (SP) and transition probability (TP) are also calculated (Figure 6). By the end of this stage, the author proposed to call this stage as “Development Risk Interdependencies Network (RIN)”.



↰	R01	R02	R03	R04	R05	R06	R07
R01	0.3	0.2	0.3				
R02		0.6			0.6	0.4	
R03			0.7		0.5		
R04			0.2	0.2		0.4	
R05				0.7	0.5		
R06					0.3	0.3	0.8
R07							0.4

Figure 6: An example of an evaluated numerical matrix

The next stage is “Risk Assessment”. As input parameters here stand the project and experts’ opinions. In addition, at this stage, the “Monte Carlo” Risk Management model is built by modeling behaviors of identified project’s risk occurrence. After this, for each identified and related risk calculated the following parameters, which we get as output parameters: local and global influence of risk, total risk loss, and total risk propagation loss.

The final stage is “Risk Treatment”. In this stage project team, according to the identified and evaluated risk, makes a plan for risk mitigation. After that, comes the evaluation of proposed plans for risk treatment. And finally, the project manager or stockholders choose the most effective way to risk treatment.

Unlike the “Atropos” model, “Monte Carlo” Risk Management model refers to mathematical calculation and the involvement of people more often, which is one of the significant disadvantages of “Atropos” Risk Management model. And the main advantage is identifying possible project risks and risks that may be caused by previous risks.

5.3. Risk Management model in Scrum development process, proposed by Syrine Ch.

The Risk Management model, proposed by Syrine Ch., was created on basis of PMBOK (Project Management Body Of Knowledge) and by making a survey by 65 experts from different countries. Unlike previously described models, it does not have any automated algorithms or mathematical models. However, this model covers all requirements described in standard ISO 31000.

The author divided this model into several stages, from risk planning to risk monitoring (Figure 7):

- Risk Planning;
- Risk Identification;
- Quantitative and Qualitative analyze;
- Risk Response;
- Risk Response Implementing;

- Risk Monitoring.

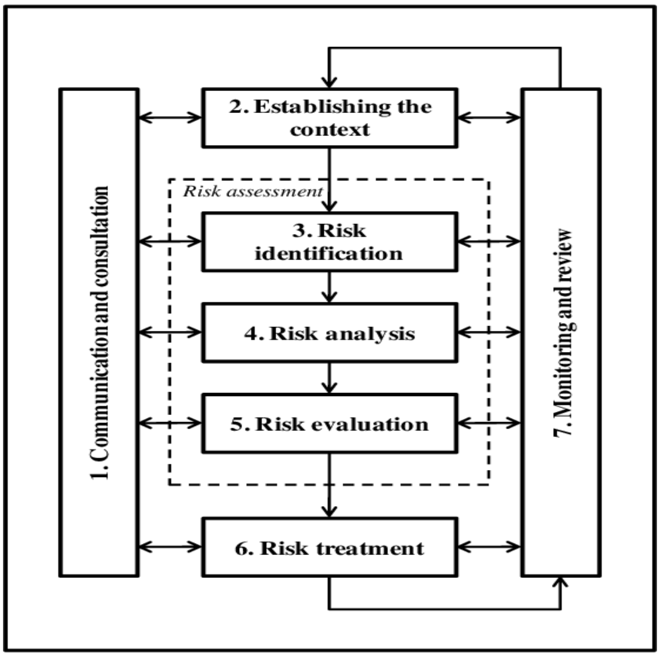


Figure 7: Risk Management model

In the first stage author highlighted “Risk Planning”. Like other models, the input for this stage is detailed information about the current project status, and as output comes a general plan of risk management.

The second stage is the “Identification of risk”. In this stage author proposed involving all Scrum team members. Risks are identified by team experience and experts’ ideas that are shared among the team. In addition, the author highlighted the importance of this stage by detailed analysis during risk identification. The output of this stage is the risk register with the following parameters:

- Description – the short description of identified risk;
- Date of risk birth – the date when risk is identified;
- Lakewood – the possibility of risk realizing;
- Impact – influence of risk;
- Category – the group for which risk belongings;
- Priority – identifying the priority among risks;
- Status – determine whether the risk is mitigated or still open.

In addition, the author highlighted the importance of sharing information about registered risks to make better collaboration between the team.

The third stage is “Quantitative and Qualitative analyze”. This stage is responsible for risk analyzinghow it can be influenced by the project. Unlike Risk Management models described before, this model does not have an exact way to how calculate the impact. Mostly, it will depend on the project, which iswhy this model is more suitable for small projects.

The next stages are “Risk Response” and “Risk Response Implementing”. In this step, Scrum team members choose the best strategies to mitigate and take an action under identified risks.

The final stage is “Risk Monitoring”. This step is designed to control mitigated risks and used as a plan for future projects.

Obtaining the ultimate risk information is possible after the product has been delivered. The risk register offers a view of all detected risk data, and future scrum projects can use this data to plan.

6. Result of analytical comparison of Risk Management model

Since we covered all the main concepts of the three above-described models such as “Atropos”, "Monte Carlo" and model suggested by Syrine Ch., we can build a comparison table to identify the most suitable Risk Management model for the organization. As the basis for comparison, we took the main components from ISO 31000 and PMBOK described in the fifth paragraph and all main stages from each Risk Management models (Table 1).

Table 1
Comparison of Risk Management model by its specification

Components\Model	"Atropos" model	"Monte Carlo" model	Model suggested by Syrine Ch.
Context establishing	+	+	+
Risk identification	+	+	+
Risk analyzing	+	+	+
Risk treatment	+	+	+
Automated process	+	-	-
Identifying risks relation	-	+	-
Storing projects history	+	-	-
Minimum human involvement	+	-	-

After comparing of three models, we can easily say that each model meets all main requirements described in ISO 31000 and PMBOK. Since these models have their specifications, all of them can be integrated into the organization depending on the project size.

However, XXI century is the century of digitalization, "Atropos" Risk Management model is more suitable for many organizations, since, it has automated business processes and requires less human involvement, which is most important.

One of the biggest cons of "Atropos" Risk Management model is the implementation cost. Since, this model requires of integration databases, APIs, Bots and etc., more organizations cannot effort to implement this model.

Thus, we can conclude, that organizations have to choose a Risk Management model according to the project size. For example, "Atropos" is suitable for big organizations with large projects, while "Monte Carlo" model is suitable for medium organizations, and the model proposed by *Syrine Ch.* is suitable for small organizations respectively.

7. Conclusion

This research presented to understand the basics of Risk and Risk Management terms by reviewing existing models. This work covered the basic meaning of Risk Management and how it is structured in different models.

To identify the most suitable Risk Management for organizations was compared the most widely used models such as "Atropos", "Monte Carlo" and the model suggested by Syrine Ch. The comparison was according to the basic Risk Management rules (from ISO 31000 and PMBOK). We noted that all authors of that models stick to the basic structure of Risk Management that is shown in Table 1. The main difference between them is the way of integration in the organization.

Making detailed comparisons between model components, allowed us to identify which models are suitable for the organization. Rather, it was revealed that all models contain all the necessary components described in the standard. Moreover, the selection of the model should depend on the type of organization and on the type of project.

In addition, it should be mentioned, that author highlighted that their model is a primitive type, and they will improve their models by collecting more information from future projects.

8. References

[1] K. Buganová, J. Šimíčková, Risk management in traditional and agile project management, Transportation Research Procedia 40 (2019) 986–993. URL: https://doi.org/10.1016/j.trpro.2019.07.138.

[2] A. Luis, Longevity of risks in software development projects: A comparative analysis with an academic environment, Procedia Computer Science 181 (2021) 827–834. URL: https://doi.org/10.1016/j.procs.2021.01.236.

[3] S. F. Alexandro, A risk prediction model for software project management based on similarity analysis of context histories, Information and Software Technology (2021). URL: https://doi.org/10.1016/j.infsof.2020.106497.

[4] L. Guan, A. Abbasi, M.J. Ryan, A simulation-based risk interdependency network model for project risk assessment, Decision Support Systems 148 (2021) 113602. URL: https://doi.org/10.1016/j.dss.2021.113602.

[5] Ch. Syrine, A framework for risk management in Scrum Development Process, Procedia Computer Science 164 (2021) 187–192. URL: https://doi.org/10.1016/j.procs.2019.12.171.

[6] B. Barafort, A. L. Mesquida, A. Mas, Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context, Computer Standards &Amp; Interfaces 60 (2018) 57–66. URL: https://doi.org/10.1016/j.csi.2018.04.010.

[7] D. Varlamova, A. Dolzhenkova, S. Korochkina, Automation in risk management" Economics and Environmental Management (2020) 78–86. URL: https://doi.org/10.17586/2310-1172-2020-13-4-78-86.

[8] J. Masso, Risk management in the software life cycle: A systematic literature review, Computer Standards &Amp; Interfaces 71 (2020) 103431. URL: https://doi.org/10.1016/j.csi.2020.103431.

[9] B. Barafort, Integrated Risk Management Process Assessment Model for IT organizations based on ISO 31000 in an ISO multi-standards context, Computer Standards & Interfaces 60 (2018) 57–66. URL: https://doi.org/10.1016/j.csi.2018.04.010.

[10] J. Arlinghaus, Assessing and mitigating the risk of Digital Manufacturing: Development and implementation of a digital risk management method, IFAC-PapersOnLine 54.1 (2021) 337–342. URL: https://doi.org/10.1016/j.ifacol.2021.08.159.

[11] S. Sankaranarayanan, Prediction of risk percentage in software projects by Training Machine Learning Classifiers. Computers &Amp, Electrical Engineering 94 (2021) 107362. URL: https://doi.org/10.1016/j.compeleceng.2021.107362.

[12] O. Okudan, A knowledge-based risk management tool for construction projects using case-based reasoning, Expert Systems with Applications 173 (2021) 114776. URL: https://doi.org/10.1016/j.eswa.2021.114776.

[13] A. Qazi, Prioritizing risks in sustainable construction projects using a risk matrix-based Monte Carlo simulation approach, Sustainable Cities and Society 65 (2021) 102576. URL: https://doi.org/10.1016/j.scs.2020.102576.