Information support of the risk management system in high-tech organizations with the involvement of private capital

Vladimir Ermakov1*, Igor Kiryakov1, Daniil Polozov1, and Ekaterina Polozova1

1RUDN University, st. Miklukho-Maklaya, 6, 117198 Moscow, Russia

Abstract. The objective of this article is to expose basic concepts of risks and encourage managers and members of high-tech companies with private capital to know more about this topic. Risk Management is taking up space in the many organizations through internal control standards. However, little mention is made of academia and risk management standards, causing organizations executives to know little about the concepts of risk and treatment. This situation makes risk plans have obvious conceptual problems that impair risk management and prevention in organizations. In addition, the article exposes actual methodologies and risk management strategies that minimize them in the environment of digital economy and innovation and also is the process of development of business structures in the conditions of risks affecting them.

1 Introduction

The theory and practice of entrepreneurship today is at a new stage of development, which is determined by globalization, the transformation of the system of economic relations between economic entities, as well as the informatization of all spheres of human activity. This cannot but affect such a process as the emergence and modification of risks and their impact on business structures. The nature of risk management activities is also undergoing numerous changes, among which it is necessary to highlight the use of qualitatively updated information tools and the provision of all types of security, including information security, along with the expansion of requirements for employees using information technologies, as well as creating and maintenance of a computer system. The management of business risks is becoming more complex against the background of the current situation of the Russian economy in the world, as well as changes in the political sphere, which are having an increasingly significant impact on economic processes, including at the level of each individual business structure. This affects the nature of competition, which implies the search for new tools for managing business structures in order to ensure a high level of their competitiveness. In the context of the transformation of business risks, existing methods and management mechanisms are no longer fully adequate to the new realities of globalization and informatization. In addition, the lack of effective management tools adapted to the conditions of geopolitical instability hinders the use of risks, first of all-

* Corresponding author: semenov.venture@mail.ru
external, in order to determine new directions for the development of domestic entrepreneurship. This problem is not limited only to external business risks, since under the influence of rapid innovative development, informatization and digital transformation of society, changes also occur in the internal environment of business activity, leading to the emergence of new risks. Insufficient scientific elaboration of these issues actualizes scientific research, aimed at the formation and scientific justification of new conditions that ensure the development of the entrepreneurial environment of the national economy on the basis of effective risk management. An important component of this is the study of the readiness of employees of modern business structures to work with risks and develop new solutions that meet the increasing requirements of today's stage of globalization. While these problems are relevant for all business structures, their solution should be based on taking into account the national and sectoral specifics of entrepreneurship [3].

Tools such as data analytics and product personalization have begun to generate a wide range of exciting business opportunities, primarily in private equity, ranging from robot-driven customer advice to smart savings accounts. But these services bring with them additional risks.

Companies that want to make the most of these new tools and products need a new approach to risk management, one that adapts to high-tech products developed in an unfamiliar way by innovative people. This means giving risk managers a broader mandate, to ensure that the company does not hinder the search for innovative proposals or compromise their safety [1].

Traditional risk management approaches tend to consist of a “yes or no” decision at certain times, or periodic review of a stable business process. A change of it or a new product, for example, is subject to pre-release approval, and the concerns identified at this point translate into additional risk controls. But before and after this approval process, risk managers have limited commitment.

In an age of innovation, this approach is bound to fail. Agile development can mean that propositions are never completely finished, but are in a constant state of development, which makes the commitment of a point in time impractical. In addition, innovation processes are often separated from traditional business, as companies isolate development teams to enable them to adopt agile working methods. This can make it difficult for risk managers to participate.

Finally, when companies are too slow in their development, they instead import innovation from abroad. This creates other challenges, as these sources are often startups that will only gradually, if at all, meet established corporate standards, leaving a long list of exceptions to corporate policy [4].

### 2 Risk management in the high-tech companies

Risk management is the process of identifying, analyzing and responding to the risks that an organization faces and is exposed to. The costs of implementing this system depend on the methods used to manage unexpected events [7].

There may be various types of risk:

- **Market risk.** Linked to fluctuations in the commercial and financial year, such as interest rates, exchange rates and the relationship between supply and demand.

- **Credit risk.** When one of the parties to a financial contract may not comply with the agreed and lose the money invested.

- **Liquidity or financing risk.** When one of the parties to a contract fails to raise enough money to honour the commitments made.

- **Operational risk.** Or the possibility of suffering losses due to failures in the processes, personnel or technical systems employed by a company.
In this way, the purpose of risk management is none other than to identify in advance the possible risks in an organization, in order to make forecasts or even, in some cases, turn them into opportunities. Thus, Enterprise Risk Management aspires to design and apply to any business administration a set of strategies created to “shield” the company from its main risk agents, which involves first making a diagnosis of weaknesses, strengths and opportunities [18].

Risk management is based on 11 principles that fit into the entire structure of the company and are related to the regulations of the implementation of risks. The framework mentions the commitment of management, the design of the risk management model, the implementation, the monitoring and review of the model, and the continuous maintenance of the model. Risk management processes help minimize uncertainty.

Identify, determine, control the risks and threats present or future in your organization.
Use a proactive, dynamic and flexible approach to successfully address any organizational change or incident.
Determine strategies to optimize decision making and planning.
Achieve the fulfillment of objectives, both at the strategic, tactical or operational level in the face of any uncertainty.
Establish action plans to ensure the operability of the company in any situation.
Safeguard critical business and operational operations during times of crisis.
Minimize downtime after any incident and improve recovery time.
Implement, automate and maintain an IMS based on international standards and under a process approach according to the PHVA Cycle (Plan, Do, verify and act) [15].

The risk management process is continuous and the results are materialized in the decisions made on the acceptance, reduction or elimination of risks that affect the achievement of the objectives. The goal is to optimize the organization's exposure to risk to avoid losses, avoid threats and seize opportunities [2].

The risk management strategy of an organization should be that all the risks it faces must be identified, evaluated, monitored and managed so that they remain within a certain limit, accepted by the management of the entity [16].

In the development of the theory of business risks, providing for minimization of their negative impact and influence on increase of level of competitiveness of enterprise structures with the developed instrumentation, ensure the embedding of new information technologies in control system business activity and revitalization of the staff at risk [3].

Risk managers must contribute to innovative development through risk identification, analysis and control recommendations, and must do so consistently and continuously. To ensure that risk controls are fully integrated into the resulting proposals, risk managers should be involved in the independent development, testing, validation and implementation stages, as well as regular review.

Digital innovation could generate new risks that will only become apparent over time and that do not conform to established taxonomies such as credit and compliance risk, so managing innovation risk will require a profound change for a company's risk functions. New tools and processes will be required.

Risk management will also need a broader mandate to reflect pre- and post-intervention points. Risk managers will need the right skills for this commitment model, and the organization will need to support agile working methods.

Risk functions in many companies are beginning to meet the challenge, often brought about by a high-profile project or company. The next task is to learn from those early movements and integrate innovation management as a key part of the risk function's mandate.

If a company's risk management doesn't adapt, innovation will simply happen elsewhere.
Implementing an integrated risk management within the organization will allow the organization’s management to focus its resources on those risks that affect the objectives achievement, in order to protect assets, ensure continuity of organization’s activities and adopting the effective decisions.

Risk management function must be a defining function within the organization and provide a complete and coherent set of activities and actions that define decision-making of the organization if the risk materializes and to guide staff in risk management.

An effectively integrated risk management system must ensure the recovery of the organization in case of interruption in activity, by maintaining its essential functions, at least of minimal levels from event appearance until its remediation.

The decisive part in the functioning of an integrated risk management system is the planning in order to ensure business continuity, because it contains measures of recovery for activities under risk event.

![Diagram](https://example.com/diagram.png)

**Fig. 1.** The management system of an organization [2].

The approach, implementation and functioning of an integrated risk management system in the organization is achieved depending on the processes undertaken, the organization situation and leadership style.

Below are some tools, and methodologies used for the management of business risks:

A risk matrix, also known as an "impact Probability Matrix", is a tool, useful for any company, that allows you to identify the risks to which you are exposed. In this way, companies can determine acceptable levels of exposure to those, as well as establish appropriate control against them and monitor the effectiveness of the chosen control method.
Physically, it is a visual guide that allows, through its design, a quick identification of the priorities that must be addressed. This also speeds up decision-making [17].

Risk analysis methodologies are divided into two main groups:

a) risk management methodologies: these are those that are oriented to the identification, evaluation and post-treatment of the risks derived from an activity. Among them is, of course, the ISO 31000 standard. There are also other standards, such as AS/NZS 4360, which provides a model of analysis focused on the principles of the ISO 9000 family of standards. Other of the most recognized methodologies are the HACCP system (Hazard Analysis and Critical Control points) and the ARO method (Operational Risk Management), which operate in the same direction.

b) quantification methodologies: in this case, these are those tools that focus exclusively on the quantification of risks. That is, they apply a series of indicators (almost always numerical) to measure the impact that risks have on organizations and, from that calculation, develop coordinated actions for their management, treatment or even elimination. - Magerit: it is a methodology of analysis and risk management that has been developed by the Board of Directors. It is specifically designed for companies that work with digital information and Computer Services. Its main function is to assess how much value a company puts at stake in a process and how to protect it. It also assists in the planning of timely treatments and in preparing organizations for audit, certification or accreditation processes. - Delphi: it is a method aimed at knowing the opinion of experts. At first, a group of anonymous specialists answers a questionnaire that draws up an organization on a specific topic, in this case Risk Management. After analyzing the results, the responders ask each of the members of the group for their opinion. Finally, the company prepares a second questionnaire, although this one with more precise and focused questions. The idea is that at the end a text is drawn up with the conclusions [5].

There are also quantitative, semi-quantitative and qualitative methods [14].

The current framework in place for internal risk control is the so-called COSO ERM 2019, also known as “COSO Enterprise Risk Management-Integrating with Strategy and Performance” [6].

This update maintains the financial focus of its predecessors, but, nevertheless, its flexibility and structure allows it to be used interchangeably by any type of activity [8].

High-tech business organizations, including those in the private sector, must maintain control of business risks as digital transformation evolves. Deloitte [19] has published "Global Digital Risk Survey 2019", a comprehensive report that analyzes the opportunities...
and challenges posed by the adoption of disruptive technologies for governance models and risk management [9].

Taking as a reference the report carried out by Deloitte, the main risks facing companies in the era of digital transformation are:

The impact of technology on the company

In many ways, technology has allowed companies to do things that would have been impossible before, it has allowed them to transform. The paradox is that many of the barriers that are now faced to achieving true digital transformation are no longer related to technology, but to culture, skills, execution capacity and risk management capacity [10].

A combination of these attributes is required to clearly decide and articulate the business model, something that many organizations seem to be still assimilating.

2. Digital transformation management

New technologies have significant potential to augment, disrupt or replace existing business models.

The risks brought by new technologies are likely to have a broad impact across the enterprise, and it is therefore critical for companies to reflect on whether their existing governance models are fit for the future and whether they can manage the considerable volume of existing change in which we are immersed [11].

This includes having a firmer idea of what the new key areas of risk are, who the figure on the fallback is and how these risks should be managed, monitored and mitigated. According to Deloitte respondents, digital risk management falls on the Chief Information Officer – CIO, or responsible for information technology systems (33%), while also on other C-suites or senior executives of the company (41%). Even so, 26% acknowledge that it is not yet clearly defined.

3. Emerging risk areas

There is no doubt that the risk map is constantly changing and organizations find themselves trying to manage known risks, such as cyber and data privacy, while also trying to understand and address areas of emerging risk.

As the line between business and technology teams continues to blur, emerging areas of risk are likely to have a greater strategic impact than traditional technology risks in the past.

4. Operating model for risk

The structure of the organization is slowly changing: digital transformation is driving new business models, new technology implementations, new processes, ways of working and evolving organizational structures [12].

This constant flow creates a challenging environment for establishing ownership and responsibility for risk, as well as responsibility for the execution of core risk management processes and the applicability of those processes to different parts of the organization. Consequently, the traditional functional model for risk management must be adapted. Therefore, the role of the risk manager clearly extends its functions.

5. Using disruptive technology to manage risk

Managing risk at scale is a complex task. While some industries have been more successful than others in using technology to manage risk, many organizations still manage key assets and processes, such as risk taxonomies, control libraries, and risk assessments in independent, legacy systems, or spreadsheets.

Significant opportunities are emerging to apply more disruptive technology to gain better value from risk management spending, but for those initiatives to be successful there must be the right Foundation: a consistently understood risk control and taxonomy library, robust and mature processes, and most importantly, clear ownership and responsibility for risk.
Even so, confidence is still lacking. In fact, 60% of respondents rate the effectiveness of current risk management tools with a 5 out of 10, or even less. However, there is sufficient technological capacity to drive this failed trust.

6. Lack of talent
Despite all the debate about the future impact of disruptive technology on the workforce, an organization's ability to get the best out of its human capital will always be a key factor in determining its success.

People are at the heart of what organizations do, and while having the right person in the right role has always been crucial, having the right people to manage risk is now more important than ever.

However, only 19% of respondents believe that their team has the right skills to get the job done. Therefore, it seems that the lack of training of the employees themselves thus becomes one of the main risk factors for any company [13].

3 Conclusions
The risks are inherent in any process, operation or activity is carried out, so that their management is a valuable tool that supports the growth and development of public and private entities. The risk assessment is a formal process that primarily requires the establishment of learning of the staff, it facilitates the creation of a culture of enterprise risk. Analyzing and evaluating risks is a permanent activity, demanded by the changing environment in the way of doing business. Faced with risks you can take two positions, ignore them and treat them. Treatment involves developing actions aimed at avoiding, reducing, sharing and accepting. The effective functioning of the internal control system requires periodic evaluations aimed at detecting weaknesses and opportunities for improvement for its constant updating. Linking control activities to the risks allows us to know the coverage on these adverse effects, the part of the risk not covered is the residual risk, which represents the appetite or tolerable risk that senior management is willing to take. The management of risk presents as advantages: to facilitate the achievement of the objectives, allows the entity to be prepared for adverse changes, reducing the potential for loss, creates and strengthens the risk culture and the image of the entity, and finally provides the means that allow the assessment of the performance.

Risk management and risk management systems, with which one seeks to channel the threats of an organization or company, are fundamental instances in the contemporary business world, since in them a high percentage of its success or failure usually lies. The reason is simple: an organization better prepared to face the possible complications that its particular production process implies, is also a company that will know what to do if a problem arises, being able to avoid that it becomes a catastrophe, when not managing to turn it rather into an opportunity for growth and investment [18].

References
1. Deloitte, Information technology risks in financial services: What board members need to know – and do
3. L. Irchenko, Improving the risk management system in the process of developing entrepreneurial structures (St. Petersburg, 2019)
4. T. Ivell, Partner en Oliver Wyman/Brink News, La gestión de riesgos en la era de la innovación empresarial

E3S Web of Conferences 371, 05062 (2023) https://doi.org/10.1051/e3sconf/202337105062
6. Deloitte, Risk Management is a game changer (2018)
7. V. Korotin, Risk management in oil and gas companies (Moscow, 2015)
9. Deloitte, Risk management in investment and innovation projects (Risk Academy, 2016)
11. Pirani, Guía para implementar un sistema de gestión de riesgos, según la ISO 31000 (2014) URL: https://www.piranirisk.com/es/academia/especiales/guia-del-sistema-de-gestion-de-riesgos-iso-31000
17. Risk management, URL: https://concepto.de/gestion-de-riesgos/