Energy-efficient internal audit for IT-risks in municipal facilities and environmental technologies

Firdaus Kharisova¹, Olga Efimova¹, Aigyl Sabirova¹, Husan Umarov²*, and Andrej Dashin¹

¹Kazan Federal University, Kazan, Russia
²Moscow State Institute of International Relations (MGIMO University), Moscow, Russia

Abstract. In this study, the authors analyze the contemporary factors within the external environment that impact the operation of municipal facilities and environmental technology endeavors, provided special emphasis to energy management and sustainability. The main goal of this research is to tailor the internal audit system to accommodate the evolving external landscape in the realm of municipal facilities and environmental technologies, ultimately advancing its efficiency. Employing a blend of analytical and synthetic techniques, along with logical and systematic approaches, the authors combine traditional internal audit methodologies with process-based management in the context of energy-efficient municipal facilities and environmental technologies. Notably, the focus of this investigation centers on addressing IT risks, which are deemed among the most consequential yet under-addressed components within the internal audit system, mainly due to the novelty of this trend in this sector. This study delves into the outcomes of an extensive exploration of IT risks, encompassing their classification and the categorization of information system and information technology risks, all of which are detailed in this article. Additionally, the research introduces a comprehensive methodology for conducting internal audits of IT risks within the sphere of municipal facilities and environmental technologies. Finally, it provides insight into the results of testing and the implementation of this methodology within a substantial municipal facility, shedding light on its practical applicability in this context.

1 Introduction

Economic instability and the global pandemic make the issue of company efficiency even more urgent. Business owners and top managers are forced to seek new approaches to improve the efficiency of companies, taking into account the realities of the time. At the same time, traditional methods of company management become ineffective due to changes in the external environment, as they do not fully cover the new risk factors and global digitalization. In this regard, new approaches and new methods of business performance management are often required. Combined solutions - integrated application of several

* Corresponding author: husan@kvell.ru

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).
methods of company efficiency management simultaneously, timely response to changes in external environment, to new business requirements - the authors see this as a way out of the current situation. Current research is intended to identify modern methods of efficiency management of the company, to give recommendations for the development of methods of actual internal audit system, taking into account current realities.

The increased quality and popularity of Internet communications and the availability of technical devices have brought the development of the economy to a fundamentally new level. If previously the objects of labor were tools, material components, nowadays it is information that is increasingly becoming the object of labor. Digital technologies as new formats of companies' work - e-commerce, mobile payments, online services and other information innovations are increasingly becoming the norm for all market participants. New digital opportunities are adjusting the old rules of organizing business processes (hereinafter referred to as BP) and leading to the emergence of new ones. At the same time, the use of any technology, along with the positive effect entails the emergence of uncertainty and risks associated with these technologies. And innovations in the field of information technology (hereinafter IT) is no exception. Widespread use of IT both in company management systems and technological processes has led to the fact that the risks associated with IT have become an important part of all business risks of the organization. If any undesirable events occur without IT risk management, the organization faces resource overruns and excessive funding. This results in direct losses and possibly the abandonment of technologies that seem too innovative and insufficiently tested. Which means it will end up with missed business opportunities.

The International Professional Standards for Internal Auditing (IPSIA) enshrines the requirement to apply the internal audit approach, which is undoubtedly significantly enhanced for IT auditing.

According to International Standard on Auditing (ISA) 315 (Revised) "Identifying and Assessing Risks of Material Misstatement by Examining the Organization and Its Environment," business risk is risk arising from significant conditions, events, circumstances, actions or inactions that could have a negative effect on an organization's ability to achieve its objectives and implement its strategy, or arising from setting inappropriate objectives and strategies.

Information Technology Risk (IT-Risk) - any risk associated with the use of IT.

According to a recent survey conducted by the Institute of Internal Auditors (The IIA) of internal audit leaders, the percentage of time spent on various risk categories in internal audit is as follows: operational risks - 30%, compliance risks - 30%, financial risks - 20%, risks caused by information systems or information technology risks - 20%. In the very near-term future, however, the picture will change, and the distribution will look as follows: operational risks - 25%, compliance risks - 30%, risks caused by information systems or information technology - 30%, strategic risks - 15%. Therefore, financial risks are objectively receding from the "leading group", while risks related to information systems or information technologies (IT risks) are moving up to the leading positions. The role of internal audit boils down to providing assistance to company management on risk management issues and consultations in this area.

Due to the specific nature of their work, the internal auditor has much more insight into the company's core business processes than other employees of the company. The very essence of internal audit makes you think about the construction of systems, the effectiveness of the combination of business processes and internal control procedures. The huge potential of internal audit lies in the fact that the internal auditor can provide a reasoned assessment of the process system, identify IT risks, develop recommendations to optimize IT infrastructure and employees' actions in working with information systems (IS).
Vladimir Repin's work "Business Processes. Modeling, Implementation, Management" provides a definition of a process as a stable, purposeful set of interrelated activities, which according to a certain technology transforms inputs into outputs of value to the consumer (client).

In the glossary to IASC Control Processes are interpreted as policies, procedures (both automated and non-automated) and measures that are part of the control system, developed and implemented to ensure the level of risk within the limits that the organization intends to accept (according to the International Professional Standards of Internal Auditing).

V. Ivanchenko defines IT audit of business process (IT audit of BP), as an audit of information technology and systems critical for the execution of a specific business process of the company with the specified criteria of quality and efficiency. One of the most important results of this type of audit is a formalized model of the examined business process.

The purpose of the IT audit is to improve the IT control system. To do this, the auditors should:
- Perform an IT risk assessment;
- contribute to the prevention and mitigation of information system failures;
- indirectly participate in IT risk management;
- help prepare regulatory documents;
- help link business risks and automated controls;
- conduct periodic audits;
- assist IT managers in properly organizing IT management;
- provide an "outsider's perspective."

In Russia, as well as abroad, there are six types of information technology audit services:
- IT survey,
- expert evaluation of IT,
- technical audit of IT,
- IT audit of BP,
- IT criterion audit,
- comprehensive IT audit.

This study examines the key issues of internal audit of IT risks of business processes due to its high and growing practical relevance.

The issues of risk-oriented internal audit are covered in sufficient detail in the International professional standards of internal audit, are touched upon in the works of Russian authors V.D. Andreev, S.M. Bychkova, V.A. Grinchenko, O.V. Ovcharenko, E.L. Skvirskaya, etc. The process-based management is also reflected in the works of V.V. Repin, E.V. Pirogova, O.I. Dolganov, A.M. Lobanov and other authors [1-19].

The study of publications of scientists and practitioners on this topic led to the following conclusions:
First, despite the existence of a considerable amount of scientific research in the field of risk-based auditing and process-based management, these publications are often of little relevance, are long overdue and do not sufficiently cover current trends.

Secondly, internal audit of business processes is covered fragmentarily and incompletely without reference to digitalization trends and peculiarities of the external environment.

Thirdly, there are no publications and methodologies on internal auditing of business processes, taking into account IT and digitalization risks.

2 Methodology
Based on the findings of the study of scientific papers on internal audit, process-based management, IT risks, we set the following goal in this work - to adapt the internal audit system to modern changes in the external environment of the organization through the consideration of IT risks in business processes in order to improve the effectiveness of the audit.

To achieve this goal, we set and solve two tasks:
1. To define and systematize IT risks of business processes.
2. To develop and test the methodology of risk-based internal audit of processes with IT risks.

To solve these tasks we will apply the following methods.
- The method of scientific literature analysis to study the current state of the scientific research problem.
- Methods of monitoring and statistical analysis of IT risks for their subsequent classification.
- Method of synthesis of risk-based audit approaches and process management building trailers.

3 Results

During the study, the authors identified the following main IT risks in the field of Information Systems and IT, which can be applied in most cases for the purposes of rating the riskiness of processes:
1. Risks of information loss due to lack of backup scheduled backup (information is lost in case of force majeure failures in the system).
2. Risks of information loss due to disorganized operational preservation of information (in case of power outages, power surges, or employees' failure to save data during work).
3. Risks of information loss, impossibility to find quickly the needed information due to the absence of file storage system, uniformity of file naming.
4. Risks associated with the possibility of cybercrime by remote access.
5. Risks related to human factor:
   - Manual data processing, information input into the Information Systems (possible distortion of information, input of incorrect data, etc.);
   - Errors of unqualified users;
   - absence in the system of automatic restrictions from unacceptable actions of the user of Information Systems (for example, re-starting in production of an order, which has already been started in production).
6. Risks associated with irrelevant or unupdated software or hardware (which leads to system failures, irrelevant data in Information Systems).
7. Risks associated with poor quality or lack of maintenance of equipment, non-compliance with operating standards.
8. Risks, connected with impossibility of the following upgrade of Information Systems, incompatibility of Information Systems (this kind of risk is especially actual when choosing Information Systems for purchase, in case of such risk the company is forced to replace Information Systems with the optimal Information System, which is fraught with financial expenses).
9. Risks associated with the lack of uniform standards, instructions for working with Information Systems (this risk leads to errors of employees in working with Information Systems, the need to start working "from scratch" due to the lack of standards for the work in case of staff turnover).
10. Cybersecurity risks in terms of theft of commercial information, scientific developments.
11. Risks associated with the lack of restricted access rights.

The specified risks are the most widespread IT-risks and are applicable to the enterprises of practically any industry.

It should be noted that in the field of IT risks, a special risk assessment is performed by involving subject matter experts in order to determine the areas in which these risks can materialize. The risk assessment is updated in anticipation of business changes on a regular basis to ensure that the most important areas of added value are addressed in the audit plan.

The grouping of IT-risks by types of expert evaluations is presented in Table 1:

<table>
<thead>
<tr>
<th>Type of expert risk evaluation</th>
<th>Serial number of the risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>assessment of IT projects or design solutions</td>
<td>8,9</td>
</tr>
<tr>
<td>assessment of the feasibility of IT investments</td>
<td>8</td>
</tr>
<tr>
<td>assessment of the value of the IT component of the company</td>
<td>8</td>
</tr>
<tr>
<td>assessment of current IT projects</td>
<td>9</td>
</tr>
<tr>
<td>assessment of the possibility of IT infrastructure conversion</td>
<td>8</td>
</tr>
<tr>
<td>IT operations management assessment</td>
<td>1, 2, 5, 6, 7</td>
</tr>
<tr>
<td>IT training assessment</td>
<td>2, 5</td>
</tr>
<tr>
<td>Assessment of hierarchy, composition of IT components</td>
<td>3</td>
</tr>
<tr>
<td>IT infrastructure information security assessment</td>
<td>4, 5, 6, 10, 11</td>
</tr>
</tbody>
</table>

The following hierarchy of investigated principles and methods was applied in the course of the study:
- internal audit as the basis for building the methodology of business process analysis,
- principles and methods of process-based management as a basis for audit,
- risk-oriented approach as an update of the proposed method in view of external and internal trends of digitalization, other external factors.

In the course of the study, according to the objective, as a synthesis of data, the methodology of internal audit of IT risks of business processes is developed:

1. Compilation of the company's BP architecture. At this stage it is necessary to break down all the activities of the company into BP, to develop the architecture of processes. All activity of the company (the whole cycle of working activity) is divided into essential stages for easy perception of BP structure. So at this stage it is important for each BP to define the owner, the boundaries of processes. It is with the owners of the processes will interact with the internal auditor to clarify the necessary information.

When decomposing processes and especially when presenting decomposition results, it makes sense to use a graphical representation of information as much as possible. At this stage, it is advisable to use BPMN notation (Business Process Model and Notation).

2. Detection of processes using IT technologies. This step requires obtaining information about the functions that make up the process. By interviewing process owners it is necessary to build process diagrams in EPC notation. EPC (Event-Driven Process Chain) is a notation of the process representation, the key elements of which are events and functions. Next, business processes are defined, at execution of which an IT risk occurs.

These processes should be analyzed in the next steps to eliminate or minimize IT risks, an example is shown in Figure 1.
3. Identification and assessment of IT risks, the formation of a risk map linked to the BP, an example is shown in Figure 2. The main objective of this stage is to obtain the output of the list of risks, arranged in descending order of importance.

Fig. 1. Author's process flowchart in EPC notation with indication of risks with linkage to functions

4. Formation of an action plan to eliminate risks, including the minimization of risks, both initially defined and identified in the course of the audit.

This methodology was tested and applied on the basis of scientific and production enterprise. The main business processes were described, process owners and process boundaries were determined. As a result of the internal audit of business processes, IT risks were identified and recommendations for their elimination or minimization were developed. The main recommendations of internal audit of IT risks of the company are given in Table 2. There was also a recommendation to update the internal control system, as part of the recommendations were partially implemented, but not executed due to lack of proper control or understanding of the employees' job responsibilities. In general, the proposed measures have a long period of implementation and testing. In this regard, the effect of their implementation can be analyzed in the digital equivalent later. As of today, we can clearly state that the implementation of the recommendations will make the IT system of the enterprise more stable, and the activities of employees more regulated and controlled.
4 Conclusions

So, as a result of the research of scientific literature and works of practitioners in the field of internal risk-based audit, process-based management by analyzing scientific literature, the authors concluded that it is necessary to update these methods taking into account the realities of the external environment, digitalization, to develop a methodology of internal audit of IT-risks.

This work also formulates the basic concepts of research and defines their relationship: business process, information technology risk (IT-risk), IT-audit of BP, IT-audit objectives are defined.

To achieve the set goal, a study of actual IT risks was conducted, a list of basic risks applicable to most companies regardless of the industry was developed, grouping of IT risks by types of expert assessments for complete coverage of possible key IT risks was given.

As a result of the study, the methodology of the internal audit of IT processes was developed. The activities of the organization as a whole are considered through the prism of the process-based management, taking into account the main risks of digitalization in the area of business processes.

Table 2. Key recommendations for internal audit of business processes of IT-risks on the example of a manufacturing enterprise

<table>
<thead>
<tr>
<th>Risk number</th>
<th>Recommended changes in the company's activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Moving to more stable CPU solutions for servers, to eliminate the error of operation, leading to a complete reboot of the server.</td>
</tr>
<tr>
<td>2</td>
<td>Placement into service of software with auto-save. Replacement of outdated uninterruptible power supplies. Repair of air conditioning system in the server room for the summer period.</td>
</tr>
<tr>
<td>3</td>
<td>Sorting the storage system by introducing PDM (Product Data Management). Full backup on a weekly basis, change tracking on a daily basis.</td>
</tr>
<tr>
<td>4</td>
<td>Restrict access to the remote desktop in favor of a VPN (Virtual Private Network) connection.</td>
</tr>
<tr>
<td>5</td>
<td>Developing a cybersecurity policy, updating job descriptions and employee work regulations. Briefing employees on cybersecurity.</td>
</tr>
<tr>
<td>6</td>
<td>Weekly updating of software for all departments.</td>
</tr>
<tr>
<td>7</td>
<td>Monthly audit of work equipment, PCs, servers, office equipment, etc.</td>
</tr>
</tbody>
</table>
In order to implement this methodology, it was tested at a specific enterprise: the company's BP architecture was made, IT risks were identified and assessed, a risk map with reference to BP was formed, processes using IT technologies were identified and described. Based on the results of the internal audit of processes a plan of measures to minimize or eliminate risks has been developed.

5 Acknowledgements

This paper has been supported by the «Kazan Federal University Strategic Academic Leadership Program».

References


4. V.D. Andreev, Complex risk-oriented audit of commercial organizations: textbook (Moscow: Magister: INFRA-M. 245, 2016)


6. V.V. Eliferov, V.V. Repin, Business processes: regulation and management. (Moscow: INFRA-M, 2020)


8. V.V. Ivanchenko, Information Technology Audit. Vestnik MFUA 1 (2015)


18. V.V. Repin, Business by the rules: regulations must work: a practical guide (Moscow: INFRA-M, 2020)

19. V.V. Sorokobatkin, Young Scientist 21(155), 244-246 (2017)