HOW CAN ISO MANAGEMENT SYSTEMS STANDARD CONTRIBUTE TO MITIGATE BUSINESS RISKS?

Irena Kogan and Valentin Nikonov

Working Party on Regulatory Cooperation and Standardization Policies
ECONOMIC COMMISSION FOR EUROPE

Groupe de travail des politiques de coopération en matière de réglementation et de normalisation
COMMISSION ÉCONOMIQUE POUR L'EUROPE

Рабочая группа по политике в области стандартизации и сотрудничества по вопросам нормативного регулирования
ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ

How can ISO Management Systems Standard contribute to mitigate business risks?

By Valentin Nikonov& Irena Kogan

Abstract

Saying 'apply risk management' to businessmen and entrepreneurs is similar to advising 'buy low, sell high'. Everybody understands that risk management is an important tool; however practical application of this methodology is still a big issue. Sophisticated tools and methods may seem too abstract, while implementation of a generic risk management process hides too many practical questions. Risk management standards come from different spheres (banking, accounting, internal auditing, security), and address different steps of the risk management process for different types of risks.

Risk management methodology can be implemented efficiently only if there is a risk management system. In the report, we focus on practical aspects of risk management and present a concept of its application by the means of implementation of an integrated risk management system. The concept is based on well-known international management systems standards.

Risk management – problems of practical implementation

Risk Management can make quite contradictory impressions - on one hand, its development gave birth to numerous mathematical models, formulas, graphs and consequently – to Nobel Prizes in Economics. On the other hand – its concepts are very simple. Basic risk management process, which is presented in various ways in different standards, can be described quite simply:

- We need to know what we are 'protecting': our strategy, assets, society, health, efficiency of markets, etc. (different levels of management have different objects);
- We need to know what are the risks (what are the events that may occur, why they may occur, how probable they are and what impact they will

have on us) and to know them as broadly as possible – this is the **identification** stage;

- We need to understand the risks that are the most important for us, and for these purposes their **quantification and evaluation** is required;
- Then, starting with the most important risks, risk management strategy must be chosen (we can accept the risk, avoid it, mitigate or transfer) – this stage can be called '**determination of the risk management strategy**';
- After the decision is taken, it needs to be implemented – that is the palpable result of the risk management process;
- As a 'bonus' step, we need to make a **'crisis management' plan** for the risks that we accepted and for those that we mitigated. This results in an action plan in case the risk occurs. It is a very important conceptual stage in the risk management process since risk management is a tool for achieving adequate, not absolute safety. Quite seldom risk mitigation can lead to a situation when the risk is lowered to zero. The idea is to know the risks and to be at least prepared for them.

Thus saying 'apply risk management' to businessmen and entrepreneurs may be similar to advising 'buy low, sell high'. Everybody understands that risk management is important; however practical application of this methodology is still a big issue. 'Nobel lectures', sophisticated tools and methods (that usually address risk quantification issues) may seem too abstract, while implementation of a generic risk management process hides too many practical questions. In the paper, we focus on practical issues and present a concept of implementation of systematic RM into business practice which is based on well-known international management systems standards.

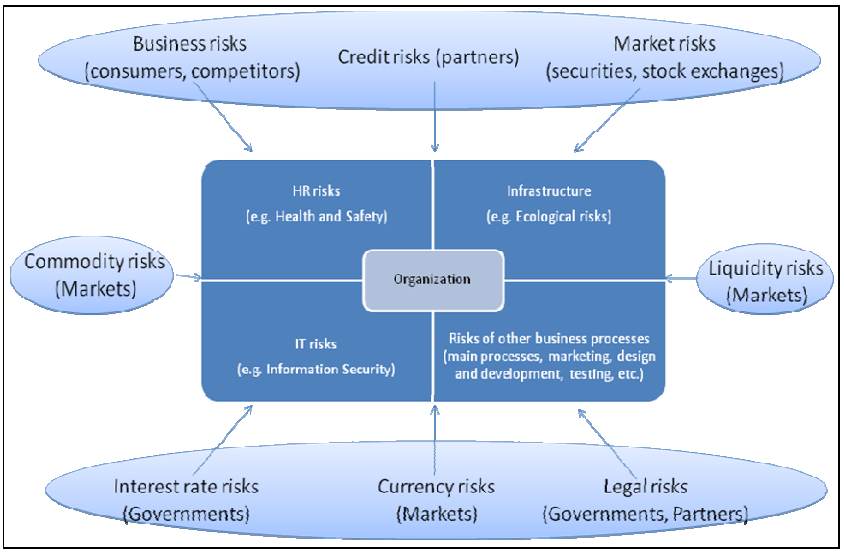
Preparatory steps: necessary conditions to risk management implementation

Different risks are managed with different tools and methods. Standards, internationally recognized methodologies are tools that may help organizations efficiently implement these techniques. They come from different spheres: from banking and finance (Basel II), from financial reporting and accounting (Sarbanes Oxley Act), from internal audit practices (COSO Integrated Risk Management Framework), from security provision (ISO/IEC 27001:2005), etc. These standards cover different risks and different steps of risk management process. At the same time, there is one important unifier: to make them all work organization first needs to create a solid basis - which is the same for all these standards and methodologies.

ISO Management Systems Standards should play a key role in risk management implementation because they create necessary conditions for successful functioning of risk management processes. The key word in the titles of ISO MS Standards for quality, environment, IT, etc. is the word 'system'. And Risk Management could be implemented efficiently into business practice on the basis of the same principles as other management systems. Reasoning for that is quite obvious:

1. **In order to manage risks systematically, organization needs a risk management system. To build a risk management system, organization, in the first place, needs to develop a transparent process and technology management system.** ISO 9001:2008, if treated like a standard for a 'general management system' has proved to be a convenient tool for implementation of a process management framework which is efficient for enhancing organization's technologies.

2. **Implementation of the operational risk management system is a key to successful enterprise wide risk management.** All organizations are influenced by a wide range of risks:



Picture 1

Some of these risks are internal - the 'reside' in business processes (they are also called operational risks), like HR risks, IT risks, infrastructure risks, etc. Other risks have external roots - they come from markets, partners, consumers, governments - like legal risks, market risks, business risks, etc (see Picture 1). These risks are managed **by business processes**.

Hence the second step to successful implementation of a Risk Management System is the development of operational risk management technologies. Operational risks are the risks of business processes; it is strictly defined in Basel II as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Again, as it will be shown later in this report, ISO/IEC 9001:2008 is a very good standard for operational risk management.

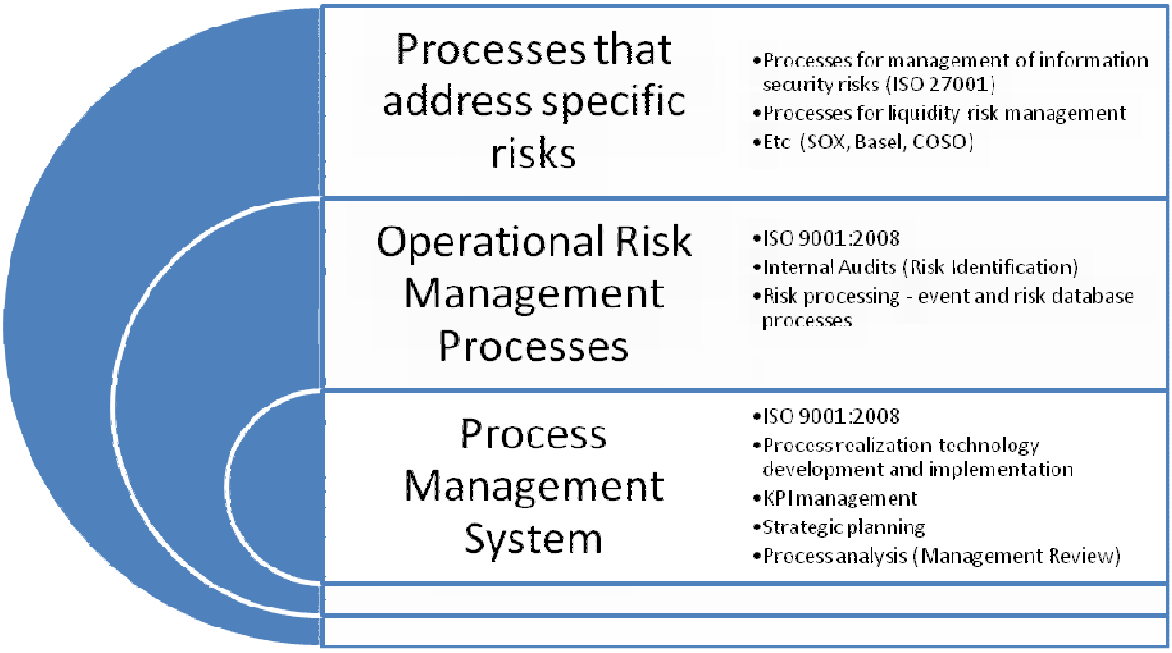
3. **Depending on the nature of risks that may impact organization, the processes that address these specific risks must be developed and integrated into a process management system**. Different standards provide tools for managing specific types of risks: ISO/IEC 14001 – ecological risks, ISO/IEC 18001 - occupational health and safety risks,

Sarbanes Oxley act was developed to ensure sound management of risks of errors in the financial reporting, etc. Systemic management of these risks can be achieved if special processes for managing these risks are implemented. These processes should not be treated as 'special processes' – they are like all others, like, for example, the marketing or sales processes, etc.

If these three steps are realized, organization will build a risk management system which won't be 'a thing in itself'. It will serve as a tool for implementation of the right actions (changing the technologies of the business processes, launching new projects – the only palpable result of risk management) to achieve profitability and safety – a common risk management objective for all organizations.

The structure of a Risk Management System

If the necessary conditions that were outlined above are met, risk management system would have the following structure:



In other words, implementation of risk management requires sound preparation. Implementation of the process management framework and development of the operational risk management processes are the necessary preliminary steps to

efficient risk management. **Process management framework and operational risk management processes are already addressed in the ISO 9001:2008 International Standard.** If the requirements of the standard (which is usually referred to as to a quality management system standard and not risk management standard) are treated in a specific way, the resulting system can be described as follows:

1. All organizational activities are divided into business processes. A process can be presented as a set of functions that result in something that has value for organization. The process inventory can be developed in the information system; to give an impression of what it is like, below on the picture it is shown in Lotus Notes:

Код	Название	Куратор	Ответственный	Цель	Критерий успеха
Выполнение трансферагентских функций					
33	Выполнение трансферагентских функций	Водопьянов С.Ю.	ДРК	Назначение регламента «Осуществление трансферагентских функций» - организация приема и обработки заявлений застрахованных лиц, поступивших в Филиалы Негосударственного пенсионного фонда «БЛАГОСОСТОЯНИЕ», заключившие с Пенсионным	о Отсутствие нарушений, связанных с выполнением своих обязанностей по Соглашению о взаимном удостоверении подписей. о Отсутствие жалоб, замечаний из территориальных органов ПРФ и иных государственных органов, положительные акты проверок, составленные сотрудниками ПФР и иными должностными лицами,
Инвестирование средств пенсионных накоплений					
30	Формирование стратегии инвестирования пенсионных накоплений	Демидов Д.Л.	ДУА	Определение оптимальной структуры инвестирования пенсионных накоплений для получения доходности, превышающей уровень инфляции на интервале 5-ти лет, при максимально допустимых рисках.	Утверждение Советом Фонда целевых показателей дохода и доходности по пенсионным накоплениям на предстоящий год.
31	Инвестирование пенсионных накоплений через управляющие компании	Демидов Д.Л.	ДУА	Достижение уровня доходности, определенного Стратегией, за счет эффективного перераспределения средств, переданных в доверительное управление.	Доходность по пенсионным накоплениям не ниже целевых показателей.

2. For every process a **technology of its realization** and a key performance indicator are determined.

3. Organization develops a 'process management framework' where it determines how the technologies of the business processes are developed, approved, implemented and analyzed.

4. When a process functions it becomes a subject to Internal Audits – this is an important tool of risk identification. During Internal Audit it can be found out:

    a. That the process conforms to the agreed technology;

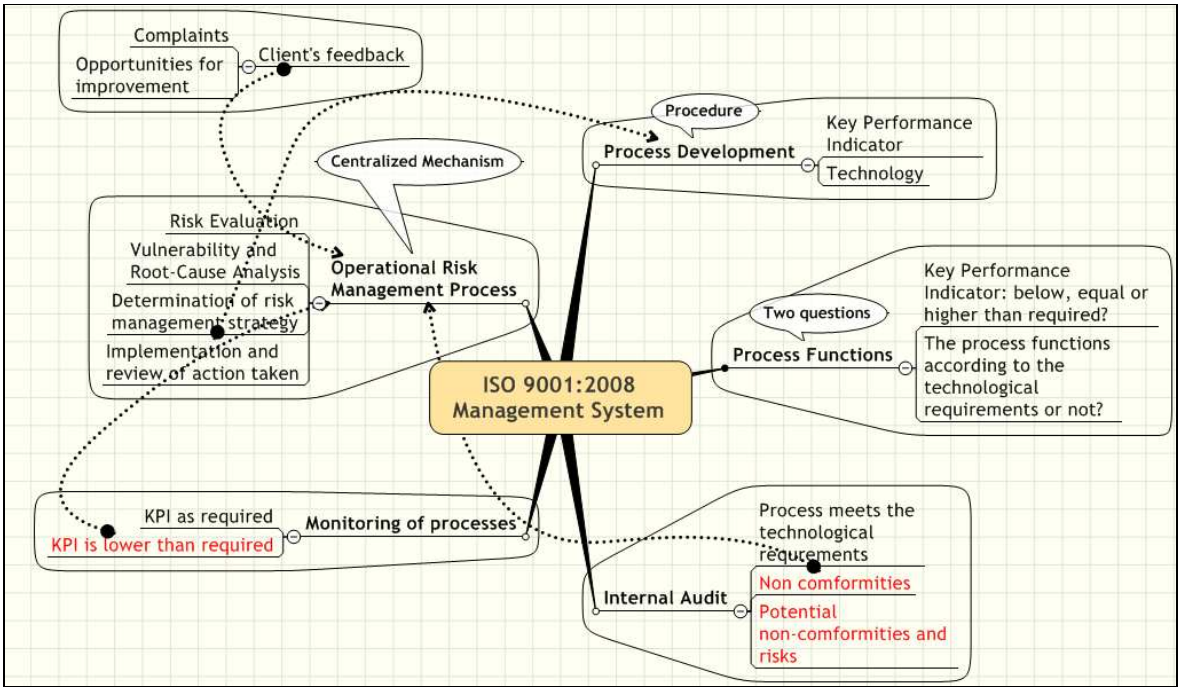
b. There are non-conformities (realized risks);

c. That there are risks in the business process that must be addressed.

5. Continual monitoring of processes provides management with information on whether they meet the planned result. If a process doesn't meet the planned result, this fact is also treated as a realized risk that must be registered.

6. There is a centralized mechanism for risk processing (aligned with requirements for corrective and preventive actions): if any deviation (a realized risks) or a risk is identified during the audit or monitoring, or a risk was spontaneously identified by any employee, or it is identified during the analysis of customer feedback, it is a subject to a general, operational risk management process. It includes risk evaluation, vulnerability and root-cause analysis, determination and implementation of a risk management strategy. Different software solutions are present at the market for automation of this process.

7. The whole system functions as presented on the picture below:



As a result, the system provides systematic and consistent risk management actions for all processes of organization – that is for all organizational activities. Any risk identified should be processed in a similar consistent way. But this is only a ground for a corporate wide risk management: since risks differ from organization to organization, the issue is how to identify the risk and which management strategy to choose.

Here the standards are also of great help. In addition to operational risk management process, ISO 9001 gives organizations advice on where to look for and how to deal with specific risks. Competence management is one of the most important mitigation strategies for Human Resources risks, described in clause 6.2 Human Resources. To manage infrastructure risks, the organization should conform to the requirements of clause 6.3 Infrastructure. The suppliers and partners risk mitigation strategy is described in clause 7.4 Purchasing. Development of supplier evaluation criteria and the supplier systematic evaluation makes an organization less vulnerable to these external risks.

Adding special processes for specific risks

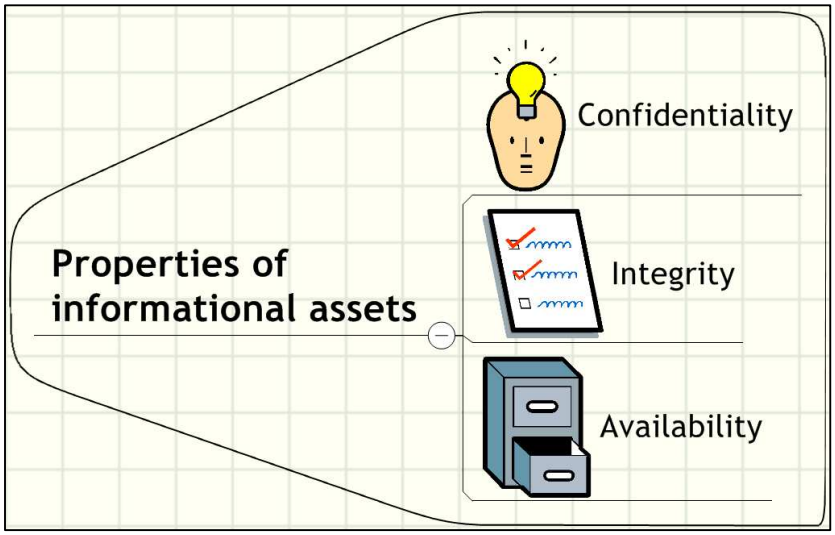
Of course ISO 9001:2008 doesn't address all the risks that organization faces: it doesn't have anything about interest rate risks, market risks, liquidity risks, information security risks, etc. But if there is an operational risk management system in place, it becomes clear what to do to manage these risks systematically. Organization needs to develop special processes, which should be integrated into process management system (literally – added into the table on Picture 2). That is the third 'layer' of the risk management system. To get this done, various standards and methodologies could be of great help – they contain recommendations on how to 'tune' these processes.

When these 'processes for specific risks' are implemented (these are 'usual routine processes' – they may have different technologies and key performance indicators), they function within one operational risk management system; these processes are systematically audited, analyzed and improved. This allows organization to systematically manage all the risks that may have an impact on

its work, and what is very important - also to manage **internal risks of the risk management processes for external risks**.

Let's take an example of information security risks. If organization wants to manage information security risks, additionally to existing processes, it implements the processes that are described in ISO/IEC 27001:2005.

Information Security risks are events that change the levels of confidentiality, integrity and availability of informational assets, leading to unexpected costs and losses for a business. In the terminology of ISO/IEC 27001:2005, everything that has value for organization and is somehow related to information – software, documents, servers, computers, databases, employees etc. - is an informational asset that **must be protected**. Without going into the details, any informational asset has at least three properties that shall be protected: confidentiality, availability and integrity (picture 4).



The degree to which confidentiality, availability and integrity of an asset in reality corresponds to the required level determines the state of the information security of this asset.

The information security risk management process differs little from a general risk management process – the concepts and functions remain the same. However, there is a difference in the technology of risk identification and in the methods for determining the risk management strategies. This is where ISO/IEC

27001:2005 is particularly helpful. It gives recommendations on how to identify informational security risks (for example, to develop a process 'management of informational assets'), and measures for mitigating these risks. These are given in Annex A of the standard.

Another example - If organization wants to comply with the Sarbanes-Oxley Act, which requires development of a system for Internal Control for Financial Reporting (required by 404 SOX) it should also consider it to be a part of an overall operational risk management system. The logic here is absolutely the same as with information security risks: financial reporting risks are those operational risks that lead to financial misstatement. The organization just needs to determine the financial statements preparation process (to add it to the process inventory), and to understand from which processes (departments) the information is being received for the preparation of statements. After that - to perform risk assessment for each account and for each process and to determine the risks that may lead to financial misstatement. Then to process these risks within the operational risk management system based on ISO 9001:20008.

Apparently, if organization creates a three level risk management system, it can implement consistent management of all the risks that may influence its competitiveness. The process management framework is the core of this system: to prove that risk management really works we need to see how processes are changed as a result of the risk analysis, how new processes and projects are developed and implemented.

Case study: integration of information security risk management into operational risk management system

Bank24.ru was the first financial institution in Russia that gained ISO 9001:2000 and ISO 27001:2005 certification. General operational risk management system was built on the basis of ISO 9001:2000 in 2003, processes for management of information security risks were integrated into the system in 2007.

Banks and other financial institutions are special organizations in terms of risk management. Like for insurance companies, risk management processes for them are the main business processes. However, in terms of operational risk management banks are absolutely similar to any other organization. It is worth

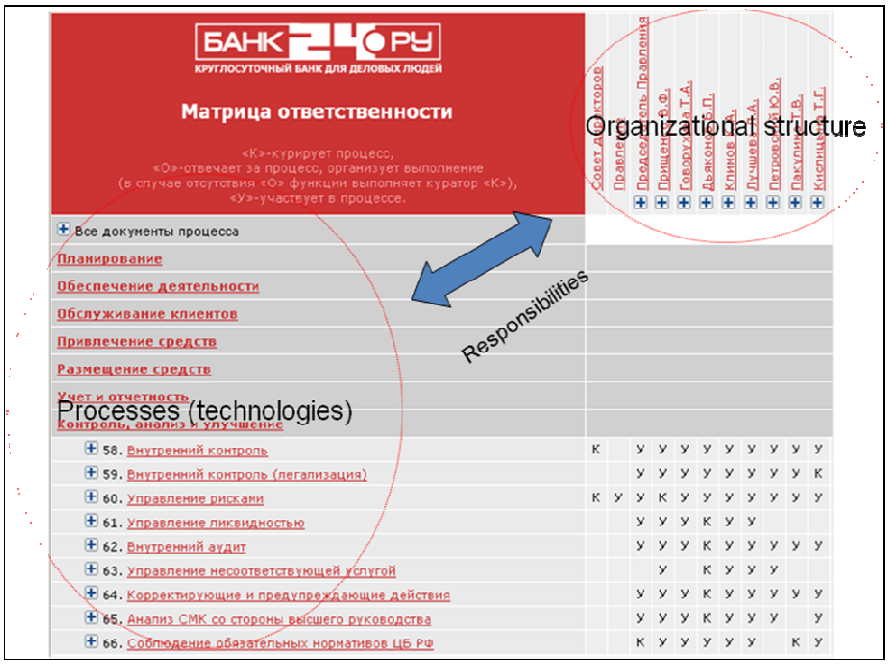
noting that regulators' risk management systems are very similar to those that function at banks: only instead of market and credit risk processes regulators manage the systemic risks of the markets being regulated; special processes and tools are required for these purposes. As it was shown above, to function efficiently these tools should be integrated into an operational risk management system.

In this case study, we'll show how information security processes were integrated into a risk management system. Information Security is just an example - other risk management processes can be added in a similar way.

Information security is very important since breaches of information security can cost a company dearly. Quoting the results of a survey into Internet security, the IT Governance Institute stated "The results show that announcing an Internet security breach is negatively associated with the market value of the announcing firm. The breached firms in the sample lost, on average, 2.1 % of their market value within two days of the announcement – an average loss in market capitalization of USD 1.65 billion per breach."

To describe how the information security risk management system (ISMS) functions at Bank24.ru, we should outline the bank's general operational risk management system which is based on ISO 9001. The quality management system standard defines procedures for managing the bank's business processes and operational risks.

The business processes are listed in Bank's Intranet in the business process inventory, where for each process responsibilities are assigned:



Each line in the matrix contains a link to a 'process Intranet site', where its technology and other valuable information is presented.

Aligned with ISO 9001 requirements for "corrective and preventive actions" is a procedure for establishing operational risk identification, evaluation, creating a working group, determining vulnerabilities and causes of risks, determining risk management strategy, and reviewing the effectiveness of its implementation.

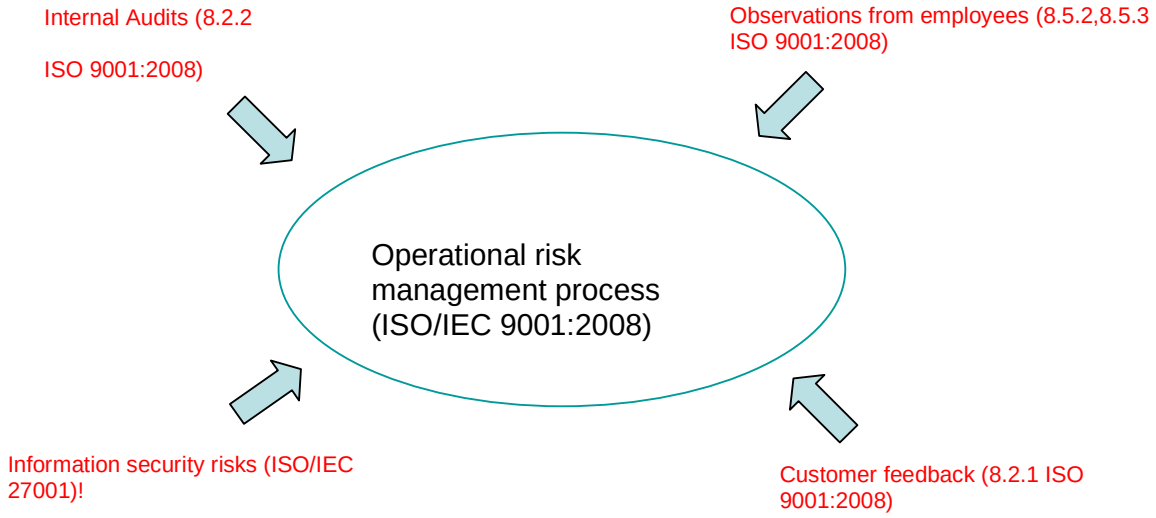
As it was shown above, the functions of such a risk management process – identification, evaluation, determination – depend little on types of risks that are managed. The main task is to find how best to apply these functions to a particular type of risk. Operational risk identification can be conducted in various ways. At Bank24.ru, information on operational risks is received from three key sources:

- From employees – any employee can register a non-conformity, i.e. a risk that has been observed or has already occurred – via special questionnaires in the Bank's Intranet
- From customer feedback –i.e. a claim (a risk that has occurred). Customer feedback analysis helps to identify risks
- From the results of internal audits providing systematic self-assessment.

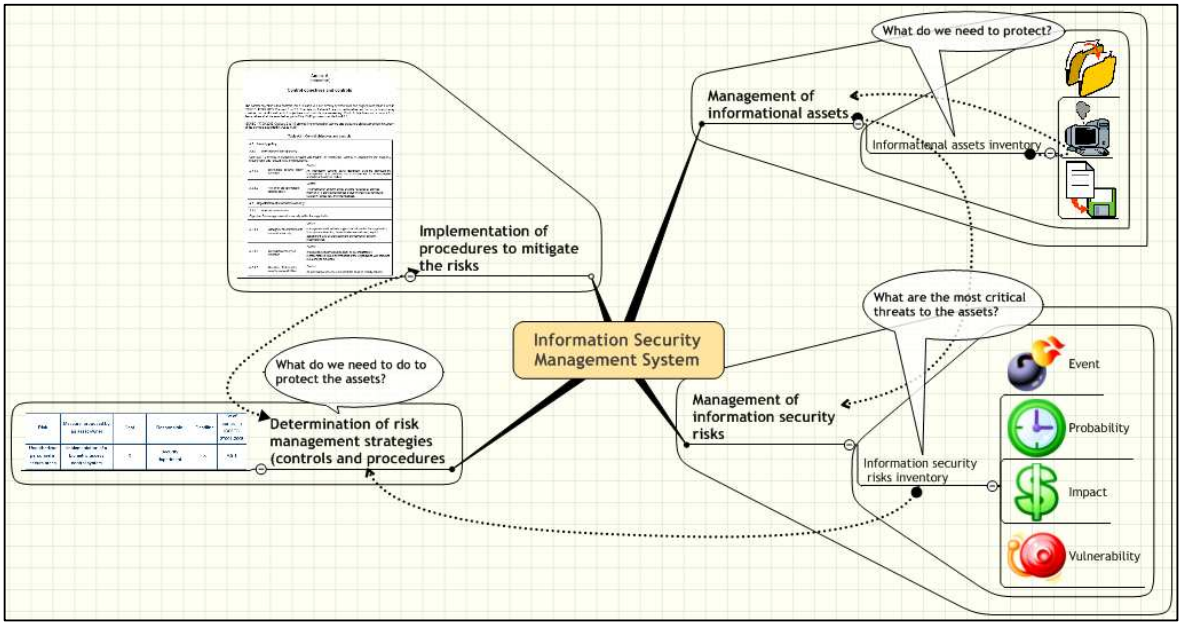
The information security risk management process differs little from a general risk management process – the concepts and functions remain the same.

However, there is a difference in the technology of risk identification and in the methods for determining the risk management strategies.

This is where ISO/IEC 27001:2005 is particularly helpful. It gives recommendations on how to identify informational security risks, and measures for mitigating these risks. These are given in Annex A of the standard. In general, the logical flow of operational risk management processes can be illustrated in the following diagram:



From an organizational perspective, information security risk management is governed by the information security coordination group which consists of representatives from various business fields (not only IT departments). The information security coordination group approves information security policies and objectives, systematically reviews the functioning of ISMS, and provides necessary resources. There are two main processes for information security risk identification: management of informational assets and management of informational risks. These two processes (described in clause 4.2 of the standard) establish the basic logic of a system:



- *Management of informational assets*. This process provides us with an answer to the question 'what are we protecting?'. For sound identification of information security risks we need to have at hand an actual inventory of informational assets, ranged by criticality. For this purpose, 'management of informational assets' procedure is implemented at the Bank. This is one of the key processes of the ISMS. The logic here is very simple: since the information security risks lead to changes in the properties of informational assets, the inventory of these assets must be available for members of Information Security Coordination Group, Information Security Department, as well as for the business owners and top management. In the inventory for each informational asset the following properties are determined: the levels of confidentiality, availability and integrity; a resulting level of criticality, the owner and the users of an asset. The informational assets management process is a process of actualizing this inventory. In general, the inventory may look like the following table (it just an example, it is not a real bank's inventory – the Bank's inventory is highly confidential!):

Name	Confidentiality	Integrity	Availability	Criticality	Owner	Users

Clients database	*High*	*High*	*High*	*High*	*The head of sales division*	*Sales division*

Given an answer to the question 'what are we protecting', we need to get an answer to the next questions 'what are the threats? From what are we protecting the assets?'. For this purpose, the information security risk management process functions within the system.

- *Information Security Risk Management Process.* Information security risks are identified for each informational asset. There are two approaches for risk identification: spontaneous (any employee can register a risk when she sees it) and systematic. Systematic information security risk identification is conducted by the information security department. It doesn't mean that the information security department identifies the risks: risks are identified by the owners of the assets. Information security department moderates the process - its responsibility is to make information security risk identification happen, to accumulate and analyze the information, to evaluate the risks. Information security department also quantifies the risks (when it makes sense), and together with the asset owners they determine the risk mitigation strategy. As a result, we get a list of risks that starts with the most critical ones at the top (the least critical at the end of the document). The report is reviewed by the information security coordination group: one of the main roles of it is to provide resources necessary for risk mitigation.

  After we find out the threats, we can turn to determination of adequate protection measures (risk management strategies).

- *Determination of risk management strategies.* Risk management strategies are determined on the basis of risk analysis. The information security risk management strategies are implemented in the very same way as other operational risk management strategies – the are the subject to the same procedure.

Most commonly, the mitigation of information security risks implies implementation of special procedures. For example, to mitigate the risk of an unauthorized access we need to implement the 'Access control' procedure. In the annex A of ISO/IEC 27001:2005 there is a list of standard controls – procedures that can be implemented to systematically mitigate the usual risks. Unless organization has accepted a risk (such decisions shall be documented), implementation of a respective control is a requirement. Without going into the details, the following procedures are recommended in the standard:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Thus, the information security risk management process may have a following table as a result:

Risk	Measure, proposed by an asset owner	Cost	Responsible	Deadline	№ of control in ISO/IEC 27001:2005
Unauthorized personnel in secure areas	Implementation of a biometric access control system	X	Security department	X	A.9.1

As it is shown in the table, for each risk we determine: what to do with it, how much it will cost, who will implement the measures and when the measures must be implemented.

The Bank implemented a list of measures to provide systematic and adequate information security. Almost all the processes specified in the Annex A were implemented – they mitigate most common risks. At the same time, some of the procedures that were implemented were not required by the standard, and some of the controls in the Annex A were excluded since the respective risks were accepted by management. Now these procedures are regularly analyzed during internal audits and management review. That guarantees their effective and efficient functioning and creates basis for continual improvement.

Since security measures were implemented on the basis of risk analysis, the Bank didn't have to implement excessive security measures. Moreover, if the business owner wanted to accept the risk and not to spend money in its mitigation, this decision was registered in the risk inventory. Absolute safety costs a lot and could never be reached – and this kind of flexibility in decision making is one of the best features of Risk Management Methodology which aims at providing organization with security measures that are not more and not less than needed and don't hamper development.

Conclusion

The case study and examples of types of risks that were presented in the report were chosen to how risk management works in practice. Certainly the concept presented above could be applied to any organization at any level.

Regulators have a very special role in risk management implementation. The following steps could help raising the efficiency of risk management application:

1. The principles of risk management implementation are the same for all parties involved in the process. Both regulators and business organizations need a sound transparent risk management system with methodologies and tools for management of specific risks integrated into it.

2. The existing risk management standards come from different spheres, and their application often results in creation of different independent systems. A better cooperation of regulators and business players in the

field of risk management and unification of risk management methodologies would help to better understanding of risk management practices.

3. Development and promotion of internationally recognized standards and guides (especially for **a risk management system)**, which would help organizations to build risk management systems on the basis of existing international management systems standards (especially ISO/IEC 9001:2008) would be beneficial for a number of reasons:

    a. It would be 'a low-cost' way to promote risk management practices: it requires only to make a shift to risk management approaches in the existing management systems which are well-know and widely applied in the business world;

    b. There is a certification scheme which provides additional expertise of the risk management systems and is an efficient tool of conformity assessment;

4. Business players and regulators have a shared interest in risk management: while businesses manage the risks that may impact their profitability and competitiveness, for regulators risk management job is way more complicated – by imposing regulations they manage systemic risks, those that may impact society and/or the whole market. Forming a risk management culture and establishing better communication in terms of risk management between regulators and business players could raise understanding and the efficiency of regulatory measures.

5. Development of specific tools for regulators for management of the systemic risks would raise the efficiency of cooperation between regulators and business players. These tools should include:

    a. Unified scale of impacts for ranging the risks which would be recognized by business players and regulators. This would help achieve clear understanding by all stakeholders the rationale for implementation of the regulatory measures.

b. Risk assessment methods for evaluation of the adequacy of the regulatory measures (they should be further developed).

c. Methods for risk management in the process of imposing a regulation.

d. Methods for performing symmetric analysis 'risk – regulation' in order to find excessive regulation of the economy (new risks emerge, old risks disappear).

Risk management is only a tool and by no means is it a panacea. It doesn't provide advice on what to do with a particular risk, it only gives some guidance and a framework for decision making. Further development and implementation of tools and methods for systemic risk management on all levels is an important task. It will increase the efficiency of business organizations, markets and economic regulations. This, in turn, will raise the level of transparency, stability and predictability of the interlinked economic systems.