Opportunities of Using IT Compliance Tools as an Organization's Management Function

Nikolay Vladimirovich Kuznetsov
Financial University under the Government of the Russian Federation, Russia.

Stanislav Borisovich Reshetnikov
Financial University under the Government of the Russian Federation, Russia.

Sergey Nikolaevich Silvestrov
Financial University under the Government of the Russian Federation, Russia.

Sergey Alekseevich Pobyvaev
Financial University under the Government of the Russian Federation, Russia.

Received April 15, 2021; Accepted July 20, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18SI04/WEB18198

Abstract

The present article deals with the study of the application and regulatory consolidation of the IT compliance function in both commercial and state-financed organizations. In addition to studying the application of this function, the article focuses on the issues of building a compliance system in the organization. In the main part of the work, compliance is considered as a system of measures taken by an organization for its effective operation. A detailed analysis of the advantages and disadvantages of the concerned system is presented, as well as the authors’ assessment of the risks and prospects associated with the implementation and application of the compliance methodology within the enterprise.

Keywords

IT Compliance Management, Compliance Function, Compliance and Ethics, Risk Management.

Introduction

Strategic development of any contemporary enterprise is impossible without the implementation of information technology (IT) infrastructure. These days, companies, firms, factories, and enterprises that specialize in producing and providing people with various contemporary products are forced to develop in the context of constantly increasing technological progress in the framework of the innovative development of the
global economic system. Economic entities are forced to increase their innovative potential and keep up with trends in ensuring production chains, which leads to strengthening of the need to create safe management systems for enterprises and business in general. Enterprises also spend huge funds on training employees to meet the new management and qualification standards of the enterprise development paradigm.

In the 21st century, the concept of IT risk includes a wide range of potential threats to the company's well-being. It is necessary to give an example of some approaches of the world's leading scientists to understanding and designating today’s concept of IT risk of a company.

Turner offers expert judgment, plan decomposition, analysis of assumptions, decision-making motivation, and brainstorming to effectively identify risk factors in a project (Adair: 1984).


1. GOST R 50922-2006 is the main standard that sets a certain meaning of terms when working on standardization of enterprise’s IT environment protection.

According to this document, if the vulnerability is exposed to a threat, there is a risk of information technology security (Ahn et al: 2014).

The IT risk analytics is the process of systematic use of certain tools and methods to identify threats to information technology security, the emergence of threats and security vulnerabilities, as well as quantifying ways to implement such threats.

Information security risk assessment is the process of identifying the degree of resistance of the company's IT infrastructure to threats and potential damage.

2. GOST R 50.1.053-2005 standard classifies and describes the following concepts (Alm, Torgler: 2006):

- Threat (information security) is a set of conditions and factors that create a potential or actual risk of violating the confidentiality, availability, and (or) integrity of information (Akhmadeev et al.: 2016, 2019a; Abbasi et al.: 2005).
• The source of a threat to information security is the subject, material object, or physical phenomenon that causes a threat to information security.
• Vulnerability (of an automated information system) is a flaw or weakness in an automated information system that may result in the implementation of a threat to the security of the processed information (Akhmadeev et al.: 2018).

On February 4, 2019, the International Organization for Standardization (ISO) released the ISO/IEC 27005:2018 standard, in which unified risk management approaches for organizations of all types and sizes, regardless of whether they were public, private, or nonprofit (Braithwaite: 2007).

This document contains recommendations for evaluating existing control mechanisms to ensure compliance with the company's goal, efficiency, and effectiveness of management. Before the publication of the ISO/IEC 27005:2018 standard, the world practice used the ISO ISO/IEC 27002 standard developed in 2005 by ISO specialists based on the British information security standard BS 7799-1:1999 (Code of Practice for Information Security Management) (Braithwaite: 2007).

It is also important to note that since the beginning of the 20th century, the British Standards Institution (BSI) has been creating local-level standards, fundamental documents for the implementation of industrial, production, and technological international standards. For a long time, this Institution was engaged in creating an IT security management system – BS 7799. Companies, such as SHELL UK, Unilever, the British Computer Society (BCS), and many others have become partners when researching in this area.

The BS 7799 is approved as a United Kingdom government standard, which has been continuously supplemented and updated since 1995 (Fine et al: 2016; Harris, Lee: 2017; Johannsen, Kant: 2020).

Below are the retrospective view and development dynamics of information security standards and information technology risk management considered in more detail.

The British standard BS 7799 has become the de facto primary and fundamental global document in the field of IT risk management. The main provisions of this standard are still used voluntarily by many companies around the world. The use of this standard by a company indicates that it is a reliable market player with a well-built effective IT infrastructure (Guy et al: 2014).
It is important to note that BS 7799 has two parts with absolutely different methods of risk management in terms of used technologies: outdated, and in the latest iteration – more advanced.

The first part of BS 7799 was revised and transferred to the ISO in 1999 (Haynes: 2005).


In May 1999, BSI released the next iteration of the BS 7799-2:1999 standard, which contained a radically revised primary version. The new standard included a thoroughly revised version that addressed the methods and algorithms of ensuring IT security inherent at that time (Klotz, Dorn: 2008; Kniese, Bülchmann: 2015).

It is important to note that this version correlates with other generally accepted management system standards, namely, BS EN ISO 9001:2000 and BS EN ISO 14001:1996, aimed at ensuring consistent and integrated implementation and operation of these IT management systems.

The BS 7799 standard was not positioned as a technical security standard because it did not prescribe the implementation of certain methods of data encryption or hardware protection. This document contains classification of data, description of access systems, differentiation of employee responsibilities, and methods for using risk management assessment procedures (Koskella: 1983; Kosov et al.: 2017).

The BS 7799 provides a tool for managing the privacy of digital infrastructure, is used in companies of various sizes, i.e. small, medium, and large businesses. The BS 7799 standard is easy to use when protecting any type of infrastructure, including financial data, personnel data, and vendor data.

Given the above, the main goal of this management tool can be formulated as the creation of common methodology for developing, implementing, and evaluating the effectiveness of Information Security Management System (ISMS) (Kolben: 2004) (or information technology security and risk management system) applicable both in the context of commercial companies and state and noncommercial structures.

The ISMS brings together people, processes, and IT systems (Kosov et al.: 2018).
The ISMS ensures well-coordinated work of the security service, IT Department, and company management to assess IT risks.

The BS 7799 standard prevents IT environments against

- Unauthorized access;
- Unauthorized changes, ensuring its accuracy and completeness;

The BS 7799 standard provides the ability to securely use the internal intranet for various operators when required.

It is important to note that this tool focuses only on privacy. However, commercial companies suffer more from losses of data or financial assets.

Using information technology systems is associated with the following possible threats (Kogler et al.: 2016):

- Industrial espionage;
- Theft and vandalism;
- Power outages (Kolben: 2004);
- Computer piracy;
- Lack of proprietary software solutions and high-power hardware;
- Unscrupulous employees;
- Hackers;
- Hardware and software failures;
- Viruses (Kosov et al.: 2017);
- Natural disasters, and much more.

The ISMS developed according to BS 7799-2:2002 ensures the availability of a well-tested structure that initiates, implements, maintains operation and manages information technology security within the enterprise. The British standard BS 7799 has gained international popularity and found application in many countries worldwide.

The BS 7799 is supported in 27 countries around the world, including the countries of the British Commonwealth, as well as, for example, Sweden and the Netherlands (Kosov et al: 2019a). It has been adopted by Australia and New Zealand. This standard is considered as the basis for national standards by the Scandinavian countries; it has attracted great interest in the USA and Canada (Kostera: 2008).
Various forms of information technology, such as hardware, software, and networks, provide solutions to enterprise business problems. Organizations use new types of infrastructure, such as cloud computing and distributed systems, as well as advanced software products, such as computer-aided design (CAD), and computer-aided manufacturing (CAM).

Accordingly, a very frequent circumstance is the occurrence of cyber-attacks in the form of data theft, compromised accounts, destroyed files, and disabled or degraded hardware systems (Kirchler, Maciejovsky: 2001).

However, this is not the only IT risk that should concern the company's management. Information technology risk has strategic, financial, operational, regulatory, and reputational implications. Technology is a great tool in the right hands, but it also presents a pervasive, potentially dangerous substantial risk (Kosov et al.: 2020a).

Materials and Methods

Today, the classification of IT risks into qualitative and quantitative ones is widely practiced based on analysis and subsequent work with them. Quantitative and qualitative analysis methods are complementary processes of unified IT risk management. Quantitative analysis includes mathematical modeling, probability theory, and many other methods, whose results should be represented by numerical metrics. The obtained absolute values clearly show the severity of risk exposure.

Due to the abundance of legal provisions and body of rules, as well as almost continuous IT support for all corporate processes, compliance requirements are no longer limited to tax or information privacy issues. The point at issue is rather that the entire business activity of the company must be "compliant".

To do this, it is necessary to get an overview of the relevant compliance requirements:

- Providing availability of rules, as well as documentary requirements for use, which the company must comply with as a priority; they constitute the first and most important task area of the global IT compliance process;
- Creating a process organizing system, a set of procedural rules, and, if possible, automated control to monitor compliance with all IT compliance requirements that is an integral part of compliance with the company's complaint policy.
- Disseminating information to all employees of the company acting in relation to existing obligations, and, if necessary, clarifying the working terms with third parties (McEvoy, Stranlund: 2009).
• Documenting the information within the organization, as well as its monitoring.
• Creating a system of change management to respond to new developments concerning requirements (Kosov et al.: 2019b, 2020b).

The IT compliance is the proper control and protection of full-cycle information, starting from the way it is received and stored to its protection and availability (how it is distributed inside and outside the corporate environment). Internal compliance functions are determined by the policies, goals, and organizational structure of the business. External goals include meeting the needs of the client/end-user while protecting the company and the client against negative aspects. Specialized tools are used to continuously identify, monitor, report, and audit compliance.

Compared to IT compliance, IT governance is a function of managing and solving critical technical, strategic, and procedural processes. IT governance is a subset of the overall corporate governance process and in most cases is controlled by the appropriate specialist (Koskella: 1983).

Risk management is the practice of reducing and managing risks through system-based control, and therefore this practice is considered as an integral function of IT governance and IT compliance. Governance, risk and compliance (GRC) are an integrated strategy for effective and appropriate management of policies, processes, and controls. Integrative management of these three functions rather than pursuing individual goals can eliminate duplication and promote the safe dissemination of information and communications.

Below are considered some of the most well-known standards that affect compliance with contemporary global IT requirements (Yong et al.: 2008).

The Sarbanes-Oxley Act (SOX) of 2002 is a comprehensive law governing financial transparency and reporting. It was passed by Congress as a direct response to the illegal actions of Enron and WorldCom. Section 404 is the most important for financial reporting control.

The Gramm-Leach-Bliley Act (GLBA) was signed into law in 1999. It dictates financial institutions to manage consumer protection (through annual notifications) with their privacy policies. This law also requires appropriate internal and external guarantees, even against the threat of illegal obtaining of information by fraudulent means (Winther, Hillersdal: 2019).
The Federal Information Security Management Act (FISMA), passed in 2002, obliges the federal bureaucracy to ensure information security by requiring an annual review of systems (Morozova et al.: 2020).

Section II of the Health Insurance Portability and Accountability Act (HIPAA) sets out policies and guidelines for regulating information, especially protected health information (PHI), by insurers, health care providers, and employers that provide health insurance (McEvoy, Stranlund: 2009).

The 2001 Payment Card Industry Data Security Standard (PCI DSS) is an industry-wide recommendation introduced by MasterCard, Visa, and other credit card companies to protect the personal data of service customers and providers.

The Statement on Standards for Attestation Engagements (SSAE 16) came into effect in 2011 substituting SAS 70 as control reporting for service organizations. Data processing centers, Internet service providers, and web hosting service providers are common IT organizations that SSAE 16 applies to (Prinz et al.: 2014).

Basel III applies to the banking industry and helps to determine the amount of capital that banks must reserve to recover losses. This requirement affects the amount of capital because it requires software that can perform more complicated computing (Wang et al.: 2020).

The common goal of IT compliance is to create a technical, procedural, and strategic framework that provides the means to achieve and validate the company's legal and ethical integrity (Fig. 1). Providing protection mechanisms, policies, and procedures can help to avoid the following:

- Damage to corporate image reputation or consumer confidence;
- Lost revenue, market opportunities, or stock price (Rietveld, Koomen: 2002);
- Recovery costs (legal costs, fines, and judgments, acquired consumer protection, capital acquisition, and loss of productivity) (Sowa: 2010).

However, achieving these goals presents many challenges. First of all, these are the complexity and volume of new legal documents that are subject to the correct interpretation. Since the rules themselves are not accompanied by a specific roadmap, there are many industry guidelines and best practices that provide clarity and guidance.

Other problem-bearing issues include:
• Lack of education among employees;
• Shadow IT problems, such as personal mobile devices that bypass corporate IT systems;
• Unauthorized applications;
• Difficulties with service providers (cloud services and data centers);
• The role of social networks;
• The number of existing regulations, updates, and new laws.

Figure 1 Algorithm of the classic “compliant” system operation

To perform the most effective quantitative analysis and achieve set goals, two conditions should be met:

a. Availability of the completed basic project;
b. Availability of basic project sequences;

Therefore, naturally, quantitative analysis is impossible without preliminary qualitative analysis of the IT risks of the enterprise or project. The negative features of this type of analysis are its high cost and requirement for the availability of accurate data. It is suitable for use in large companies that can finance this costly analysis technology.

Qualitative analysis allows identifying possible types of risks, as well as the causes of occurrence, and scope of distribution. The qualitative risk analysis is mainly carried out at the stage of developing the company's business plan, while the advance analysis serves to obtain basic information before starting work on IT risks. Additional but also very significant results of the qualitative analysis should include determining the borderline values of possible changes in all project factors (variables) that are checked for risk.

IT risk management includes regular assessment and implementation of preventive measures to reduce identified risks to an acceptable minimum. The number of identified risks is directly proportional to the increase in investment in IT infrastructure. In the USA,
for example, the law requires companies to manage IT risks and develop the internal information technology infrastructure of enterprises or organizations (the Sarbanes-Oxley Act, adopted in 2002). Standards in the field of IT security, which must be followed by domestic enterprises, such as ISO 17799, BS 7799, and ISO 27001, also provide IT risk management mechanisms. Assessment of the latter allows the company to determine the optimal amount of expenses to provide IT security and intelligently plan measures to support it.

Unfortunately, there are no obvious rules that would state in which specific cases a particular method for conducting IT security risk analysis should be applied, such as CORAS, CORBIT, OCTAVE, or CRAMM (Fig. 2).

In Russian companies, the situation is complicated by the limitations of domestic software products designed to assess and manage IT risks.

Russian companies often suffer from the limitations of domestic software products, the lack of a competitive software market in the field of analysis, monitoring, and assessment of enterprise IT risks. Unfortunately, most of them are based not on IT risk management methodologies, but information security standards, such as BS 7799 or ISO 17799, and therefore allow determining the degree of compliance with a particular standard rather than the level of IT risks. Besides, they usually do not take into account the opinions of the owners of information assets when determining the amount of potential damage.

Concept

Normal security procedures and regulations no longer ensure the security of industrial companies' IT systems, exposing them to risks, such as disclosure of commercial secrets,
personal information about employees and customers, as well as theft of technologies and product samples.

Electronic crime has evolved from dilettantism and recreational hacking of corporate networks to organized groups of criminals in remote regions of the world connecting to companies' internal IT systems to steal operational and production data. Hidden behind national borders and laws, many criminal syndicates operate without fear of retribution. Data thieves maliciously hack into companies' IT systems with the confidence that governments in many countries, especially in Asia, will not be able or willing to extradite them or prosecute.

When analyzing any IT risk situation, it is necessary:

1. To identify participants in the risk situation (subjects);
2. To reveal objects related to the risk situation (what is affected by the risk);
3. To identify the characteristics and features of the conditions for the occurrence of a risk situation (individual approach);
4. To identify subjects that are affected by the current situation and goals that are affected by the occurrence of risk;
5. To identify the time or period of occurrence;
6. To identify the way of manifestation;
7. To identify the place of manifestation.

Next, it is necessary to determine the signs by which the IT risk situation was detected. At the next step, efforts should be directed to identify the cause-and-effect relationships of occurrence of risk conditions. By identifying the causes, the outcome of a particular risk or threat is determined. Next, an expert opinion is given on whether the resulting IT risk is translated into an IT security problem or not. If the IT risk is translated to an IT security problem, the latter is attributed to a certain class of risk problems depending on:

- Content (which area of the company's operation is affected: financial, production, logistics, etc.);
- Priority (requiring or not urgent intervention);
- The level of management for decision-making (according to the level of access to the solution of the problem by the company's specialists);
- Timeframe (long-term or short-term problems).
The next step is to put forward a hypothesis by the relevant departments and individual employees of the company about the reason that causes a certain consequence for the company. After the hypothesis is identified, the following methods and procedures are performed: specification and abstraction, synthesis and analysis, modeling, algorithmization, reengineering, and many other ways to solve the problem.

**Results**

At the current stage of technological development, there exist a huge number of IT threats to the enterprise.

The processes developed by the authors have been further applied in practice in IT risk management. The authors see risk management based on a step-by-step model, which can also be used to transform the effect of risk to the company's benefit (Fig. 2)

---

**Figure 2** Enterprise IT risk management model (IT security threat scenario) (compiled by the authors)
An especially important preliminary point for analyzing IT risks is the analysis of the external environment in which the company operates. According to the authors, the PEST method is an accessible and generally used research method. The analysis is carried out in four areas of market conditions, namely, political, economic, social, and technological (abbreviated as PEST).

Monitoring is at the heart of the enterprise IT risk management process. Monitoring is carried out by employees of the IT security department using routine periodic automated checks aimed at determining the compliance of the assessment of the vulnerability of the enterprise’s information technology environment with the risk, namely its quantitative and qualitative indicator.

The second stage is associated with the assessment and classification of IT risks, which includes the risk identifying process from both the external and internal environment, comparing the identified risks with the risk map, and ranking them by criteria. This stage allows determining the nature of the risk impact on the economic environment, as well as clarifying the context and nature of the threat.

Here one can also predetermine the strategic response, as well as a possible scenario for further work with IT risk.

Methods of qualitative analysis of the threat are mainly used.

The probability values are assigned to each of the threats.

At the third stage of management, the IT risks, already identified and ranked according to their impact, are considered in terms of the best and most effective option of the action taken to eliminate them, namely:

a) Elimination;
b) Mitigation;
c) No action is taken.

Conclusion

Various forms of IT, such as hardware, software, and networks, provide solutions to business problems. Organizations use new types of infrastructure, such as cloud computing and distributed systems, as well as advanced applications, such as
computer-aided design (CAD), computer-aided manufacturing (CAM), and enterprise resource planning (ERP).

The rapid development and spread of new information and telecommunication technologies have increasing impact on politics, economics, management, finance, science, culture, and other spheres of society’s life both within national borders and in the world in general.

Many companies create risk maps using probabilistic forecasts. Not only do they generate risk maps to reflect impact and probability, but they also demonstrate what risks look like when they are combined in one place. The value of such maps is that they reflect pooled experiences of all parties involved in the analysis. Besides, risk maps contain comprehensive information about risks in one place, which is easy to view. The base risk map captures both risk impact and its probability, and uses different scales:

- Low (probability of occurrence is below 30%), medium (from 30 to 70%), or high (more than 70%);
- Unlikely, possible, probable, or almost certain;
- Insignificant, unlikely, probable, highly probable, and expected.

During monitoring, audit, and verification processes it is necessary to meet the following requirements:

- Control over IT risks should be monitored for their effectiveness;
- Identification and assessment processes should be reviewed regularly and whenever significant changes occur;
- The IT risk management process should be periodically audited to ensure that deficiencies are identified and eliminated to ensure continuous improvement.

As a result, the IT risk management process takes place which is expressed in the following:

- Decision-making, planning, and prioritization are improved;
- Capital and resources can be allocated more efficiently;
- Anticipating what might go wrong, minimizing the amount of efforts, or in the worst case, preventing a disaster or serious financial loss can be expected;

The likelihood that the business plan will be delivered on time, significantly increases.
References


