Bîlcan, Florentina Raluca; Ghibanu, Ionuț Adrian; Bratu, Ion Ionuț et al.

Article

The relationship between internal control and security risk management

Provided in Cooperation with:
Dimitrie Cantemir Christian University, Bucharest

Reference: Bîlcan, Florentina Raluca/Ghibanu, Ionuț Adrian et. al. (2019). The relationship between internal control and security risk management. In: Academic journal of economic studies 5 (4), S. 139 - 144.

Academic Journal of Economic Studies
Vol. 5, No. 4, December 2019, pp. 139–144
ISSN 2393-4913, ISSN On-line 2457-5836

The Relationship between Internal Control and Security Risk Management

Florentina Raluca Bîlcan[1], Ionuț Adrian Ghibanu [2], Ion Ionuț Bratu [3], George Adrian Bîlcan[4]

[1,2,3,4] Valahia University, [1]E-mail: bilcan.florentina.raluca@gmail.com, [2]E-mail: ghibanu.ionut.adrian@gmail.com,
[3]E-mail: bratu.ion.ionut@gmail.com, [4]E-mail: bilcan.george.adrian@gmail.com

Abstract

Understanding the control environment, the characteristics of the information system as a whole is an important and decisive step towards establishing the degree of credibility of the system itself and the information it provides. This article investigates this potential link between internal control and security risk management. The results show Internet network vulnerabilities can lead to surprise attacks network users leading to unauthorized access to the private network with theconsequences. Contrariwise, an advanced security environment can implement too strict security measures, generating improper network operation.

Keywords

Internal control, probability, security risk management, procedures

JEL Codes: D80, D81

Received: 01 November 2019 **Revised: 22 November 2019** **Accepted: 10 December 2019**

1. Introduction and literature review

Any entity is subject to risks: risks related to the own functioning of the organization and risks specific to each activity. In order to avoid unacceptable risks, the organization creates its own security and control measures, tolerating acceptable risks (Andriole, 2010; He *et al.,* 2012).

The importance of assessing the risks of an entity is marked both by the negative impact that can be avoided by developing a protection policy and by the probability that can be avoided by developing a preventive policy (Azizah and Islam, 2014). Within a general framework, any organization faces the following categories of risks: rich ones related to the design and functioning of the systems (risks related to the complexity of the methods; risks associated with the information system; risks related to the attitude of the managers); risks related to the economic situation of the entity; risks related to the general organization of the entity (Steinthórsdóttir, 2004).

Knowing the risk factors regarding the security of the information will help the manager to focus his attention on the essential points, thus avoiding to omit the fundamental aspects or to lose himself in unnecessary details (Core, 2015). Essentially, the risk of information security needs to be evaluated very well, because applying too detailed procedures can have negative effects. This stage of identifying information security risks will allow the entity to create an action plan taking into account not only the threats of the system itself but also what has already been implemented to deal with them (Elbannan, 2009).

The main objective of the internal control is to design and implement control procedures to enable it to reduce the risk of information security to an acceptable level (Andress, 2003). This evaluation, recognized by the specialized literature and the legislation in force as a mandatory step in an internal audit mission, is not carried out using a unique and rigorous method.

The importance of internal control has been recognized in the literature for more than half a century (Abbott *et al.,* 2000; Bob, 2009; Mikalef and Pateli, 2017), and the factors that contribute to increasing the recognition of importance of internal control are:

- the purpose and size of the business entities have become so complex that the management must rely on numerous reports and analyzes for an efficient control of the transactions;
- verification and recapitulation in a good internal control system allows protection against human weaknesses and reduces the possibility of errors;
- it is impracticable for specialists not to rely on the internal control system of the organization.

Also, some authors define Internal control as being the totality of control systems of any kind, implemented by management in order to conduct business in an orderly and effective manner, to ensure compliance with management policies, to protect assets and to guarantee, as far as possible, the accuracy and the complete stage of the recorded information (Andriole, 2010; Cannon *et al.*, 2008; Lin *et al.*, 2017).

The risk of information security control is the risk associated with the deficiencies of the internal control system, which will not be able to detect possible errors in the information systems (Todorovic, 2013). Generally, after obtaining the understanding of the internal control systems, a preliminary assessment of the control risk is made at the assertion level. Then, after conducting the control tests, a reassessment of the security control risk of the information will be carried out so that, finally, before the conclusion based on the substantive procedures and other evidence it can be assessed if the evaluation is confirmed (Elbannan, 2009).

A widely publicized and used technique is the so-called "salam fraud", which consists of introducing lines of code in the program that calculates and lowers bank interest, in order to "round down" these amounts of customers, and their progressive accumulation is transferred to the offender's account (Andress, 2003). It can also be applicable in the calculation of the wage rights of the employees of a company. The available techniques are very diversified: "computer trojan horse" is an unauthorized program code implanted in the authorized program, which performs activities unknown to the user (Stepchenko and Voronova, 2015). When the program is executed, the destructive secret instructions, very difficult to detect "come to light" causing bigger or smaller problems (Bob, 2009).

In this sense, fraud detection controls aim at: segregation of functions, rotation of functions, encryption of data and programs or control of sensitive data (Mikalef and Pateli, 2017). The question still arises whether this activity of internal control of management information systems is necessary? This chapter aims to capture the relationship between internal control and security risk management in the contemporary economy. Thus, the control of the applications in a computer system aims at both an administrative control that promotes the efficiency of the operation, as well as a control of the reliability of the application.

2. The relationship between internal control and security risk management

Knowledge of the internal control system allows for an effective planning and development of a proactive information security strategy, as this will have implications in the assessment of the control risk and the procedures that will be used in order to reduce the security risk to a minimum acceptable level (Yang *et al.*, 2014). As a basic principle, managing the security risk of information involves testing the internal control system, a test that will allow it to formulate an assessment as to the extent to which the respective systems work according to the information needs of the entity (Andriole, 2010).

A well-known fact is that a strategy for controlling the security of the information system requires (Awais and Hussain, 2015) the following steps to be taken:

- asset analysis - involves an identification and evaluation of the resources of the IT system that are to be protected: operating system, applications, network infrastructure, information processed by the system;
- analysis of existing security policies and practices;
- analysis of possible system threats that may affect its weaknesses at any given time, causing impacts (these threats exist anyway, they cannot be controlled, but only monitored, detailed on manifestation procedures and techniques, and the conclusions will be the basis for assessing the vulnerabilities of their own system);
- financial impact analysis allows value estimation of the entity's losses as a result of exploiting system vulnerabilities by threats;
- determination of residual risk which should contain the signaling of the weak, neutral points of the system associated with the corresponding threats, their probability of taking place and all the recommendations that need to be applied if the risk does not fall to an acceptable level.

On the other hand, the internal control system at the level of an organization can be defined as the whole of the procedures and policies adopted by the management that assists in the fulfillment of the management objectives regarding the assurance of a systematic and efficient management of the activities, including the adherence to the management policies the prevention and detection of frauds and errors (Hoitash *et al.*, 2009).

Internal control of information security has a wide scope (Hiller and Russel, 2013) but aims to analyse:

- the control environment, which represents the general attitude and the actions taken by the management regarding the internal control system, with effects on the control procedures applied, the importance given to the

control within the organization (Cannon *et al*., 2008). A solid control environment cannot, by itself, ensure the effectiveness of the internal control system, which is why it is necessary to complete its own control procedures.

- the control procedures that the entity has established in order to prevent or detect and correct errors are represented by a series of internal policies and regulations, which aim to: verification of instrumentation of recordings both from a technical point of view and from the point of view of arithmetic accuracy; control of primary documents and their approval; control of computer applications and information system (He *et al.,* 2012). These operations are aimed at controlling the development of the existing computer system and controlling access to data and programs.

The control environment sets the tone of the organization, influencing the control consciousness at the personnel level. It is the basis of all the other components of internal control, ensuring discipline within the organization that must be respected and a structure of the entity, so that the internal control system can be effectively applied (Arukonda and Sinha, 2015).

The internal control must be efficient, not cause additional costs and allow the saving of material, financial and human resources. Indeed, there may be a situation to design a good system of internal control but this may be misunderstood and put into practice by those involved in that entity (wrongly trained personnel regarding the implementation of internal control) or formally treated (Todorovic, 2013).

All the information security policies and measures provide management with reasonable assurance that the objectives will be achieved, although a number of inherent limitations may appear (Kurosawa *et al*., 2017), such as:

- the cost of internal control should not exceed the expected benefits derived from it;
- internal controls tend to be directed toward routine transactions rather than unusual transactions;
- there is a risk of human error caused by negligence, unprofessional reasoning or misunderstanding of information security rules;
- evading internal controls through tacit agreements between a management member and an employee.

For a correct evaluation of the internal control regarding the security of the information a series of investigations must be carried out:

- description of data collection and processing procedures in the existing system, in order to determine for each significant area, which are the procedures used by the entity for collecting information, processing data, recording transactions, circulating and archiving documents (Hiller and Russel, 2013);
- the conformity tests, which have the purpose of obtaining confirmation that the description of the procedures from the previous stage was correctly understood and corresponds to the procedures applied in the respective entity (in other words, they allow to verify the existence of the procedure and not to ensure that it is properly applied);
- preliminary assessment of the control risk can be made a preliminary assessment of it, thus highlighting the strengths and weaknesses of the existing system, all competing in determining the area of control tests that will be carried out in the next phase (Arukonda and Sinha, 2015);
- the control tests are carried out to obtain the tests regarding the efficiency of the internal control system and the way of conducting the internal controls throughout the period (Davila, 2012).

Taking into account the objectives of internal control, through these tests, the compliance of the internal control existing within the entity with the written measures adopted by it is monitored to ensure the efficiency of the activities carried out and the consistency of applying this control (its permanence). The reported deviations can be caused by factors, such as changes of the key personnel, which implies from the specialists to carry out detailed research on these aspects, especially research regarding the changes of the personnel in the key functions of the internal control (Andriole, 2010).

The level of these procedures depends on the level of assurance of the control tests; when the control tests cannot be performed or do not provide sufficient evidence, the substantive procedures are executed (Rankin *et al*., 2012). Moreover, when the weaknesses are identified within the internal control system, its approach will be to apply the substantive procedures.

In particular, the general control is intended to supervise the information system as a whole, having an impact on all the computer applications that work in the computerized environment. Only the presence of this control does not guarantee the reliability of a computer application nor the completeness and accuracy of its outputs, as their credibility is dependent on the control of the applications.

The internal control system identifies four categories of control mechanisms (Yang *et al*., 2014) represented by:

- restrictive control which has the effect of reducing the probability of a deliberate attack;

- preventive control that protects known or alleged vulnerabilities and reduces the impact of a successful attack;
- detective control that detects initiated or ongoing attacks and alarms the appropriate system;
- corrective control that reduces the effect of an attack by monitoring the correctness and integrity of the data.

Preventive control aims at detecting problems before they occur and involves: hiring only qualified personnel, adequate training, control of access to sensitive information so that it is allowed only to authorized persons. As far as the detective control is concerned, it aims to discover and correct the errors that have arisen through a verification of the input / output data, the control of the communications of this information and the control of the total transactions processed (Todorovic, 2013).

It should be mentioned that the corrective control aims to minimize the impact of threats, to remedy the problems discovered by the detective control, to identify the causes of the problems, to correct the errors assigned to them, which implies procedures to resume execution (Lin *et al.*, 2017).

3. Results and discussions

In digital economy, the objectives of the control tests do not differ from those corresponding to a manual environment; however, some procedures may be nuanced, including the vision of control of the "computer tool": the general control of the information system and the control of computer applications, with specific control tests (Mikalef and Pateli, 2017).

The classic verification techniques are: narrative descriptions, questionnaires (internal control questionnaire), flowchart diagrams that can be used individually or in combination. Today, there is an accelerated pace of replacing them with modern computer-assisted techniques. Thus, data query tools may be appropriate when the internal control system does not provide obvious evidence to document the performance of internal controls. The general objective of internal control in a computerized environment does not differ structurally from the classical steps and procedures. Exceptions arise only from the need for the internal auditor to know the existing computer system, to understand the computer applications used in the automatic processing of data, and to the way in which it satisfies the user's requirements.

The image on the significance and complexity of the IT environment is defined by the characteristics such as:

- the organizational structure of the IT environment, which places particular emphasis on the need to separate incompatible functions addressed to the same person;
- the complexity and importance of the automatic processing of each application significant;
- data availability and vulnerability of data / information storage media.

In this context, the extent of the risks takes on another dimension (Davila, 2012), their nature being influenced by:

- the density of information is much higher than in classical, paper-based systems;
- transparency of documents regarding the conduct of operations: the absence of the input documents - the data can be entered into the system without the basis of supporting documents - is the example of the transactions in the online systems; lack of visible "traces" of transactions;
- the strong integration of the systems appears as a consequence of the improvement of the forms of communication and of the proliferation of the computer networks;
- the lack of traces of possible criminal attacks is another worrying element of the new working environment.

At the same time, security control ensures the protection of the organization from unauthorized access to the resources of the organization, both from its employees and from people outside it (Stepchenko and Voronova, 2015). The requirements of a security in the field of information technology are often rendered by the following terms:

- assurance: the fact that the system works as expected, meets the requirements of the users;
- identification/authentication: the process by which the computer recognizes the presence of a potential user of the system;
- access control: access to information resources can be restricted to different categories of users;
- accuracy: ensures the completeness and integrity of the information;
- securing the electronic transfer: by ensuring the confidentiality, integrity, authenticity of the transmitted message and its non-repudiation;
- continuity of services: ensures the availability of data and processes of system users.

Nevertheless, the security strategy of a system must enjoy implicitness, coherence and compliance with existing standards. What gives a solid foundation to a society is the adopted information security policy, and it can be defined as "a set of rules and practices that regulate how an organization uses, manages, protects and distributes its sensitive information" (Core, 2015).

A number of vulnerabilities, such as incorrect management of user rights by the network administrator, failure to log in users after a number of failed logins, incorrect password management, inefficiency of the user control mechanism, lack of a log to remember the last successful or failed logon, failure a system for controlling access to files depending on the level of authorization, leads to unauthorized access, improper to the network resources (Bob, 2009).

4. Conclusions

A particular interest appears today, when the technical evolution has seen an unprecedented increase, on computer fraud - known in the specialized literature and under the name of "computer crime" (Lin *et al.*, 2017). As the advances in the field of information technology were being recorded at a rapid pace, the methods, the means of committing the crimes with the help of the computer were noticed with a great magnitude.

These illicit attacks and poor exploitation of information systems can cause significant financial damage (Stepchenko and Voronova, 2015). Serious damages may also result from the disclosure of sensitive or strategic information regarding the development policies of new products, financial or client information. It is thus necessary to ensure the security of the information systems as well as the data stored on them.

In addition, choosing the right strategy for addressing the security of a system must start from the unanimously accepted truth that there is no valid universal security product. The practice has shown that there is no "single recipe" which, once implemented, will assure the beneficiary that the data will not be altered or stolen (Davila, 2012). Security control ensures the protection of the organization from unauthorized access to the resources of the organization, both from its employees and from people outside it. Therefore, it can be said that an information security policy defines the overall policy of the organization in the information field, as well as the responsibilities in the system.

Acknowledgement

This work is supported by project POCU 125040, entitled "Development of the tertiary university education to support the economic growth - PROGRESSIO", co-financed by the European Social Fund under the Human Capital Operational Program 2014-2020

References

Abbott, L. J., Park, Y., & Parker, S. (2000). The effects of audit committee activity and independence on corporate fraud. Managerial Finance Journal, 26(30), 55-67.
Andress, A. (2003). Surviving Security: How to Integrate People, Process, and Technology. Auerbach Publications, Boca Raton, FL, USA.
Andriole, S.J. (2010). Business impact of Web 2.0 Technologies. Communications of the ACM, 53(12), 67-79.
Arukonda, S., & Sinha, S. (2015). The innocent perpetrators: reflectors and reflection attacks. Advanced Computer Science, 4, 94–98.
Awais, A., & Hussain, S. (2015) Understanding Corporate Governance and Board of Directors: A Generic Analysis. Academic Research International Journal, 6(4), 20- 25.
Azizah, M., & Islam, N. (2014). Do risk management, internal control and corporate reputation positively impact on firm value? A panel data econometric analysis and policy implications. International Finance and Economics Journal, 1(2), 12-28.
Bob, T. (2009). Corporate Governance: Principles, policies, and practices. Oxford University Journal, 4(1), 115-117.
Cannon, D.M., Godwin, J.H., & Goldberg, St.R. (2008). Risk management and governance. Journal of Corporate Accounting & Finance, 20(1), 1-99.
Core, F (2015). Big data analytics: a managerial perspective, Springer.
Davila, A. (2012). New trends in performance measurement and management control. In Performance Measurement and Management Control: Global Issues, 25, 65-87.
Elbannan, M. A. (2009). Quality of internal control over financial reporting, corporate governance and credit ratings. International Journal of Disclosure and Governance, 6(2), 127- 149.
He, D., Chen, C., Chan, S., & Bu, J. (2012). Secure and efficient handover authentication based on bilinear pairing functions. IEEE Transactions on Wireless Communications, 11(1), 48–53
Hiller, J., & Russel, R. (2013). The challenge and imperative of private sector cybersecurity: An international comparison, Computer Law & Security Review, 29(3), 236–245.

Hoitash, U., Hoitash, R., & Bedard, J. C. (2009). Corporate governance and internal control over financial reporting: A comparison of regulatory regimes. The Accounting Review, 84(3), 839-867.

Kurosawa, K., Ohta, H., & Kakuta, K. (2017). How to make a linear network code (strongly) secure? Designs, Codes and Cryptography, 82(3), 559- 582.

Lin, Z., Lin, D., & Pei. D. (2017). Practical construction of ring LFSRs and ring FCSRs with low diffusion delay for hardware cryptographic applications. Cryptography and Communications, 9, 431-440.

Mikalef, P., & Pateli, A. (2017). Information technology-enabled dynamic capabilities and their indirect effect on competitive performance: Findings from PLS-SEM and fsQCA. Journal of Business Research, 70, 1-16.

Rankin, M., Stanton, P., McGowan, S., Ferlauto, K., & Tilling, M. (2012). Contemporary issues in accounting (1st ed.). Australia: John Wiley & Sons Australia, Ltd.

Steinthórsdóttir, L. (2004). Internal control–corporate governance, internal audit and strategic renewal. Monetary Bulletin, 6(1), 85-95.

Stepchenko, D., & Voronova, I. (2015). Assessment of Risk Function Using Analytical Network Process. Inzinerine Ekonomika-Engineering Economics, 26(3), 264-271

Todorovic, I. (2013). Impact of Corporate Governance on Performance of Companies. Montenegrin Journal of Economics, 9 (2), 47-53.

Yang, C. N., Wu, C. C., & Wang, D. S. (2014). A discussion on the relationship between probabilistic visual cryptography and random grid. Information Sciences, 278, 141–173