Information Security Audit and Main Findings in Czech and Slovak Companies

Petr Doucek, Martina Kuncova, Luděk Novák & Lea Nedomova

University of Economics, Faculty of Informatics and Statistics, Prague, Czech Republic, e-mail: doucek@vse.cz.

Abstract Ensuring the security of information systems of companies is one of the important functions of the Corporate Informatics Department. One effective tool for building secured information systems is to audit their security. This article analyzes the results of 66 security audits in companies in the Czech Republic and the Slovak Republic during the years 2015-2018. The structure of the audit findings and their groups corresponds to the structure of ISO/IEC 27001: 20013. Using the data, we have formulated two hypotheses. The first hypothesis was about the dependence of the audit results on the size of the company; the second hypothesis examined the dependence of the audit results on the year of its performance. We used Pearson's chi-square independence test to verify these hypotheses. We have grouped the detailed audit results to provide clear proof. Based on the achieved results, we can say that the analyzed audit results showed the dependence of the audit results on the size of the company as well as on the year the audit was performed. The discussion then explains the reasons for the identified dependencies.

Keywords: information security, information security management system, security audit, ISO/IEC 27001:2013.

University of Maribor Press

DOI https://doi.org/10.18690/978-961-286-388-3.10
ISBN 978-961-286-388-3

1 Introduction

The implementation and use of information and communication technologies in everyday life come with certain risks. In addition to common risks, such as the failure of physical equipment of the terminal, security risks are becoming increasingly important. Security is one of the basic features that both users and operators request from information systems. It is because they request guaranteed confidentiality, credibility, availability, and integrity of the data in these systems (ISO 27001:2013; Novák & Doucek, 2017). In the case of more complicated systems that work with certain values, users and operators also request clear provability of operations performed by any entity within the system as well as the traceability of the author of such operation (Bilbao & Bilbao, 2013). Companies and government organizations are increasingly compelled, if not required by law, to ensure that their information systems will comply with various standards. Such organizations operate business or mission-critical systems where a lack of or lapse in security protections translates to serious confidentiality, integrity, and availability risks that, if exploited, could result in information disclosure, loss of money, or, at worst, loss of life (Hale & Gamle, 2019). These standards may be the federal standards NIST SP-800-53 for the USA and ISO 27000 family standards that are more common in Europe. Generally, most companies in Europe consider the ISO/IEC 27001 standard an acceptable information security standard. The ISO/IEC 27001 standard is the basic security audit standard for the public administration and for private companies in the Czech Republic and the Slovak Republic. In this case, it is the 2013 version. This standard regulates information security in several areas that are shown in Figure 1.

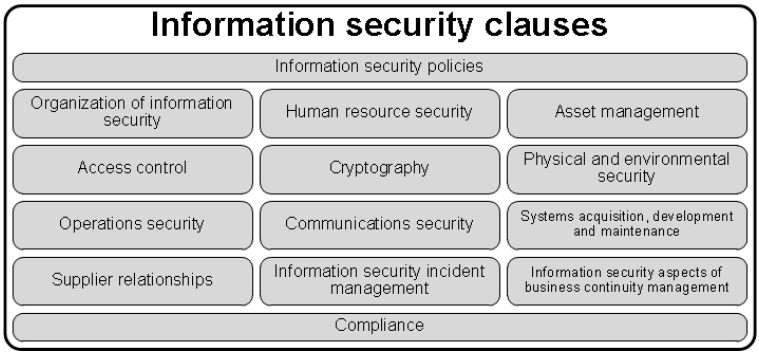

Figure 1: Information security areas according to ISO/IEC 27001:2013
source:(ISO 27001:2013)

Just like other management system standards, this Information Security Management System standard (ISMS) provides tools for a potential continuous improvement of the information security management system through the application of the managerial concept PDCA. This concept uses the ISMS audit tools mainly to develop the management system as well as to adapt it to changes in the environment. (Veber, Nedomova & Doucek, 2016; Herath & Herath, 2014).

The aim of the article is to point out the main shortcomings that have been identified during information security audits performed according to ISO/IEC 27001: 2013 in companies in the Czech Republic and the Slovak Republic. Another aim of the article is to present answers to two hypotheses formulated below.

2 Methodology

In this article, we used data from audits performed in companies in the Czech Republic and the Slovak Republic. These data were collected throughout the years 2015-2018 and concern 66 different audits carried out in 24 organizations (9 small organizations having up to 50 employees; 7 medium-sized organizations having between 50 and 250 employees and 8 large organizations with over 250 employees). These 66 audits can be divided by type as follows: 12 initial certification audits, 37 supervision audits, 10 re-certification audits, and 7 other audits. For all audits, the ISO/IEC 27001: 2013 criterion standard was used as the primary audit criterion. These audits resulted in a total of 631 findings (2015–137, 2016–125, 2017–234 and 2018–135). Out of these, 18 were categorized as non-conformities, 297 as observations, and 316 as opportunities for improvement. The identified non-conformities were divided according to individual areas of the ISO/IEC 27001: 2013 standard. The numerically marked audit categories correspond to the sections of this standard as following:

- Category "4" – Context of the Organization – Understanding of .the organization, its needs and expectation of interested parties and scope of the information management system.
- Category "5" – Leadership - Leadership and commitment, security policy, organizational roles, responsibilities and planning to achieve them.
- Category "6" – Planning - Action to address risks and opportunities, information security objectives and planning to achieve them.

- Category "7" – Support – Resources, competencies, awareness, communication and documented information.
- Category "8" – Operation - Operational planning and control, information security risk assessment and treatment.
- Category "9" – Performance Evaluation - Monitoring, measurement, analysis and evaluation, internal audit, management review.
- Category "10" – Improvement - Nonconformity and corrective action, continual improvement. (ISO 27001:2013)

The next categories marked with an A before the number correspond to the sections of the annex to this standard:

- Category "A05" – Information Security Policies - To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
- Category "A06" – Organization of information security - To establish a management framework to initiate the implementation and operation of information security within the organization and to ensure the security of teleworking and use of mobile devices.
- Category "A07" – Human Resource Security – To assure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered
- Category "A08" – Asset Management - Responsibility for Assets, Information Classification, Media Handling.
- Category "A09" – Access Control - Business requirements on access control, User access management, User responsibilities, System and application access control.
- Category "A10" – Cryptography - To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
- Category "A11" – Physical and Environmental Security - Secure areas, Equipment.
- Category "A12" – Operations Security - Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring,

Control of operational software, Technical vulnerability management, Information system audit and consideration.

- Category "A13" – Communication Security – Network security management and information transfer.
- Category "A14" – System acquisition, development, and maintenance – Security requirements of information systems, security in development and support process and data testing.
- Category "A15" – Supplier relationships – Information security in supplier relationship and supplier service delivery management.
- Category "A16" – Information Security Incident Management - To ensure a consistent and effective approach to the management for information security incidents, including communication n security events and weaknesses.
- Category "A17" – Information security aspects of business continuity management – Information security continuity shall be embedded in the organization´s business continuity management system.
- Category "A18" – Compliance - Compliance with legal and contractual requirements, Information security review. (ISO 27001:2013)

In total, there are 21 categories (sections of the standard and its Annex A).

The standard statistical functions of MS Excel were used to evaluate the obtained data. To test the hypotheses, we used Pearson's chi-square independence test (McHugh, 2013) at the 5% level of significance.

We worked with the data sample of 316 observations on three levels:

- The first adjustment (Data 1) was to exclude the above-mentioned categories with a low number of findings. Thanks to this adjustment, only 8% (by company) and 10% (by year) of observations are less than five. Therefore, the Chi-square independence test can be used. This change gave us 12 categories of analysed audit findings.
- The second adjustment (Data 2) consisted in merging the categories. Instead of the original 21 categories, we ended up with 12 categories; we merged the categories "4," "5," "6," "7," and "8,", the categories "9" and "10," the

categories "A05," "A06," and "A07," the categories "A10" and "A11" and the categories "A13" and "A14." Thanks to these adjustments, all observations are greater than five in case of classification of data by company size (see Table 3), and only two values (2%) are less than 5 in case of classification of data by year (see Table 4).

The third adjustment (Data 3) consisted in radically merging all categories into two groups, i.e., the categories "4,"……., "10" into one group, and the categories "A05,"…….., "A18" into another group.

2.1 Formulation of hypotheses

For the purposes of this article, we have formulated two hypotheses. The first one is about the dependence of security audit results on the size of the company where the audit was performed.

- *Hypothesis: H0: The results of audit findings do not depend on the size of the company.*

The second hypothesis assumes that immediately after the ISO/IEC 27001:2013 criterion standard was issued, i.e., in 2014, the audit results will be worse than in the following years, because the changes brought by the new version of the ISO/IEC 27001 standard have already been implemented into ISMS.

- *Hypothesis: H0: The results of audit findings do not depend on the year of observation.*

3 Results

As mentioned in the methodological section, the presented data sample came from security audits performed during the years 2014–2018 in companies in the Czech Republic and the Slovak Republic.

3.1 Audit results

Based on security audits (performed according to ISO/IEC 27001: 2013 and its Annex A - areas marked with letter A), we identified areas where there were minimum findings or non-conformities and areas that showed a high number of findings or non-conformities.

Problem-free audit categories

- Category "5" – Leadership, Category "8" – Operation, Category "10" – Improvement, Category "A05" – Information Security Policies, Category "A06" – Organization of information security, Category "A10" – Cryptography.

Problematic audit categories

- Category "6" – Planning, Category "9" – Performance Evaluation, Category "A8" – Asset Management, Category "A9" – Access Control, Category "A11" – Physical and Environmental Security, Category "A12" – Operations Security, Category "A16" – Information Security Incident Management, Category "A18" – Compliance.

These findings are following conclusions presented in (Longras et al., 2018) that they have shown for the conditions of Portugal.

3.2 Hypothesis 1 – Relationship between company size and audit conclusions

Verification of Hypothesis 1 – we performed Chi-square tests to determine whether the audit findings are dependent on the size of the audited company.

- *Hypothesis: H0: The results of audit findings do not depend on the size of the company.*

We structured the audit findings based on the data categories (Nykanen & Karkkainen, 2014) mentioned in the section Methodology.

The application of Chi-square tests of independence on data sorted by company type brought different results, depending on how data were adjusted. In the case of the first adjustment (exclusion of categories) and the third adjustment (two categories), the Chi-square test at the 5% level of significance recommends rejecting Hypothesis H0 about independence on the size of the company. However, in the case of partly merged categories, the p-value is 0.14 and therefore, Hypothesis H0 should not be rejected (see Table 1). This result may be due to the interdependence of some categories, and may be resolved by merging categories or by using other tests (Lipsitz et al., 2015).

Table 1: Results of Chi-square independence tests by company size

Firm Size / Type of Audit	Data 1	Data 2	Data 3
No of categories	15	12	2
Chi-square test statistics	48.81	29.17	6.39
Chi-square critical value	41.33	33.92	5.99
degrees of freedom	28	22	2
p-value	0.0087	0.1401	0.0408

source: own

Based on these results, we focused on correlations, i.e., the linear dependence of the number of observations by company size. The calculated correlation coefficients (Table 2) show a high linear dependence between the results of small and medium-sized companies.

Table 2: Correlation coefficients of the number of findings by company size

Firm Size/Type of Audit	2 Medium		3 Large	
Data	Data 1	Data 2	Data 1	Data 2
1 Small	0.8616	0.9446	0.3334	0.6715
2 Medium			0.3876	0.5832

source: own

Therefore, we combined the audit results for small and medium-sized companies together and performed the dependence analysis again.

Table 2: Correlation coefficients of the number of findings by company size

Firm Size S+M, L / Type of Audit	Data 1	Data 2	Data 3
No of categories	15	12	2
Chi-square test statistics	41.05	26.51	6.30
Chi-square critical value	23.68	19.68	3.84
Degrees of freedom	14	11	1
p-value	0.0002	0.0054	0.0121

source: own

This time, the results are the same in all data groups (Table 2), all p-values are lower than 5%, i.e., **Hypothesis H0 is rejected and there is a difference in audit findings between the group of small and medium-sized companies and large companies.**

3.3 Hypothesis 2 – Relationship of the year of the audit and its conclusions

Verification of Hypothesis 2 - we performed Chi-square tests to determine whether the audit findings are dependent on the year of observation.

- *Hypothesis: H0: The results of audit findings do not depend on the year of observation.*

The analysis of independence on the year of observation did not show the difference in results as in the case of previous tests. For all three data groups, the p-value is less than 5%, i.e., the Chi-square independence test recommends to rejecting Hypothesis H0 about independence on the year of observation. We can thus say that the findings vary from year to year.

Table 4: Results of Chi-square independence tests by year

Year/Type of Audit	Data 1	Data 2	Data 3
No of categories	15	12	2
Chi-square test statistics	64.08	52.65	8.21
Chi-square critical value	58.12	47.40	7.81
Degrees of freedom	42	33	3
p-value	0.0157	0.0163	0.0418

source: own

Table 5: Correlation coefficients of the number of findings by the year of observation

Year/Type of Audit	2016		2017		2018	
Data	Data 1	Data 2	Data 1	Data 2	Data 1	Data 2
2015	0.2452	0.7039	-0.0905	0.1997	0.3312	0.5220
2016			0.4578	0.5121	0.4578	0.7075
2017					0.7021	0.6942

source: own

The correlation coefficients (Table 5) show that the year 2015 differs the most in terms of linear dependence. Taking into account the recommendation of Sharpe (2015) concerning data partitioning into smaller groups to see whether there are differences between all years or just between certain years, this fact is also supported by Chi-square test results for summary data (Data 3) and a couple of years (Table 6), where the p-values clearly show the rejection of Hypothesis H0 about independence on the year of observation just for the year 2015 compared to the years 2017 and 2018.

Table 6: Resulting p-value when using Chi-square tests to compare a couple of years (for Data 3)

Chi-square tests 2x2 (year), p-value	2016	2017	2018
2015	0.0510	0.0073	0.0403
2016		0.7023	0.9553
2017			0.7437

source: own

Hypothesis H0 was rejected. There is a difference in audit findings between individual years. In particular, the results from audits performed in 2015 are different from those found in later years.

4. Conclusions and Discussion

The article presents the results of information security audits in different companies in the Czech Republic and the Slovak Republic during the years 2015–2018 from two different aspects Hoy & Foley (2015). The first aspect is the size of the company and the audit findings. In this case, we were able to prove the dependence of results from information security audits on the size of the company. The results were significantly identical for small and medium-sized companies but different for large companies. This conclusion can also be supported by the concept of organizational structures for corporate informatics management, including information security management. In small and medium-sized businesses, the role of CISO (Chief Information Security Officer) is usually shared role, so its possibilities are more limited. Information security services in these types of companies are outsourced, which can lead to an overall lower level of required corporate ISMS compliance with ISO / IEC 27001. (Kurowski, Litwing & Luckemeyer, 2015).

There is a perfect explanation for the anomalies in the findings from 2015 as compared to other years. It is the second version of the ISO/IEC 27001 standard that was issued in October 2013. Considering that companies had only one year to switch from the 2005 version and that there were some major changes in the standard (structure, more monitored areas and the depth of their details, etc.), it is understandable that audit findings during the first year were more elementary than in the following years. Moreover, the standard was not issued in the national language, which means that smaller companies had more problems to adapt to it. With the passage of time and experience gained by ISO/IEC 27001 standard users as well as by consultants, audit findings became less frequent.

Although the results are in line with our expectations and are consistent with the results of other research, our study has its limitations as the sample size was small - only 66 audits. If it were possible to obtain data from other companies or data from other countries, it would be possible to examine not only the differences between

countries but also, for example, the differences between the sectors in which the companies operate.

Acknowledgments

Paper was processed with contribution of the Czech Science Foundation project GAČR 17-02509S and with support from institutional-support fund for long-term conceptual development of science and research at the Faculty of Informatics and Statistics of the University of Economics, Prague (IP400040).

Literature

Bilbao, A., & Bilbao, E. (2013). Measuring Security. In *Proceedings of the 47TH International Carnahan Conference on Security Technology (ICCST)*. DOI: 10.1109/CCST.2013.6922054

Hale, M. L., & Gamble, R. F. (2019). Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards. *Requirements Engineering, 24(3), 365-402,* DOI: 10.1007/s00766-017-0287-5

Herath, H. S. B., & Herath, T. C. (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems*, *57*, 54-63, DOI: 10.1016/j.dss.2013.07.010

Hoy, Z., & Foley, A. (2015). A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits. *Total Quality Management & Business Excellence*, *26(5-6), 690-702,* DOI: 10.1080/14783363.2013.876181

ISO 27001:2013 *Information Technology-Security Techniques-Information Security Management Systems-Requirements*. International Organization for Standardization

Kurowski, S., Litwing, R., & Luckemeyer, G. (2015). A View on ISO/IEC 27001 Compliant Identity Lifecycles for IT Service Providers. In *Proceedings of the World Congress on Internet Security (WorldCIS)*. DOI: 10.1109/WorldCIS.2015.7359420

Livshitz, I. I., Yurkin, D. V., & Minyaev, A. A. (2016). Formation of the Instantaneous Information Security Audit Concept. In *Proceedings of the International Conference on Distributed Computer and Communication Networks (DCCN 2016)*. DOI: 10.1007/978-3-319-51917-3_28

Longras, A., Pereira, T., Carneiro, P., & Pinto, P. (2018). On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations. In *Proceedings of the 9TH International Conference on Intelligent Systems (IS)*. DOI: 10.1109/IS.2018.8710558

McHugh, M. L. (2013). The Chi-square test of independence. *Biochemia Medica, 23(2),143–9,* DOI: 10.11613/BM.2013.018

Novák, L., & Doucek, P. (2017). Regulation of Cyber Security in the Banking Sector. In *Proceedings of the IDIMT-2017 Digitalization in Management, Society and Economy* (pp. 49-54). Linz: Trauner Verlag Universität

Nykanen, R., & Karkkainen, T. (2014). Comparison of two Specifications to Fulfill Security Control Objectives. In *Proceedings of the 13th European Conference on Cyber Warfare and Security (ECCWS)*, DOI: 10.13140/RG.2.1.4331.

Sharpe, D. (2015). Your Chi-Square Test is Statistically Significant: Now What? Practical Assessment, *Research & Evaluation, 20(8),* Retrieved from https://pareonline.net/getvn.asp?v=20&n=8

Lipsitz, S. R., Fitzmaurice G. M., Sinha D., Hevelone N., Giovannucci E., & Hu, J. C. (2015). Testing for independence in J × K contingency tables with complex sample survey data. *Biometrics, 71(3), 832–840,* DOI:10.1111/biom.12297. Retrieved from http://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC4567525&blobtype=pdf

Veber, J., Nedomova, L., & Doucek, P. (2016). Corporate Digital Incident Investigation. *Quality Innovation Prosperity, 20(1), 57–70*, DOI: 10.12776/QIP.V20I1.656.