European Research Studies Journal
Volume XXVII, Issue S2, 2024

pp. 325-333

Information Security Management in Polish Manufacturing: Key Insights from a Survey

Submitted 08/09/24, 1st revision 20/10/24, 2nd revision 06/11/24, accepted 30/11/24

Maciej Szmit[1], Anna Szmit[2]

Abstract:

Purpose of the paper: *The research goal was exploratory. Its main objective was to collect data and describe the current state of selected aspects of establishing and maintaining ISMS in Polish manufacturing enterprises. In particular, the focus was on aspects such as the formalization level of ISMS, use of external support by specialized companies, and the budget allocated for information security questions.*
Design/Methodology/Approach: *The survey was conducted using the CATI (Computer-Assisted Telephone Interview) technique. The survey was conducted among 300 companies engaged in manufacturing activities in Poland included in the Dun & Bradstreet database. Selected companies were assigned to one of four employment ranges: Micro (0-9 employees), Small (10-49 employees), Medium (50-249 employees), and Large (over 249 employees).*
Findings: *The text presents the survey results on information security frameworks/methods used by companies, popularity of employees' certificates, use of external support, budgets allocated on information security management, and formal documentation of ISMS.*
Practical Implications: *The results constitute a knowledge base on the the examined aspects of ISMS in surveyed enterprises and can be a form of the basis for further, more in-depth analysis and research.*
Originality/Value: *To the authors' knowledge, this type of research has not been conducted in Poland yet. The results of this study were presented at 15th Scientific Conference. MASEP 2024 (Measurement and Assessment of Social and Economic Phenomena, 27-28.11.2024, Lodz).*

Keywords: *Information Security Management Systems, Information Security Management Methodologies, Cybersecurity.*

JEL codes: *M15, K24, L29.*

Paper type: *Research paper.*

[1]*Dr., PhD Meng: Department of Computer Science, Faculty of Management, University of Lodz, Poland, e-mail: maciej.szmit@uni.lodz.pl;*
[2]*Dr., PhD Meng: Institute of Management – Faculty of Organization and Management, Lodz University of Technology, Poland, e-mail: anna.szmit@p.lodz.pl;*

1. Introduction and Literature Review

Information security management belongs - from a management sciences perspective – to the field of GRC (Governance, Risk Management, and Compliance). The term *"governance"* referring to the oversight of organizations by their owners (shareholders), senior executives or stakeholders, and overall management approach based on a set of principles and norms or even decision-making methodology.

A comprehensive analysis of the use of the governance concept is provided e.g. in the article (Szulc, 2019). *"Compliance"* means conforming, especially with legal requirements, regulations (in the case of regulated markets), or commitments made by the organization.

GRC has been defined as *"the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty, and act with integrity"* (Mitchell, 2007). The concept itself was first used in the early 21st century, with the first use attributed to Michael Rasmussen, then an employee of Forrester Research Inc. Some authors distinguish between subsequent generations of GRC (from GRC1 to GRC4 - see, e.g., (Risk Optics, 2002)). At the heart of GRC is risk management, especially in the context of information security risk management (see, e.g., Piśniak, 2015).

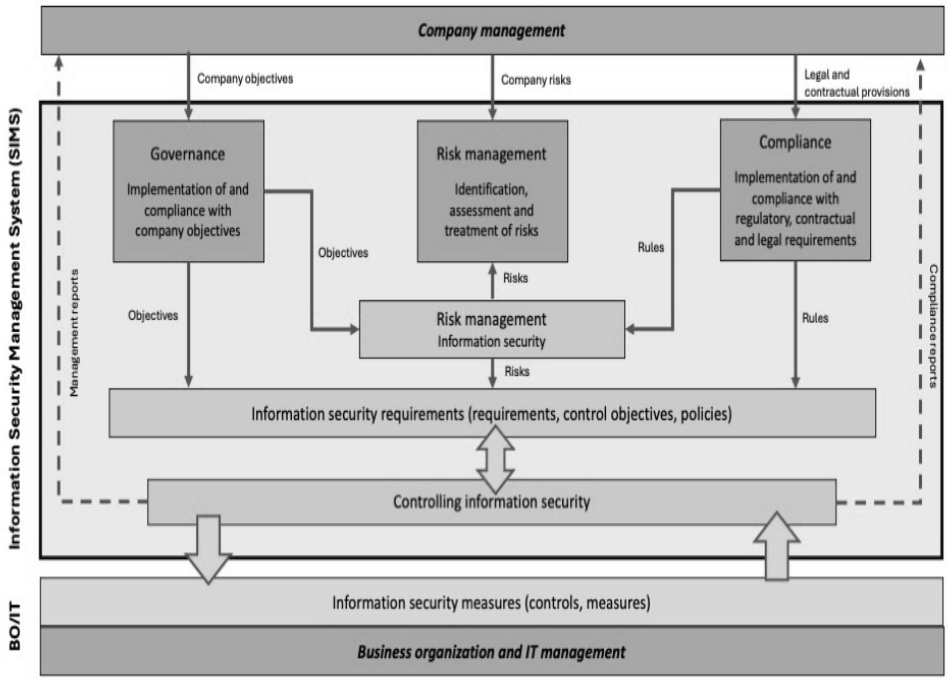
The concept of ISMS is related to the ISO/IEC 27k family of standards. ISMS had been defined as the part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (withdrawn version of ISO 27000 - (ISO/IEC 27000:2009-2.23)).

The management system itself is understood as a set of guidelines, policies, procedures, processes, and related resources (material, human, and immaterial) aimed at ensuring that the organization fulfils its tasks (see, e.g., Gillies, 2011; Humphreys 2007, pp. 11-44; ISO/IEC 27000:2016-2.46). The relationships between ISMS and GRC are schematically presented in Figure 1.

The concept of ISMS is nearly 30 years old and originates from the British standards BS 7799, first published in 1995, which gave rise to the ISO/IEC 27k family of standards, currently consisting of over sixty standards.

With the rapid development of modern techniques and ongoing socio-cultural changes, there is a need for both horizontal growth of standards and solutions supporting various aspects of security management, as well as vertical standardization of particular issues concerning narrow details of security management (for example, standards such as (ISO/IEC 27037; ISO/IEC 27041; ISO/IEC 27042; ISO/IEC 27043) dedicated to digital forensics and digital evidence).

Figure 1. *Incorporating the Information Security Management System (ISMS) into corporate control processes.*



Sources: *Olabode, 2019; SPARA Cybersecurity Group, 2023.*

Additionally, the number of issued certificates of compliance with the (ISO/IEC 27001) standard has been increasing in recent years. In 2022, according to the report by the International Organization for Standardization (International Organization for Standardization, 2022), 888 organizations in Poland and 70710 worldwide were certified.

Aside from ISO standards, there are numerous other methodologies and frameworks that various organizations promote for information security management. These include, for example, the NIST Cybersecurity Framework (NCF, also known as NIST CSF) developed by the National Institute of Standards and Technology (Cybersecurity Framework, 2023), COBIT developed by ISACA (Control Objectives for Information and related Technology, 2019), and EBIOS RM (Expression of Needs and Identification of Security Objectives Risk Manager) developed by the ANSSI (National Cybersecurity Agency of France) (Agence Nationale de la Sécurité des Systèmes d'Information, 2018).

Various organizations including commercial companies offer a range of tools (including computer-assisted risk management tools, referred to as Integrated Risk

Management Solutions, IRMS, in Gartner (2023) terminology, as well as training and certifications related to security. The popular roadmap (Jerimy, 2022) included 473 certifications divided into eight groups of security-related matters as of January 2023.

For maturity assessment of ISMS in organizations, models such as the C2M2 - Cybersecurity Capability Maturity Model (Office of Cybersecurity, Energy Security, and Emergency Response, 2022), currently available in version 2.1, Capability Maturity Model Integration CMMI (currently developed by ISACA CMMI Institute - see ISACA CMMI, 2022) in version 2.0, and extending them, COBIT Performance Management (CPM), and similar ones, are used.

As can be observed, simply understanding the multitude of available (and changing) approaches, models, standards, methodologies, platforms, tools, and certifications can be challenging, hence it may be an interesting to attempt to investigate the popularity of solutions used in various organizations, both commercial ones and public sector authorities.

In our previous research (Szmit, Szmit, and Lisiak-Felicka, 2019; Lisiak-Felicka and Szmit, 2016)), we mainly focused on studying the state of selected aspects of ISMS in local government administration, particularly in the context of legal requirements related to personal data protection imposed by GDPR (EU Official Journal L 119/1 of 04.05.2016). This article presents the results of a survey covering three hundred Polish manufacturing enterprises.

2. Research Methodology

The research goal was exploratory. Its main objective was to collect data and describe the current state of selected aspects of establishing and maintaining Information Security Management Systems in Polish manufacturing enterprises. In particular, the focus was on aspects such as the formalization level of ISMS (documentation, use of formal methodologies or frameworks, possession of information security-related certificates by individuals working under control of the company), use of external support by specialized companies, and the budget allocated for information security questions.

The research was conducted using a diagnostic survey method, using computer-assisted telephone interviewing (CATI). Respondents answered the following questions:

- Which formal cybersecurity/information security methods or frameworks do you use? (Multiple-choice question, options: none, NIST NCF, PCI DSS, ISO/IEC 27002, CMMC, SCF, other - specify).
- Who deals with information security/cybersecurity issues in your company… (single-choice question, options: only full-time employees, all

these issues are handled by external companies, both full-time employees and external companies)?

- What certificates do the information security specialists you employ or the people serving you in this regard have? (multiple-choice question) (options: ISO/IEC 27001 LA, CISA, CISM, CISSO, CEH, CompTIA Security+, GSEC, other - specify, they do not have any certificates, it was not considered when hiring employees and/or choosing an external company)?
- What percentage of your dedicated budget do you allocate to cybersecurity?
- Does your company have formal documentation of the Information Security Management System (and how many pages does it have)? (if yes, specify the number of pages)?

The survey was conducted among companies engaged in manufacturing activities in Poland included in the Dun & Bradstreet database. Selected companies were assigned to one of four employment ranges: Micro (0-9 employees), Small (10-49 employees), Medium (50-249 employees), and Large (over 249 employees).

3. Research Results and Discussion

The tables below show the responses to specific questions:

Table 1. *Answers to the question: "Which formal cybersecurity/information security methods or frameworks do you use?" grouped by company size.*

	Number of companies	None	NIST NCF	PCI DSS	ISO/IEC 27002	CMMC	SCF	Other
Micro	37	76%	8%	5%	14%	5%	5%	3%
Small	127	34%	12%	10%	49%	14%	8%	0%
Medium	88	8%	27%	26%	55%	30%	5%	0%
Large	48	17%	17%	27%	65%	21%	13%	4%
Total	300	29%	17%	17%	49%	19%	7%	1%

Source: *Own study.*

Table 2. *Answers to the question: „Who deals with information security/cybersecurity issues in your company …" grouped by company size.*

	Number of companies	only full-time employees	all these issues are handled by external companies	both full-time employees and external companies
Micro	37	89.19%	2.70%	8.11%
Small	127	62.99%	13.39%	23.62%
Medium	88	44.32%	21.59%	34.09%
Large	48	41.67%	20.83%	37.50%
Total	300	57.33%	15.67%	27.00%

Source: *Own study.*

Table 3. *Answers to the question: „What certificates do the information security specialists you employ or the people serving you in this regard have?" grouped by company size.*

ISO/IEC 27001 LA	101
CISA	55
CISM	60
CISSO	57
CEH	32
CompTIA Security+	47
GSEC	38
Other	0
None	54
This was not taken into account/unknown	67

Source: *Own study.*

Table 4. *Answers to the question: "What percentage of your dedicated budget do you allocate to cybersecurity?" grouped by company size.*

	Number of companies	there is no separate budget for cybersecurity issues	approximately less than 1% of annual revenue	1%-3% of our annual revenue	4%-5% of our annual revenue	6%-10% of our annual revenue	11%-20% of our annual revenue	above 20% of our annual revenue
Micro	37	33	2	0	1	1	0	0
Small	127	59	19	11	26	7	2	3
Medium	88	20	14	13	22	17	2	0
Large	48	8	4	13	16	3	4	0
Total	300	120	39	37	65	28	8	3

Source: *Own study.*

Table 5. *Answers to the question: "Does your company have formal documentation of the Information Security Management System (and how many pages does it have)?" grouped by company size.*

	Number of companies	No	5-104	105-204	205-304	305-404	405-504	705-804
Micro	37	25	12	0	0	0	0	0
Small	127	37	78	9		1	1	1
Medium	88	27	48	7	3	1	2	0
Large	48	20	23	3	2	0	0	0
Total	300	109	161	19	5	2	3	1

Source: *Own study.*

Analyzing the results presented above, several observations can be made. Firstly, the dominant position of ISO/OSI standards is evident both among the applied frameworks and among the certifications held by individuals working with ISMS (ISO/IEC 27001 Leading Auditor certificate) in respective companies. Compared to the number of ISO/IEC 27001-compliant ISMS certifications in Poland, this leads to the conclusion that the role of ISO/IEC 27k standards is much broader than just their use for building certified management systems.

Secondly, the relatively high utilization of CMMC (Cybersecurity Maturity Model Certification) and NCF indicates the significant popularity of standards developed by the National Institute of Standards and Technology. It can be expected that this results from connections with American companies (both in terms of capital ties and the use of IT consulting support) and the convenience of working provided by the rich set of NCF tools for information security management specialists compared to other frameworks.

Thirdly, although a relatively large percentage of companies do not use any methodologies or do not have formalized documentation of ISMS or have it in a rudimentary form (49 companies reported documentation up to 20 pages, while 109 companies - lack of documentation), almost two thirds apply some formalized approach and possess documentation of reasonable size.

Also, nearly two thirds of companies employ or utilize the services of individuals holding some well-known certifications related to information security. Of course, assessing documentation "by thickness" is a highly unreliable method; nevertheless, it provides some idea of the effort required for its preparation.

Additionally, the mere fact of hiring someone who once obtained an – even relatively highly regarded in the market certificate – does not necessarily reflect positively on the quality of information security management in the company. Nonetheless, all these pieces of information together suggest that in a significant portion of surveyed companies, the approach to the discussed issues is appropriate, and its importance is correctly recognized.

Also, the fact of having a dedicated budget for cybersecurity issues in 180 of the surveyed companies – regardless of their size – seems to confirm this assumption.

4. Conclusions, Proposals, Recommendations

The large number of incompatible information security frameworks and tools may, in practice, cause organizational interoperability difficulties between organizations building their Information Security Management Systems based on different methodologies.

Although providing detailed recommendations for enterprises may be hard at the current stage of development of various approaches, it is advisable to ensure that the ISMS is built in line with best practices recommended by the ISO/IEC 27002 standard.

Additionally, employees responsible for its implementation should possess not only technical expertise but also management competences (the measure of which can be appropriate certifications). It is also essential to recognize that maintaining cybersecurity often involves significant costs, which should be appropriately accounted for in the company's budget.

References:

Center for Internet Security Risk Assessment Method. 2021. Center for Internet Security. https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method.

Control Objectives for Information and related Technology. 2019. ISACA, pobrano z: https://www.isaca.org/resources/cobit.

Cybersecurity Capability Maturity Model (C2M2), version 2.1. 2022. Office of Cybersecurity, Energy Security, and Emergency Response. https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf.

Cybersecurity Framework. 2023. National Institute of Standard and Technology. https://www.nist.gov/cyberframework.

Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager 2019. Agence Nationale de la Sécurité des Systèmes d'Information, https://cyber.gouv.fr/publications/ebios-risk-manager-method.

Gartner Glossary. 2023. Gartner. https://www.gartner.com/en/information-technology/glossary.

Gillies A. 2011. Improving the quality of information security management systems with ISO27000. TQM Journal, 23(4), pp. 367-376.

Governance, Risk management, and Compliance. 2023. SPARA Cybersecurity Group, https://spara.ir/assets/en_css/files/GRC.pdf.

Humphreys, E. 2007. Implementing the ISO/IEC 27001 Information Security Management System Standard, Artech House, Norwood.

IRM, ERM, and GRC: Is There a Difference?, Risk Optics .2022. https://reciprocity.com/irm-erm-and-grc-is-there-a-difference.

ISACA CMMI Institute. 2022. ISACA CMMI, https://cmmiinstitute.com,

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems requirements.

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls.

ISO/IEC 27037:2012 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence.

ISO/IEC 27041:2015 Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method.

ISO/IEC 27042:2015 Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence.

ISO/IEC 27043:2015 Information technology -- Security techniques -- Incident investigation principles and processes.

Jerimy, P. 2022. Security Certification Roadmap. https://pauljerimy.com/security-certification-roadmap.

Lisiak-Felicka, D., Szmit, M. 2016. Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, European Association for Security, Kraków.

Mitchell, S. GRC360: A framework to help organisations drive principled performance. International Journal of Disclosure and Governance, 4, pp. 279-296. DOI: https://doi.org/10.1057/palgrave.jdg.2050066.

Olabode, G.A. 2019. Impact of Cyber Security Implementation in an Economy Driven by Cyber Physical System (CPS). In: M. Olalere (red.), O. Osho, O.M. (red.), Olaniyi, S.M. (red.), Abdulhamid, S.O. (red.), Ganiyu (red.), H. Chiroma (red.), Proceedings of the Cyber Secure Nigeria 2019 Conference, Cyber Security Experts Association of Nigeria, Abuja, pp.1-5.

Piśniak, M. 2015. Ryzyko w teorii podejmowania decyzji, Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie, 19, pp. 116-126.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Dz. U. UE L 119/1 z 04.05.2016.

Szmit, M., Szmit, A., Lisiak-Felicka, D. 2019: The Assessment of GDPR Readiness for Local Government Administration in Poland. In: Borzemski, L. (ed.), Wilimowska, Z. (ed.), Świątek, J. (ed.): Proceedings of 39th International Conference on Information Systems Architecture and Technology – ISAT 2018, Advances in Intelligent Systems and Computing 854(3), pp. 417-426. Springer, Cham.

Szulc, M. 2019. Pojęcie governance w piśmiennictwie na temat nauk o zarządzaniu, Studia i prace Kolegium Zarządzania i Finansów Zeszyt Naukowy SGH, 176, pp. 85-110.

The ISO Survey. 2022. International Organization for Standardization. https://www.iso.org/the-iso-survey.html.