European Research Studies Journal
Volume XXIX, Issue 1, 2026

pp. 478-489

The Effectiveness of Security Management Systems in Public Organizations: A Cybersecurity Perspective

Submitted 13/12/25, 1st revision 29/12/25, 2nd revision 20/01/26, accepted 25/02/26

Marta Chodyka[1], Sylwia Wojciechowska-Filipek[2], Zbigniew Ciekanowski[3], Aneta Chrząszcz[4], Sławomir Żurawski[5]

Abstract:

Purpose: *This article aims to assess the effectiveness of security management systems in public organisations using statistical data and institutional reports, with particular emphasis on the relationship between the maturity of these systems and the level of threats, including cybersecurity threats and incidents. The article aims to fill a research gap in the empirical analysis of the actual functioning of security systems in the public sector.*
Design/Methodology/Approach: *The research was conducted using triangulation of research methods. Statistical data from institutional reports, document analysis (control and audit reports), comparative methods and analysis of scientific literature on security management, risk management and organisational resilience were used. The main research problem was formulated as follows: to what extent does the maturity of security management systems affect the level of threats and the effectiveness of public organisations' responses? The research hypothesis was that public organisations with more mature security management systems have fewer security incidents, shorter response times, and greater organisational resilience than entities with fragmented or informal security systems.*
Findings: *The study indicates a clear relationship between the maturity of security management systems and the level of risk in public organisations. Entities with integrated security systems, regular risk analyses, functioning audit mechanisms, and a developed security culture are characterised by fewer incidents (including cybersecurity incidents) and a higher effectiveness in responding to threats.*
Practical implications: *The article contributes to research on security management in the public sector by empirically confirming the importance of system maturity for organisational resilience.*

[1]*John Paul II University in Biala Podlaska, Poland, ORCID: 0000-0002-8819-2451, e-mail: m.chodyka@dyd.akademiabialska.pl;*
[2]*University of Warsaw, Faculty of Management, Poland, ORCID: 0000-0002-1847-1957, e-mail: SWojciechowska@wz.uw.edu.pl*
[3]*John Paul II University in Biala Podlaska, Poland, ORCID: 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*
[4]*John Paul II University in Biala Podlaska, Poland, ORCID: 0000-0001-9749-274X, e-mail: a.chrzaszcz@dyd.akademiabialska.pl;*
[5]*Andrzej Frycz Modrzewski Krakow University, Poland, ORCID: 0000-0001-9527-3391 e-mail: slawomir.zurawski@onet.pl;*

Originality value: *The results also have a practical dimension and can serve as a basis for improving security management systems and data-driven decision-making in public organisations.*
Keywords: *Security management, public organisations, effectiveness of security systems, cybersecurity, risk management, organisational resilience*

JEL codes: *H83, H12, D81, M15.*

Paper Type: *Research paper.*

1. Introduction

Contemporary public organisations operate in an environment characterised by high levels of uncertainty, complexity, and a dynamically changing threat structure. In addition to traditional organisational and legal risks, cyber, information, and systemic threats are becoming increasingly important and can significantly disrupt the continuity of public service delivery. As a result, security management is no longer seen as a support function, but is becoming one of the key elements of strategic management in the public sector.

Institutional analyses and reports indicate that the effectiveness of security management systems in public organisations remains varied and often insufficient, given the scale and nature of contemporary threats. The results of audits conducted by the Supreme Audit Office reveal numerous irregularities in the identification of risks, the updating of procedures, and the use of audit results to improve security systems.

In turn, data published by CERT Polska confirms a systematic increase in cybersecurity incidents in public administration, highlighting the growing vulnerability of public institutions to information security threats. Similar conclusions are drawn in reports by international organisations, including the OECD, which emphasise the need to integrate security into risk management and management control processes in the public sector.

Despite the growing number of publications devoted to security management, there is still a lack of empirical research based on statistical data and institutional reports that would allow for an assessment of the actual effectiveness of existing security systems in public organisations.

Many studies are normative or descriptive in nature, focusing on postulates and theoretical models, while making limited use of quantitative data and control results as a basis for inference. This creates a research gap concerning the relationship between the maturity of security management systems and the level of threats and incidents in the practical functioning of public institutions.

This article aims to assess the effectiveness of security management systems in public organisations using statistical data and institutional reports, with particular emphasis on the relationship between the maturity of these systems and the scale and nature of the threats they face.

The article attempts to empirically verify the thesis that public organisations with integrated, systematically implemented security management mechanisms exhibit higher organisational resilience and lower vulnerability to threats.

2. Security Management Systems in Public Organisations – A Theoretical and Institutional Approach

The security of public organisations is currently one of the key management categories, determining the ability of state institutions to perform public tasks continuously and effectively. In an increasingly complex security environment, encompassing both traditional threats and new forms of risk – in particular cyber, information and organisational risks – security cannot be treated solely as a support function. Still, it must be an integral part of strategic management.

The literature on the subject emphasises that effective security management in the public sector requires a shift from a reactive to a systemic, proactive approach (Kieżun, 2012, pp. 214-216).

In theoretical terms, a security management system in a public organisation can be defined as an orderly set of standards, procedures, organisational structures and human resources aimed at identifying threats, assessing risks and taking preventive and corrective measures. Organisations that have implemented effective risk management processes are better prepared to deal with potential threats (Ciekanowski *et al.,* 2024, p. 143).

This understanding of security is consistent with the approach presented in the reports of the Supreme Audit Office, which treat security as an element of management control and a condition for ensuring the legality, effectiveness, and continuity of public sector entities (Supreme Audit Office, 2025). In this context, the security system is one of the pillars of institutional risk management.

The specific nature of public organisations means that security management systems operate within an extensive regulatory environment that, on the one hand, promotes standardisation of activities but, on the other hand, can lead to formalisation and reduced decision-making flexibility.

One of the main security problems in public administration is the gap between the formal existence of procedures and their actual application. This phenomenon is referred to in the literature as "apparent institutionalisation of security", leading to a reduction in real organisational resilience. (Grudniewski *et al.,* 2025, pp. 912-914).

An integrated security management system in a public organisation is presented in Figure 1.

Figure 1. *Integrated security management system in a public organisation*

Source: *Own study based on reports by the Supreme Audit Office, CERT Polska, the Government Security Centre and the OECD.*

An essential component of security management systems in public organisations is risk management, which, according to the guidelines of the Ministry of Finance, should be a continuous process involving the identification, analysis and monitoring of risks affecting the achievement of the entity's objectives (Ministry of Finance, 2023, pp. 12-16).

In many sectoral institutions, risk management is declaratory and does not translate into concrete managerial decisions, thereby weakening the effectiveness of the entire security system.

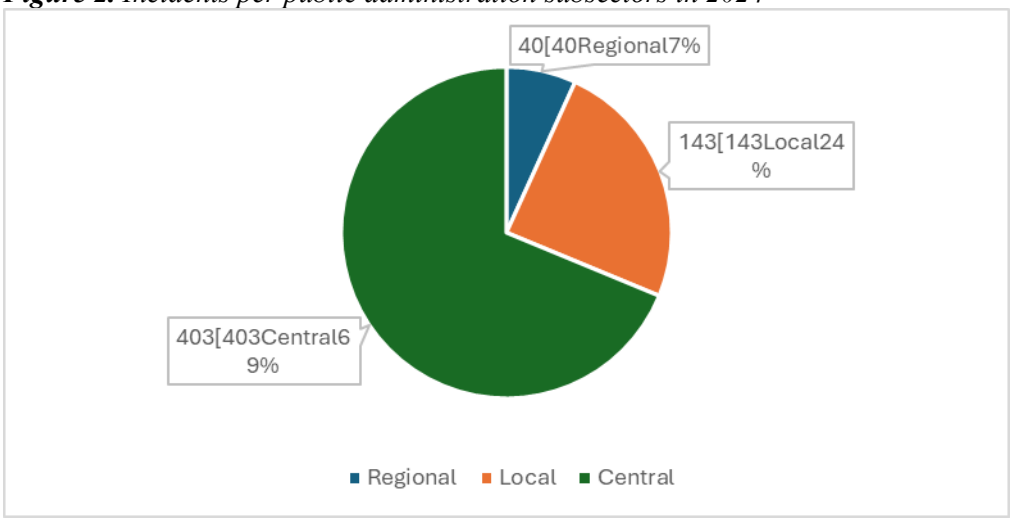
In recent years, the fields of information security and cybersecurity have become particularly important, posing significant challenges for public organisations. Data published by CERT Polska indicate a systematic increase in the number of cyber incidents in public administration, with a simultaneous low level of maturity of information security management systems in some entities (CERT Polska, 2025, pp. 89-91). pp. 89-91).

In 2024, CSIRT NASK handled 3,450 incidents in public entities. This is an increase of 58% compared to the previous year. The highest number of incidents was recorded in public administration – 1,911 cases.

This phenomenon is also supported by scientific research, which indicates a significant correlation between the competence of management staff and the effectiveness of the security mechanisms implemented (Białas, 2017, pp. 133-135).

From an international perspective, analyses conducted by the OECD and ENISA emphasise that effective security management systems in the public sector are characterised by a high degree of integration with planning processes and the use of empirical data in decision-making (OECD 2024, ENISA 2025). Security is viewed as a dynamic process that requires continuous improvement, audits and adaptation to the changing threat environment. Between January and December 2024, ENISA analysed 586 publicly reported cyber incidents targeting public administrations in the EU. The incidents are broken down by public administration subsector in 2024, as shown in Figure 2.

Figure 2. *Incidents per public administration subsectors in 2024*



Source: *ENISA Sectorial Threat Landscape - Public Administration, 2025, p. 9.*

The literature also increasingly emphasises the importance of security culture as a factor determining the effectiveness of security management systems. A lack of awareness of threats among public administration employees reduces the effectiveness of even the best-designed formal systems (Sienkiewicz-Małyjurek, 2016, p. 58). In this sense, organisational security should be seen not only as a set of procedures, but also as an element of organisational culture.

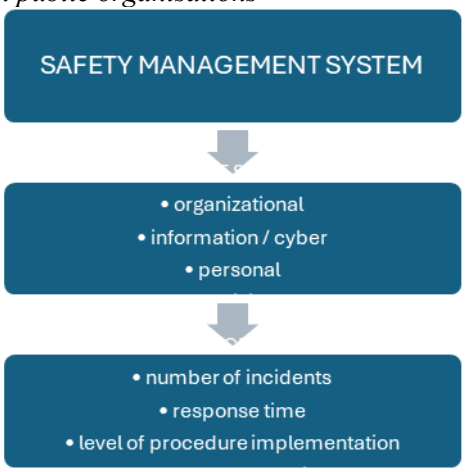
In summary, security management systems in public organisations are complex institutional structures whose effectiveness depends on the degree of integration with management processes, the quality of human resources and the use of reporting and statistical data. An analysis of the literature and national and international reports clearly indicates that a fragmented, formalistic approach to security reduces the

resilience of public organisations, which justifies an empirical assessment of the effectiveness of these systems in the remainder of this article.

3. Operationalisation of Security Management Effectiveness

The operationalisation of the effectiveness of security management in public organisations requires translating theoretical categories into measurable empirical variables that enable comparative analysis and evaluation of the functioning of security systems in practice. The literature on the subject emphasises that the effectiveness of security systems should be considered multidimensionally, taking into account both quantitative and qualitative effects, as well as organisational and human resource conditions (Ciekanowski, 2018). The operationalisation of the effectiveness of security management systems is presented in Figure 3.

Figure 3. *Operationalisation of the assessment of the effectiveness of security management systems in public organisations*



Source: *Own study based on an analysis of reports by NIK, CERT Polska, OECD and literature on the subject.*

It has been assumed that the effectiveness of a safety management system means a public organisation's ability to reduce the number and impact of threats through conscious and systematic management activities based on risk analysis, statistical data, and the results of inspections and audits. This approach is consistent with that presented by Z. Ciekanowski, who points out that the effectiveness of safety management is not a static feature, but the result of a continuous process of improving organisational structures and procedures (Ciekanowski *et al.,* 2018).

The fundamental element of operationalising effectiveness is the use of quantitative indicators based on statistical data from institutional reports. Key measures include the number of security incidents, their type structure and the dynamics of changes over time.

Data published by CERT Polska indicates that in 2019-2024, the public sector experienced a systematic increase in the number of cybersecurity incidents, with their scale varying by the maturity level of information security management systems. The incident rate per organisational unit allows for comparisons of the effectiveness of security systems across different categories of public organisations.

The quantitative indicators are supplemented by organisational measures relating to the degree of implementation of security management systems. These include, among others, the existence of a formal security policy, separate organisational structures responsible for security, and the regularity of risk analyses and internal audits.

As Sławomir Żurawski points out, the lack of consistency between formal regulations and their practical application is one of the main barriers to effective security management in public organisations (Żurawski *et al.,* 2025, p. 161).

Data from the Supreme Audit Office's audit reports and reports on the functioning of management control are also crucial for the operationalisation process. These sources enable the identification of recurring organisational irregularities, such as outdated procedures, insufficient management oversight, or a fragmented risk management approach. Indicators derived from audit results allow a qualitative assessment of the effectiveness of security systems, complementing statistical analysis.

An essential component of operationalising effectiveness is also personnel indicators relating to staff competence and preparation. The literature on the subject emphasises that the human factor is a key determinant of the functioning of security systems, and that ignoring it reduces organisational resilience (Ciekanowski *et al.,* 2023, p. 804). In this study, personnel indicators include, among others, the number of safety training courses, the share of trained employees among total employees, and the presence of mechanisms to raise awareness of risks.

The operationalisation of security management effectiveness was based on the triangulation of data sources, combining statistical data, institutional reports, and findings from the scientific literature. Research indicates that public organisations that systematically use empirical data in their decision-making processes achieve a higher level of security system effectiveness and better results in mitigating the effects of threats.

The adopted operationalisation methodology therefore not only enables the measurement of the effectiveness of security management systems but also the identification of the factors that determine their functioning. This allows us to move from a normative description to an empirical analysis, which forms the basis for further considerations in the third part of the article, devoted to the relationship

between the maturity of security systems and the level of threats in public organisations.

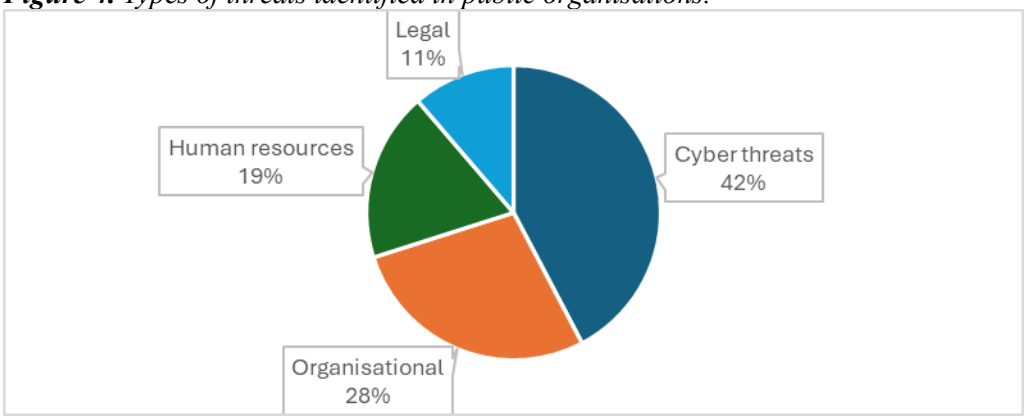
4. Analysis of the Relationship Between the Maturity of Security Systems and the Level of Threats in Public Organisations

The empirical analysis focused on identifying the relationship between the maturity level of security management systems and the scale and impact of threats in public organisations. To this end, security system effectiveness indicators were compiled using statistical data from reports by the Supreme Audit Office, CERT Polska, and on the functioning of management control in public finance sector entities. The use of a multi-year approach enabled the identification of trends and the assessment of the sustainability of the observed relationships.

The analyses indicate significant differences in threat levels depending on the degree of implementation and integration of security management systems. Public organisations characterised by high system maturity, understood as the existence of a coherent security policy, regular risk analyses, clearly assigned management responsibilities and functioning audit mechanisms, report a relatively lower number of security incidents per organisational unit.

This correlation confirms the thesis that the effectiveness of security systems results from their embedding in management processes, rather than from the mere fact of formal regulation of procedures. Figure 4 shows the types of threats identified in public organisations.

Figure 4. *Types of threats identified in public organisations.*



Source: *Own study based on reports by the Supreme Audit Office, data from CERT Polska and reports on the functioning of management control in public finance sector entities.*

An apparent correlation can be seen in the area of information security and cybersecurity. CERT Polska data indicate that in 2019–2024, the increase in the number of incidents mainly affected entities with a low level of organisational

maturity in information security management. At the same time, organisations that implemented integrated information risk management mechanisms were characterised by shorter response times to incidents and a smaller scale of their operational impact.

These results align with studies that measure the effectiveness of security systems not only by the number of incidents, but above all by the organisation's ability to absorb disruptions and quickly restore business continuity (Żurawski *et al.,* 2025, p. 580).

An analysis of NIK audit data reveals the critical role of organisational and human resource factors in shaping the effectiveness of security systems. Recurring causes of ineffectiveness include failure to update procedures, ambiguous assignment of responsibilities and insufficient staff training.

Entities that invest in training, competence development, and the building of a safety culture achieve higher effectiveness indicators, especially in the areas of prevention and response. These conclusions confirm Z. Ciekanowski's study (Ciekanowski *et al.,* 2025, p. 58), which identifies the human factor as a key determinant of organisational resilience in the public sector.

The use of audits and controls as tools to improve security systems also proved to be an essential factor in differentiating risk levels. Public organisations that systematically implement and monitor post-audit conclusions are less susceptible to recurring incidents and more consistent in their actions.

In this context, auditing serves as a feedback mechanism, enabling the organisation to learn and adapt its security system to changing conditions. This relationship is emphasised by Marta Chodyka, who points to auditing and control as key instruments for improving the effectiveness of security management in public administration (Chodyka *et al.,* 2025).

Extending the interpretation of the results to include the work of other authors places the empirical analysis in the broader context of public management and organisational resilience theory. Public organisations capable of responding effectively to threats are characterised by high levels of coordination, communication, and leadership in crises (Boin and Hart, 2010, pp. 361-363). A key factor in effectiveness is the ability of institutional systems to process information and adapt in conditions of uncertainty (Comfort, 2007, pp. 190-192).

In international literature, the security of public organisations is increasingly analysed through the prism of organisational resilience. Hollnagel points out that resilience is not about eliminating all threats, but about a system's ability to function despite disruptions (Hollnagel, 2014, 145-147). In this context, the empirically observed relationships between the maturity of security systems and shorter response

times and less severe incident effects support this concept. Similar conclusions are drawn by von Solms and van Niekerk, who emphasise the importance of organisational culture and staff competence for the effectiveness of information security systems (von Solms, van Niekerk, 2013, pp. 99-101).

From a security governance perspective, it is also essential to consider inter-institutional cooperation. Effective management in the public sector requires coordinating multiple entities and integrating decision-making across levels (Kooiman, 2003, pp. 114-116). The results of the empirical analysis indicate that public organisations that use reporting data to coordinate and support organisational learning achieve a higher level of security system effectiveness.

There is a clear and lasting relationship between the maturity of security management systems and the level of risk in public organisations. Organisations that treat security as a strategic element – supported by statistical data analysis, audits and competence development – achieve a higher level of organisational resilience and better results in mitigating the effects of risks. These findings provide empirical confirmation of the adopted operationalisation and serve as a direct basis for drawing conclusions and making practical recommendations.

5. Conclusions

The theoretical and empirical analysis confirms that the effectiveness of security management systems in public organisations remains a key factor in determining their resilience to contemporary organisational, informational, and systemic threats. The results of the research clearly indicate that security in the public sector cannot be treated as a set of separate procedures or reactive measures, but should be an integral part of an organisation's strategic and operational management.

An analysis of statistical data and institutional reports has revealed a significant correlation between the maturity level of security management systems and the scale and impact of threats occurring in public organisations.

Entities characterised by a high level of system maturity – understood as the existence of a coherent security policy, regular risk analyses, clearly defined management responsibilities and functioning audit and control mechanisms – report a relatively lower number of security incidents, shorter response times and a smaller scale of negative consequences of undesirable events.

Thus, the research hypothesis, which assumed a positive correlation between the maturity of security systems and the level of organisational resilience, has been confirmed. The field of information security and cybersecurity is critical to the effectiveness of security management systems. Empirical data indicate that public organisations that have implemented integrated information security risk management mechanisms and invested in staff competencies are able to mitigate the

effects of incidents more effectively, even as the number of incidents increases. This means that the effectiveness of security systems is not only measured by the reduction in the number of threats, but above all by the organisation's ability to respond quickly, adapt and restore continuity of operations.

An important conclusion from the research is also the confirmation of the key role of the human factor and safety culture in the functioning of safety management systems. Even the most sophisticated formal solutions do not bring the expected results in the absence of appropriate staff competencies, low risk awareness and limited management involvement.

The results of empirical analyses confirm that public organisations that systematically invest in training, competence development and organisational learning mechanisms achieve a higher level of security system effectiveness.

The research also demonstrated the importance of auditing and control as tools for improving security management systems. Public organisations that treat the results of controls not only as an element of reporting but also as a basis for modifying procedures and organisational structures are characterised by greater consistency of actions and less susceptibility to recurring incidents. In this context, auditing serves as a feedback mechanism, enabling the adaptation of security systems to a dynamically changing threat environment.

It should be noted that the effectiveness of security management systems in public organisations results from their integration with management processes, the quality of human resources, and the use of statistical data and institutional reports in decision-making. Organisations that treat security as a strategic element, based on risk analysis, auditing, and continuous improvement, achieve a higher level of organisational resilience and better results in mitigating the effects of threats.

The results of the research have both scientific and practical dimensions. They confirm the validity of a systemic and empirical approach to the analysis of security management in the public sector. In practical terms, they provide a basis for formulating recommendations on strengthening management's role in security, integrating risk management systems, and making wider use of statistical data and audit results in decision-making processes.

Further research should focus on an in-depth comparative analysis of individual categories of public organisations and on identifying good practices that can be transferred between public sector entities.

References:

Białas, A. 2017. Information and service security in modern institutions and companies. Wydawnictwo Naukowe PWN, Warsaw.

Boin, A., Hart, P. 2010. Organising for effective emergency management. Australian Journal of Public Administration, Vol. 69(4), pp. 357-371.

Comfort, L.K. 2007. Crisis management in hindsight. Public Administration Review, Vol. 67(S1), pp. 189-197.

Chodyka, M., Nowicka, J., Mazur, S., Ciekanowski, Z., Kacperska, E.M., Zdunek, M. 2025. The Role of Management Control in Ensuring Organisational Security. European Research Studies Journal, Volume XXVIII, Issue 3, 03-14.

Ciekanowski, Z., Majkowska, J., Załoga, W. 2018. The Impact of the Environment on the Functioning of Organisations. Modern Management System, 4/2018 vol. 13.

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Zdunek, M., Żurawski, S. 2024. Risk Management and Organisational Resistance to Threats. European Research Studies Journal, Volume XXVII, Issue 1, 142-153.

Ciekanowski, Z., Nowicka, J., Żurawski, S., Mikosik, P. 2023. Human Resources in Organisational Security Management. European Research Studies Journal, Volume XXVI, Issue 4, 802-812.

Ciekanowski, Z., Rejman, K., Żurawski, S., Kacprzak, M., Sirojc, Z. 2025. Personal Safety in the Management of Contemporary Organisations. European Research Studies Journal, Volume XXVIII, Issue 1, 57-66.

ENISA Sectorial Threat Landscape - Public Administration, 2025.

Framework on management of emerging critical risks (EN), OECD 2024.

Grudniewski, T.M., Żurawski, S., Nowicka, J., Ostrowska, M., Ciekanowski, M., Kacprzak, A. 2025. Managing the Leadership Crisis and Institutional Security in the Non-Governmental Sector in Poland. European Research Studies Journal, Volume XXVIII, Issue 2, pp. 907-919. https://doi.org/10.35808/ersj/4017.

Hollnagel, E. 2014. Safety-I and Safety-II. London: CRC Press.

Information on audit results. Ensuring information security and continuity of IT systems in local government units, NIK Warsaw. 2025.

Kooiman, J. 2003. Governing as Governance. London: Sage.

Kieżun, W. 2012. The pathology of transformation. Warsaw: Poltext.

Sienkiewicz-Małyjurek, K. 2016. Crisis management in public administration, 2nd edition. Warsaw: Difin.

Order of the Minister of Finance of 28 August 2023 on the preparation and monitoring of the implementation of the unit's activity plan, the report on its implementation and the submission of a statement on the state of management control by unit managers in government administration departments – budget, public finance and financial institutions.

von Solms, R., van Niekerk, J. 2013. From information security to cyber security. Computers & Security, Vol. 38, pp. 97-102.

Żurawski, S., Chodyka, M., Nowicka, J., Grudniewski, T.M., Dawidziuk, R., Gralak, K. 2025. The Impact of Cyberthreats on the Security of Important Sectors of the Economy on the Example of the Healthcare Sector. European Research Studies Journal, Volume XXVIII, Issue 2, 150-162.

Żurawski, S., Chrzaszcz, A., Ciekanowski, Z., Pauliuchuk, Y., Pietrzyk, S., Wyrzykowska, B. 2025. Effectiveness of Information Security Incident Management Systems: Identifying Practices, Challenges and Development Perspectives. European Research Studies Journal, Volume XXVIII, Issue 1, 575-588.