Journal scientific and applied research, vol. 29, 2025
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

CENTRALIZED AND DECENTRALIZED SECURITY MANAGEMENT MODELS: ORGANIZATIONAL CHOICE AND STRATEGIC APPLICABILITY

Tsvetelina I. Metodieva

DEPARTMENT OF COMMUNICATION AND COMPUTER ENGINEERING AND SECURITY TECHNOLOGIES, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712, 115, UNIVERSITETSKA STR., E-MAIL: ts.metodieva@shu.bg

ABSTRACT: *This study examines the advantages, disadvantages, and applicability of centralized, decentralized, and hybrid security management models in contemporary organizations. Based on a comparative analysis and an organizational maturity-based approach, a framework for strategic model selection is proposed. The study highlights the importance of adaptability and integration between central control and local responsibility, especially in the context of modern cyber threats, globalization, and regulatory requirements [1,2].*

KEY WORDS: *Security, Centralized management, Decentralization, Hybrid model, Organizational maturity, Information security.*

1. Introduction

Organizational security is a fundamental component of the sustainable and effective functioning of modern institutions. It is not limited to the technical aspects of information security, but encompasses a wide range of managerial, cultural and regulatory practices. One of the key issues is the choice of security management structure: centralized, decentralized or hybrid.

The purpose of this report is to present a systematic overview of these three models, their applicability to the maturity of organizations, as well as to offer strategic guidance for choosing an appropriate model.

2. Security building models

Before making a strategic decision regarding the security structure of an organization, a clear understanding of the main models for building it is necessary - centralized, decentralized, and hybrid.

Centralized model

Centralized models are successfully applied in organizations with high requirements for control and compliance – e.g. the banking sector or the energy sector. [5] In the Bulgarian context, an example of centralized management is observed in the systems of the Ministry of Interior (MI) and the State Agency for Electronic Governance [9,13].

Decentralized model

Decentralization is characteristic of multinational companies and institutions with high organizational autonomy, such as universities [6]. In Bulgaria, a similar practice is observed in state higher education institutions, where faculties implement their own policies within a common framework [10,11].

Hybrid model

The hybrid model combines central policy with local implementation, an approach that addresses the need for flexibility and control in a highly dynamic risk environment [4]. This practice is common in large corporate structures and public organizations with complex hierarchies [1].

For a clearer understanding of the advantages and limitations of the considered models, it is necessary to make a comparative analysis that outlines their main differences in the context of security management.

The comparison between the models is presented in table 1, based on an adaptation from ISO/IEC 27001 and the analysis of Whitman & Mattord [7].

Table 1 Comparison between centralized and decentralized models

Criterion	Centralized model	Decentralized model
Control	Strong and central	Distributed
Flexibility	Low	High
Incident response	Slower	Faster
Compliance with standards	Easier	More difficult
Expenses	Lower	Higher
Communication	Vertical	Horizontal and vertical
Management complexity	Low	High

The comparative analysis performed shows that the choice of a security management model cannot be universal, but depends on a number of internal characteristics of the organization, among which the level of maturity of the security system occupies a leading place [14].

To be effective in practice, benchmarking between models must be tailored to the specific context of the organization – most notably its current level of maturity in security management.

In order to choose the most appropriate security management model, it is necessary that it be consistent with the organization's current level of maturity in this area [15].

Table 2 Model recommendation according to security maturity

Maturity level	Recommended model	Justification
0 - 1	Centralized	Low readiness of units
2 - 3	Hybrid	Balanced delegation is needed
4	Decentralized/Hybrid	Maturity for autonomous driving

Table 2 presents the recommended relationship between the level of maturity of the security system and the corresponding organizational model – centralized, decentralized or hybrid management. The proposed structure is based on a five-stage maturity assessment model, with each stage reflecting the degree of formalization, effectiveness, and integration of security processes within the organization. At lower maturity levels (0–1), the centralized model is most appropriate, as it provides the necessary degree of control and coordination in conditions of insufficiently developed processes. At medium maturity (levels 2–3), a hybrid approach is recommended, combining centralized policies with delegated functions at the local level. At high maturity (level 4), decentralization becomes possible and desirable, as the organization now has the capacity to independently implement and control security measures. This relationship between maturity and model choice is essential for effective strategic security management.

After presenting the theoretical models and their correlation to the maturity of the security system, practical examples should be presented that illustrate their real-world application in various organizational contexts.

Table 3 Practical examples

Organization	Model	Justification
Central Bank	Centralized	Regulations and the need for central control
International Trade Corporation	Hybrid	Local adaptation + centralized monitoring
University	Hybrid	Faculties have autonomy but follow common policies

They are supplemented with real cases from Bulgarian institutions:

• Centralized structure: National Health Information System (NHIS);

• Decentralized: Sofia University;

• Hybrid: NRA, with centralized monitoring, but local implementation of measures in the territorial directorates. [10]

The choice between the three models should not be perceived as an end goal, but as part of a dynamic process, taking into account:

• organizational culture;

• technological infrastructure;

• regulatory requirements;

• geographical distribution;

• human and financial resources.

The hybrid model is the most flexible, but requires maturity, coordination, and clarity of responsibilities.

Centralization allows for uniformity and control, but risks loss of flexibility. Decentralization brings adaptability, but also diversity. The hybrid model offers balance, especially when organizational maturity is present [2,9].

Security management [12] is not only a matter of technology, but above all an organizational decision related to structure, control and culture. This study highlights the need for:

• maturity assessment before choosing a model;

• strategic approach to delegation;

• creation of a communication framework between central and local units;

• continuous improvement of the model in relation to the evolving environment.

The choice of a security model [12] should be the result of a systematic analysis based on:

• maturity level;

• cultural and structural characteristics;

• availability of resources;

• regulatory framework (e.g. GDPR, NIS2, ISO 27001).

It is recommended to periodically rethink the model in light of changes in technology, threats, and regulations [1,10].

Acknowledgments

This article is supported by internal research project RD-08-109/05.02.2025 “Design and build a scalable research platform for Edge AI/HPS analytics”, Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department of Communication and Computer Technology and Security Technologies.

References:

[1] Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.

[2] Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. Information Systems Management, 24(4), 361–372.

[3] ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems.

[4] National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1.

[5] Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

[6] Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business School Press.

[7] Whitman, M. E., & Mattord, H. J. (2022). Principles of information security (7th ed.). Cengage Learning.

[8] European Union. (2023). Directive (EU) 2022/2555 (NIS2 Directive).

[9] State Agency for Electronic Governance. (2022). Guide for assessing the maturity of information security systems in the administration. Sofia

[10] Popov, V. (2021). Models of information security management in public administration. Scientific papers of the University of National and World Economy, (1), 93–105.

[11] Stamenov, I. (2020). Information Security and Cybersecurity in Organizations. Sofia: Tsenov Academic Publishing House.

[12] Hristov, Hr., Boyanov, P., Trifonov, T., Approaches to identify vulnerabilities in the security system of the social organization and computer resources, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), vol. 5, 2014, pp. 101-107, DOI: https://doi.org/10.46687/jsar.v5i1.115.

[13] Dimanova, D., Kuzmanov, Z., Risk management in information security, Conference proceedings MATTEX 2018. Information, Technical and Economical Problems of Security Systems, October 2018, Shumen, ISSN: 1314-3921, vol. 2, part. 1, pp. 139-145.

[14] Dimanova, D., Kuzmanov, Z., International security standards, Conference proceedings MATTEX 2018. Information, Technical and Economical Problems of Security Systems, October 2018, Shumen, ISSN: 1314-3921, vol. 2, part. 1, pp. 131-138.

[15] Simeonova, I., Metodieva, TS., Model for administrative security management in a municipality, Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 26, Shumen, 2024, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 93-105, DOI: https://doi.org/10.46687/jsar.v26i1.397, Indexed in EBSCO (USA), ROAD, Crossref, National Centre for Information and Documentation (Bulgaria), Google Scholar, Mendeley, ResearchGate.