European Research Studies Journal
Volume XXIX, Issue 2, 2026

pp. 880-894

Organisational Security Management in the TSL Sector in the Context of Contemporary Threats

Submitted 23/04/26, 1st revision 05/05/26, 2nd revision 20/05/26, accepted 30/06/26

Tomasz Grudniewski[1], Zbigniew Ciekanowski[2], Jarosław Wołejszo[3], Rafał Parczewski[4], Aneta Chrząszcz[5], Barbara Drapikowska[6]

Abstract:

Purpose: *The aim of this article is to identify and analyse the key determinants of integrated security management in companies operating in the transport, freight forwarding and logistics (TSL) sector, and to develop an original security management model integrating risk management, operational security, information security, cybersecurity, personnel safety and business continuity management, with a view to enhancing organisational resilience and the efficiency of logistics processes.*
Design/Methodology/Approach: *The article addresses the following research question: How does integrating key areas of safety management increase the organisational resilience of enterprises in the TSL sector? A research hypothesis was formulated, according to which the implementation of an integrated safety management model encompassing risk management, operational safety, information security, cybersecurity, personnel safety and business continuity management contributes to increasing organisational resilience and improving the operational effectiveness of companies in the TSL sector. The research employed a method of critical analysis and synthesis of the relevant literature, an analysis of international management standards (ISO 31000, ISO 28000, ISO 22301 and ISO/IEC 27001), an analysis of selected industry reports, and a method of conceptual modelling.*
Findings: *The analysis demonstrated that effective security management in TSL sector enterprises requires integrating risk management, operational security, cybersecurity, information security, personnel security, and business continuity management into a single management system. The developed model enables comprehensive threat identification, supports the decision-making process and enhances the organisational resilience of enterprises.*
Practical implications: *The proposed model can serve as a tool to support management in the TSL sector in designing and improving security management systems. Its application may*

[1]*John Paul II University in Biala Podlaska, Poland, ORCID: 0000-0003-3394-8992, e-mail: gisbourne2@gmail.com;*
[2]*The same as in 1, ORCID: 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*
[3]*President Stanisław Wojciechowski University of Kalisz, Poland, ORCID: 0000-0002-7216-3496, e-mail: j.wolejszo@uniwersytetkaliski.edu.pl;*
[4]*Military University of Technology, Poland, ORCID: 0000-0002-2603-0596, e-mail: rafal.parczewski1@wat.edu.pl;*
[5]*The same as in 1, ORCID: 0000-0001-9749-274X, e-mail: aneta.chrzaszcz@op.pl;*
[6]*War Studies University, Poland, ORCID 0000-0002-6852-2791, e-mail: bdrapikowska@o2.pl;*

contribute to improving business continuity, reducing risk levels and increasing the efficiency of logistics and transport processes.
Originality/Value: *The article's originality lies in the development of a proprietary integrated safety management model for companies in the TSL sector, which integrates strategic, operational, and supporting areas of safety into a single management system. The model contributes to the development of research on organisational security and may serve as a basis for further empirical research into the assessment of its effectiveness in business practice.*

Keywords: *Integrated security management, organisational security, TSL sector enterprises, risk management, organisational resilience, business continuity.*

JEL codes: *D81, M11, M15, L91, R41.*

Paper type: *Research article.*

1. Introduction

The transport, freight forwarding and logistics (TSL) sector plays a vital role in the functioning of the modern economy, ensuring the efficient flow of raw materials, products and information between participants in domestic and international supply chains. The dynamic growth of e-commerce, advancing globalisation, rising customer expectations and the rapid digitalisation of logistics processes mean that companies in the TSL sector are operating in an increasingly complex and unpredictable environment.

At the same time, there is a growing number of threats that could disrupt transport and logistics processes, including operational, cyber, organisational and personnel risks, as well as the effects of economic, geopolitical and environmental crises. Consequently, organisational security is becoming one of the key factors influencing companies' ability to maintain business continuity, organisational resilience and long-term competitiveness.

The modern approach to security management goes beyond the traditional understanding of the protection of people, property or information. Comprehensive security management, integrating risk management, cybersecurity, logistics process security, information security, personnel security and business continuity management, is becoming increasingly important.

The integration of these areas enables more effective identification of threats, mitigation of their impacts and the building of an organisation's resilience to internal and external disruptions. This is confirmed by international management standards, in particular ISO 31000 on risk management, ISO 28000 on supply chain security,

ISO 22301 on business continuity management, and ISO/IEC 27001 on information security management systems.

An analysis of the relevant literature indicates that existing studies most often focus on selected aspects of security in TSL sector enterprises, such as risk management, cybersecurity, transport security or supply chain resilience. Attempts to present a comprehensive model integrating all key areas of an organisation's security within a single management system, however, are relatively rare. Filling this research gap is significant both from the perspective of the development of management and quality sciences and from the perspective of the operational practice of logistics enterprises.

The aim of this article is to develop an original model of integrated security management in companies in the TSL sector, taking into account the contemporary operating conditions of organisations and the requirements arising from international management standards.

The study analyses the safety conditions within organisations, presents the process of hazard identification and risk management, and subsequently proposes a model integrating the key elements of an enterprise's safety management system. Achieving this objective enables the identification of solutions that support the building of organisational resilience, enhance business continuity and reduce risk levels in enterprises in the TSL sector.

2. Security Management Conditions in TSL Sector Enterprises

The transport, freight forwarding and logistics (TSL) sector is one of the most important elements of the modern economy, responsible for ensuring the continuous flow of raw materials, semi-finished products and finished goods between manufacturers, suppliers and customers. The dynamic growth of global supply chains, the ongoing digitalisation of logistics processes and the increasing number of threats mean that an organisation's security is becoming one of the key factors determining its ability to operate effectively and maintain a competitive advantage.

Modern TSL companies cannot limit security to the physical protection of infrastructure or cargo alone. Comprehensive security management, encompassing people, processes, information, technologies and relationships with business partners, is becoming increasingly important. This is confirmed by the requirements of the ISO 28000:2022 standard, which highlight the need to establish an integrated security management system covering all areas of the organisation's operations (ISO 28000:2022).

Organisational security is now viewed as an organisation's ability to maintain the continuity of its processes whilst minimising the impact of internal and external threats. It encompasses the protection of both tangible and intangible assets,

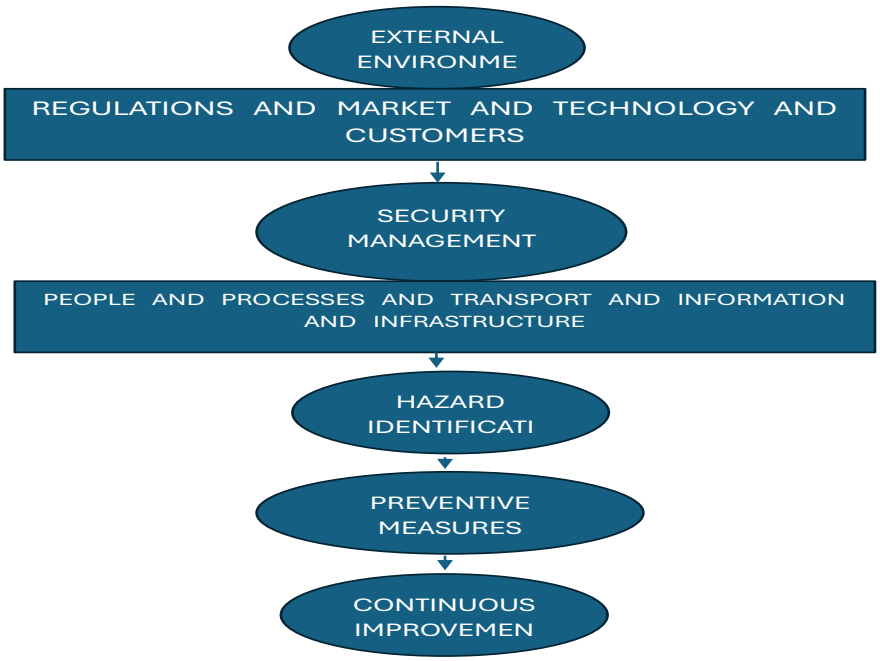
including information, technical infrastructure, IT systems, personnel and the organisation's reputation.

Management literature emphasises that organisational security is not a separate area of a company's operations, but should be an integral part of all management processes – from strategic planning, through the organisation and implementation of logistics processes, to monitoring and continuous improvement (Chockalingam *et al.,* 2017). This approach enables more effective identification of threats and the implementation of preventive measures even before a crisis situation arises.

The specific nature of companies in the TSL sector makes them particularly vulnerable to a range of risks. These organisations operate in an environment characterised by rapid change, a large number of supply chain participants and significant dependence on transport infrastructure and ICT systems.

Any disruption to the transport process, IT system failure, delivery delay or data loss can lead to significant financial losses and a loss of customer trust. For this reason, the security of TSL companies should be analysed in a systematic manner, covering organisational, technical, information and human resources aspects. The determinants of organisational security in TSL sector companies are set out below (Figure 1).

Figure 1. *Determinants of organisational safety in companies in the TSL sector.*



Source: *Own study.*

A key element of modern safety management is the process-based approach. This means that safety should be taken into account at every stage of the logistics process – from transport planning, through warehousing and transhipment, right through to the delivery of the product to the end customer. Safety management must not be limited solely to responding to incidents, but should be based primarily on anticipating them, analysing risks and implementing appropriate preventive measures.

This approach increases an organisation's resilience to disruptions and enables business continuity to be maintained even in the event of unforeseen incidents. In the day-to-day operations of TSL companies, the range of threats is systematically expanding. In addition to traditional threats such as damage to cargo, theft or breakdowns of transport vehicles, cyber threats, disruptions to IT systems, human error, staffing issues and risks arising from the globalisation of supply chains are becoming increasingly significant.

The transport of dangerous goods constitutes a particularly regulated area of operational risk, in which international and national legal requirements must be translated into detailed internal organisational instructions and procedures (Szkudlarek and Szkudlarek, 2024). The high level of digitalisation within companies means that information security is becoming just as important as the physical security of the logistics infrastructure (Żurawski *et al.,* 2025). The loss of data availability, its modification or disclosure to unauthorised persons can lead to the disruption of operational processes and significant economic losses (Ali, 2026).

Effective security management therefore requires the implementation of a unified system encompassing threat identification, risk assessment, planning of preventive measures, monitoring of security levels and continuous improvement of the organisation.

This approach is reflected in the ISO 28000:2022 standard, which states that the security management system should be integrated with the organisation's other management systems and cover all processes affecting the security of the organisation's operations. This standard also emphasises the importance of leadership, management commitment and organisational culture as key determinants of the security system's effectiveness. The key areas of security for companies in the TSL sector are presented in Table 1.

Table 1. *Key areas of security for companies in the TSL sector.*

Area	Examples of threats
Transport	collisions, delays, theft
Warehousing	fires, equipment failures
Information	cyberattacks, data breaches
Human resources	staff errors, staff turnover

Area	Examples of threats
Infrastructure	system failures, power cuts
Suppliers	disruption to the supply chain

Source: *Own analysis based on ISO 28000.*

Companies in the TSL sector are also increasingly using solutions that support organisational resilience, such as business continuity management, logistics process monitoring systems, data analytics, artificial intelligence and Internet of Things technologies. The integration of these solutions enables real-time monitoring of transport processes, faster identification of threats and the implementation of measures to mitigate the effects of potential incidents (Mishra *et al.,* 2018). As a result, organisational security becomes not only a tool for risk mitigation, but also a factor in building competitive advantage and enhancing the efficiency of the company's operations.

Modern companies in the TSL sector operate in an environment characterised by a high level of uncertainty and the complexity of threats. Effective security management requires a shift away from fragmented security measures towards an integrated model encompassing all areas of the organisation's operations. This approach not only minimises risk but also enhances organisational resilience, improves the quality of logistics processes and ensures business continuity in a rapidly changing environment.

3. Threat Identification and Risk Management in Companies within the TSL Sector

Modern companies in the transport, freight forwarding and logistics sectors operate in an environment characterised by high volatility in economic, technological and organisational terms. The growing complexity of global supply chains, the digitalisation of logistics processes and rising customer expectations mean that risk management is becoming one of the most important elements of an organisation's safety management system.

The literature emphasises that effective risk management should not be limited merely to responding to the consequences of disruptions, but should, above all, focus on their early identification, analysis and the implementation of measures to reduce the likelihood of their occurrence (Oliveira *et al.,* 2017). It is precisely this approach that forms the basis of the ISO 31000 standard, which states that risk management should be an integral part of all organisational processes and should support decision-making at both the strategic and operational levels.

The identification of risks in TSL companies involves recognising all factors that could negatively impact the execution of logistics processes. In practice, these risks are multi-dimensional and encompass both internal and external factors. The most common include breakdowns of transport vehicles, damage to warehouse

infrastructure, staff errors, inadequate planning of logistics processes, disruptions to ICT systems, cyber-attacks, the termination of cooperation with suppliers, as well as random events such as natural disasters or geopolitical crises (Hermoso-Orzáez and Garzón-Moreno, 2022). The modern approach to security management involves analysing the interdependencies between these threats, as the occurrence of a single incident often leads to a domino effect throughout the entire supply chain.

A key stage in the security management process is risk analysis, which involves determining the likelihood of a threat occurring and the scale of its potential consequences for the organisation. This analysis enables the prioritisation of security measures and the rational allocation of financial and organisational resources.

In TSL companies, both qualitative methods, based on expert assessment, and quantitative methods utilising statistical models, scenario analysis or multi-criteria risk assessment methods are employed. IT systems supporting real-time data analysis are also increasingly being used, enabling the monitoring of threats and the forecasting of potential disruptions to logistics processes.

The literature indicates that the effectiveness of risk management depends on the correct classification of threats. In companies within the TSL sector, five basic risk groups can be identified:

- operational risk, associated with the execution of transport and warehousing processes;
- financial risk, resulting from changes in operating costs and loss of financial liquidity; technological risk, covering failures of IT systems and technical equipment;
- human resources risk, associated with a shortage of skilled staff and human error;
- and cyber risk, the significance of which is growing rapidly alongside the ongoing digitalisation of businesses (Emrouznejad, Abbasi, and Sıcakyüz, 2023).

This approach enables a comprehensive assessment of an organisation's vulnerability to disruptions and the selection of appropriate protective measures (NIST, 2024).

Business Continuity Management (BCM) is also playing an increasingly important role in an organisation's security management. Its primary objective is to ensure that the organisation's key processes can be maintained even in the event of serious disruptions. In accordance with the guidelines of ISO/TS 22318, business continuity management should include an analysis of the impact of threats on the organisation's operations, the preparation of contingency plans, the definition of recovery procedures, and the systematic testing of the effectiveness of the adopted solutions (ISO/TS 22318:2021).

In the TSL sector, this is of particular importance given companies' high dependence on timely deliveries, cooperation with business partners and the availability of logistics infrastructure.

Building organisational resilience is also a key element of modern security management. Resilience refers to a company's ability to anticipate threats, prepare for their occurrence, respond effectively and quickly return to normal operations once a crisis has ended (Ciekanowski *et al.,* 2024).

In TSL companies, organisational resilience encompasses, amongst other things, supplier diversification, the development of alternative transport routes, the maintenance of adequate safety stock levels, the development of staff competencies, and the implementation of systems to monitor logistics processes.

Research indicates that organisations characterised by a high level of resilience achieve better operational results and rebuild their production and logistics capacities more quickly following disruptions (Lang, Zanker and Glöser-Chahoud, 2026).

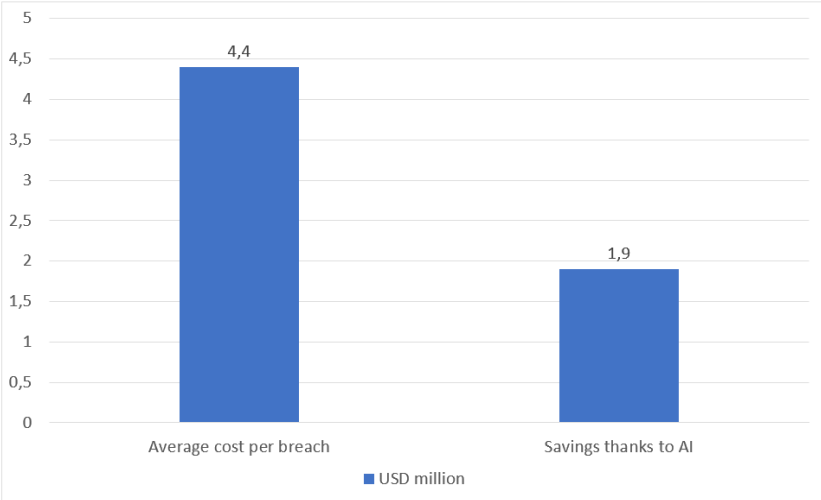
In recent years, cybersecurity has become particularly important for companies in the TSL sector. The development of transport management systems (TMS), warehouse management systems (WMS), Internet of Things (IoT) technology, artificial intelligence and cloud-based solutions has significantly increased the efficiency of logistics processes, whilst simultaneously creating new areas of vulnerability for organisations to cyberattacks.

These threats include, amongst others, ransomware attacks, data theft, the takeover of logistics systems and the disruption of communications with business partners. The NIST SP 800-161r1 document emphasises that cybersecurity risk management should cover the entire supply chain, rather than just the organisation's own resources, because the vulnerability of a single supplier can disrupt the entire organisation. (NIST, 2024). Selected organisational security indicators are presented below (Figure 2).

Increasingly, companies are also using artificial intelligence and predictive analytics tools to support the risk identification process (Chodyka *et al.,* 2026). Machine learning algorithms enable analysis of large datasets related to transport, warehousing, and order fulfilment, identifying anomalies and predicting potential disruptions before they occur.

These solutions enhance the effectiveness of risk management, reduce an organisation's response time and support decision-making by senior management (Jahin, Naife, Saha, and Mridha, 2025).

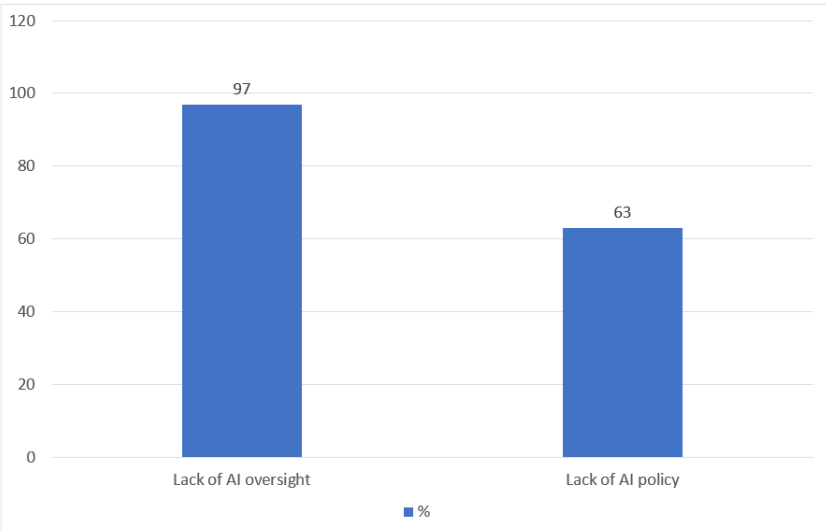
Figure 2. *Selected organisational security indicators.*



Source: *IBM Cost of a Data Breach Report 2025.*

At the same time, they require an appropriate level of information security and high-quality data used in analytical processes. The use of systems supporting transport planning, warehouse management, fleet monitoring, and data analysis increases the efficiency of business operations but also introduces new risks related to information security and access control for systems utilising AI solutions. The findings of the IBM Cost of a Data Breach Report 2025 indicate that many organisations are implementing AI-based solutions without adequate oversight mechanisms or formal policies governing their use. These data are presented in the chart below (Figure 3).

Figure 3. *Selected areas of organisational immaturity in AI security management*



Source: *Own analysis based on IBM, Cost of a Data Breach Report 2025.*

Effective risk management in TSL sector enterprises requires a comprehensive approach encompassing threat identification, analysis of the organisation's vulnerabilities, risk assessment, the implementation of preventive measures, and systematic monitoring of their effectiveness.

Integrating risk management with the organisation's security management system helps to increase the company's resilience to disruptions, improve the continuity of logistics processes and mitigate the negative effects of crisis events. Consequently, it forms the foundation for building an integrated security management model, which will be presented in the next section of this article.

4. An Integrated Safety Management Model for Companies in the TSL Sector

Modern companies in the transport, freight forwarding and logistics sector operate in an environment characterised by the growing complexity of operational processes and a rapidly changing economic and technological landscape. The rise in the number of threats, advancing digitalisation, the development of intelligent transport systems and an ever-increasing reliance on global supply chains mean that the traditional approach to organisational security is proving insufficient.

Effective security management now requires the integration of measures covering risk management, information security, cybersecurity, infrastructure protection, personnel security and the assurance of business continuity.

This approach is consistent with the requirements of the ISO 31000, ISO 28000, ISO 22301 and ISO/IEC 27001 standards, which highlight the need to establish a coherent security management system covering all organisational processes. The model described below is illustrated in the figure below (Figure 4).

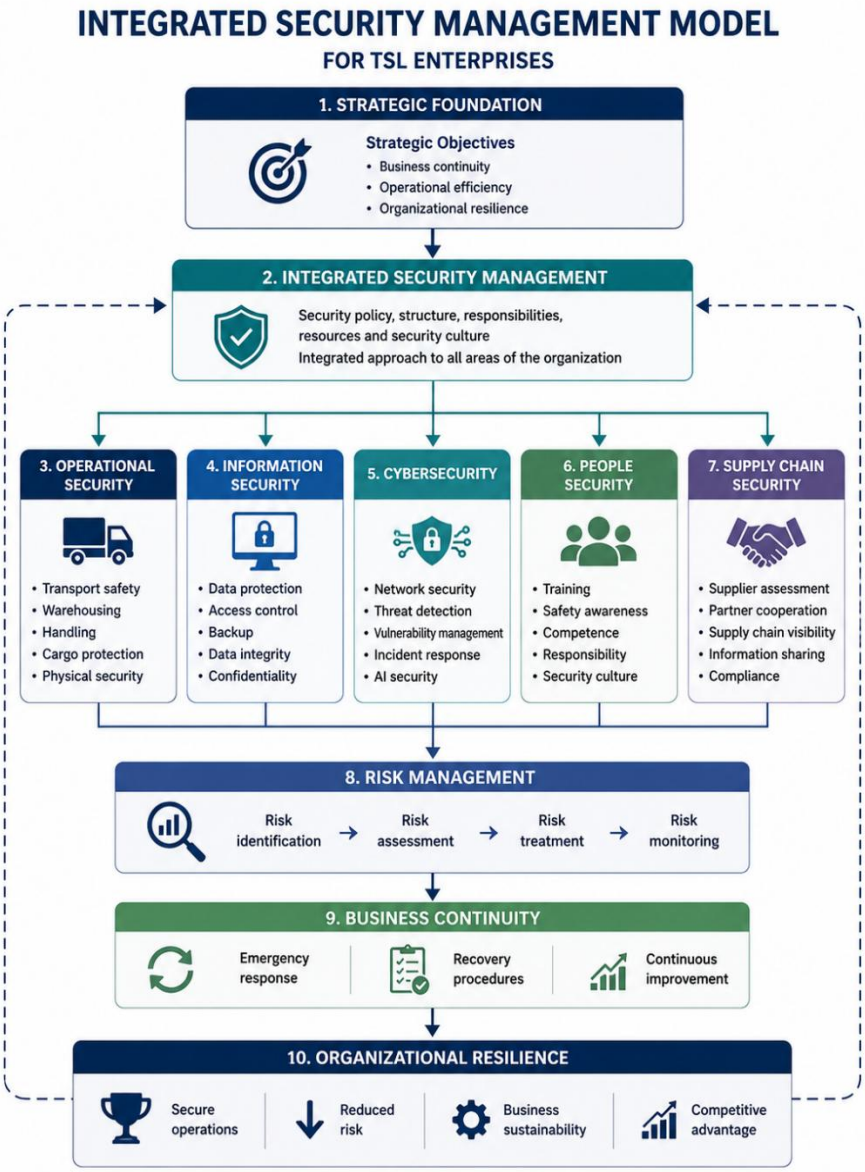
The fundamental premise of the integrated security management model is to treat security as a key element of an organisation's strategic management. This means that decisions concerning security should be taken into account as early as the strategic planning stage, rather than solely as measures taken in response to incidents as they occur.

The organisation's management should define the security policy, strategic objectives and the level of acceptable risk, and then ensure that adequate organisational, financial and technical resources are available to enable the implementation of these objectives.

The commitment of top management is one of the fundamental prerequisites for the effective functioning of a security management system, as reflected both in ISO standards and in numerous studies on organisational management.

The second element of the model is comprehensive risk management covering all processes carried out within the TSL company. This process should begin with the systematic identification of hazards, followed by an analysis of the likelihood of their occurrence and an assessment of the potential consequences for the organisation's operations.

Figure 4. *Model of integrated security management in TSL sector organisations.*



Source: *Own work based on a review of the literature (ISO 31000:2018; ISO 28000:2022; ISO 22301:2019; ISO/IEC 27001:2022; NIST SP 800-161r1).*

The results of the risk assessment form the basis for selecting appropriate measures to prevent, mitigate or accept risk in accordance with the adopted safety policy. Another key element is the continuous monitoring of risk levels and the periodic updating of risk assessments in light of changes in the company's operating environment.

Another pillar of the model is the security of logistics processes. In companies within the TSL sector, security should cover all stages of service delivery, from transport planning, through warehousing and transhipment, to the delivery of the consignment to the end recipient.

At each of these stages, it is essential to identify potential risks and implement appropriate control measures. Of particular importance is the monitoring of logistics processes using TMS and WMS systems, GPS technology, the Internet of Things, and analytical tools that enable the real-time detection of irregularities and the implementation of corrective actions.

Information security and cybersecurity remain key components of the integrated model. The development of digital technologies has meant that TSL companies at are increasingly reliant on ICT systems responsible for transport planning, fleet management, warehouse operations and communication with business partners.

For this reason, organisations should implement solutions compliant with the requirements of the ISO/IEC 27001 standard and NIST guidelines, covering information access management, data encryption, security incident monitoring, data backup and regular staff training in cybersecurity. Managing the risks associated with the use of artificial intelligence and cloud services is also of particular importance.

Human resources management is also an integral part of an organisation's security. Numerous studies indicate that the human factor remains one of the most common causes of security incidents. Therefore, companies in the TSL sector should develop a security culture based on threat awareness, staff accountability and the systematic improvement of skills. This includes conducting regular training sessions, practical exercises, internal audits and assessments of staff awareness levels regarding information security, data protection, occupational safety and crisis response.

Business Continuity Management (BCM) plays a key role in the proposed model. Companies in the TSL sector should have business continuity plans and crisis response procedures in place, enabling them to maintain core logistics processes even in the event of serious disruptions. This applies, amongst other things, to IT system failures, power cuts, transport disruptions, cyber-attacks or the loss of key suppliers. Regular testing of contingency procedures and analysis of lessons learnt from actual incidents help to enhance the organisation's resilience.

The final element of the model is a mechanism for continuous improvement. The safety management system should be subject to systematic evaluation through the monitoring of performance indicators, the conduct of internal audits, the analysis of incidents, and the implementation of corrective and preventive actions.

In practice, TSL companies apply the Deming cycle (PDCA), which enables the planning of actions, their implementation, the assessment of their effectiveness, and the introduction of improvements. This approach ensures the flexibility of the safety system and allows it to be adapted to the organisation's changing operating conditions.

The presented model of integrated security management assumes close cooperation between all organisational units of the company and the integration of security with core management processes. As a result, security ceases to be merely a protective function and becomes one of the key elements in building organisational resilience, operational efficiency and the company's competitive advantage.

Implementing the integrated model helps to reduce risk levels, enhance the organisation's ability to respond to disruptions, and ensure the stable operation of companies in the TSL sector amidst today's economic and technological challenges.

5. Conclusion

Modern companies in the transport, freight forwarding and logistics sectors operate in an environment characterised by rapid technological change and a growing number of operational, organisational, cyber and economic risks.

For an organisation to function effectively, it is therefore necessary to move away from a fragmented view of security towards a comprehensive approach that integrates all key areas of the company's operations.

Organisational security should not be treated solely as a protective function, but as one of the fundamental elements supporting the achievement of strategic objectives, ensuring business continuity and building long-term organisational resilience.

The analysis carried out has shown that effective security management in TSL sector enterprises should be based on the systematic identification of threats, a comprehensive risk assessment and the implementation of preventive measures covering logistics processes as well as information security, cybersecurity, staff protection and cooperation with supply chain participants.

The use of modern technologies also plays a significant role, including TMS and WMS systems, the Internet of Things, data analytics and artificial intelligence, which support the monitoring of logistics processes and enable the faster identification of potential threats. At the same time, the development of these

technologies requires the implementation of effective cyber risk management mechanisms and the fostering of a safety culture within the organisation.

The proprietary model of integrated security management for enterprises in the TSL sector, developed in this article, proposes a comprehensive approach to organising a security system, integrating risk management, operational security, information security, cybersecurity, personnel security, supply chain security and business continuity management.

The application of such a model makes it possible to increase the organisation's resilience, reduce vulnerability to disruptions and improve the efficiency of logistics processes. The model can serve as a practical tool to support management in designing and improving safety systems within companies in the TSL sector.

It should be emphasised that the considerations presented here are conceptual in nature and are based on an analysis of the relevant literature and current safety management standards. A reasonable direction for further research is the empirical verification of the proposed model in companies within the TSL sector, taking into account variations in their size, business profile and the degree of digitalisation of their logistics processes.

The results of such research may form the basis for further refinement of the model and the development of tools enabling the assessment of the maturity level of organisations' safety management systems.

References:

Ali, R. 2026. Operationalising Information Security Management: A Procedural Framework Analysis of ISO/IEC 27001:2022. Implementation in a Financial-Technology Organisation. https://arxiv.org/abs/2604.23230.

Chodyka, M., Ciekanowski, Z., Krecikij, J., Wronka, S., Żurawski, S., Drapikowska, B. 2026. The Impact of Artificial Intelligence on Organisational Security Management, European Research Studies Journal, Volume XXIX, Issue 2.

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.

Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations, NIST. https://www.nist.gov/publications/cybersecurity-supply-chain-risk-management-practices-systems-and-organizations.

ISO 28000:2022. Security and resilience — Security management systems — Requirements.

ISO/TS 22318:2021. Security and resilience — Business continuity management systems — Guidelines for supply chain continuity management.

Jahin, M.A., Naife, S.A., Saha, A.K., Mridha, M.F. 2025. AI in Supply Chain Risk Assessment: A Systematic Literature Review and Bibliometric Analysis. https://arxiv.org/abs/2401.10895.

Chockalingam, S., Hadziosmanovic, D., Pieters, W., Teixeira, A., van Gelder, P. 2017. Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications. https://arxiv.org/abs/1707.02140.

Emrouznejad, A., Abbasi, S., Sıcakyüz, V.C. 2023. Supply chain risk management: A content analysis-based review of existing and emerging topics. Supply Chain Analytics, Volume 3.

Hermoso-Orzáez, M.J., Garzón-Moren, J. 2022. Risk management methodology in the supply chain: a case study applied. Annals of Operations Research, Volume 313.

Lang, S.M., Zanker, C., Glöser-Chahoud, S. 2026. From risk to resilience: a multi-layered framework for supplier risk assessment to strengthen supply chain resilience. International Journal of Physical Distribution & Logistics Management, Volume 56, Issue 5.

Mishra, D.K., Henry, S., Sekhari, A., Ouzrout, Y. 2018. Traceability as an integral part of supply chain logistics management: an analytical review. https://arxiv.org/abs/1811.06358.

Oliveira, U.R., Marins, F.A.S., Rocha, H.M., Salomon, V.A.P. 2017. The ISO 31000 standard in supply chain risk management. Journal of Cleaner Production, 151.

Szkudlarek, I., Szkudlarek, K. 2024. Bezpieczeństwo przewozu towarów niebezpiecznych – przepisy wewnętrzne na przykładzie Polskich Kolei Państwowych Polskich Linii Kolejowych S.A. Studia Kaliskie, Vol. 12, pp. 349-366.

Zurawski, 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.