Article

Not peer-reviewed version

Business Intelligence as a Strategic Resource: Integrating the SIDeARM Model into Strategic Management and Corporate Security

Miroslav Mitrovic *

Posted Date: 16 September 2025

doi: 10.20944/preprints202509.1321.v1

Keywords: business intelligence; strategic management; corporate security; SIDeARM model

 doi:10.20944/preprints202509.1321.v1

Article

Business Intelligence as a Strategic Resource: Integrating the SIDeARM Model into Strategic Management and Corporate Security

Miroslav Mitrovic

Faculty of Business and Law, MB University, Belgrade, Serbia; mitrovicmm@gmail.com

Abstract

Organisations today operate in an environment marked by geopolitical instability, technological disruption, and systemic risks that threaten continuity and competitiveness. Traditional approaches to management, based primarily on financial and operational indicators, are insufficient to address these complex challenges. Previous research has emphasised the importance of information and analytical systems for decision-making, yet their integration into strategic management frameworks remains underdeveloped. This paper aims to explore the role of business intelligence as a strategic resource and examine how it can be effectively institutionalised within corporate security and governance. The study introduces and evaluates the SIDeARM model, which aims to integrate intelligence functions with adaptive risk management to enhance decision-making and organisational resilience. The research is based on a multi-layered methodology that includes a review of relevant academic and professional literature, the development of a conceptual framework structured around four intelligence domains, and the application of analytical tools such as scenario planning, risk assessment techniques, and intelligence dashboards. To illustrate the practical value of the framework, three case studies from the energy, pharmaceutical, and financial sectors were analysed, each selected for its exposure to volatility and systemic risks. The results confirm that business intelligence evolves from a supportive technical function into a strategic cornerstone of corporate decision-making. The SIDeARM model offers a structured pathway that combines precision in analysis with agility in strategy, enabling organisations to anticipate risks, adapt to disruptions, and reinforce their legitimacy through ethical and transparent practices. Case studies demonstrate that the model is transferable across industries, supporting resilience in critical infrastructure, innovation management, and financial stability. As the study is primarily conceptual and supported by illustrative cases, its conclusions require further empirical testing. Future research should expand validation of the SIDeARM model across different industries and organisational contexts, combining qualitative and quantitative approaches to assess its scalability and long-term applicability.

Keywords: business intelligence; strategic management; corporate security; SIDeARM model

1. Introduction

In the contemporary global environment, business organisations operate in conditions marked by rapid technological change, intensified competition, and an expanding spectrum of risks that go beyond purely economic parameters.

Traditional approaches to corporate strategy, once predominantly focused on market positioning and resource optimisation, are increasingly complemented by mechanisms of Business Intelligence (BI) and strategic intelligence, which serve as integrative frameworks for informed decision-making and organisational resilience (Watson, 2018; Lowenthal, 2020). The ability to transform data into actionable knowledge has become a central determinant of sustainable

 doi:10.20944/preprints202509.1321.v1

competitive advantage, aligning managerial decision-making with dynamic external and internal environments (Fleisher & Bensoussan, 2015).

Within this context, Strategic Management scholarship emphasises the importance of linking intelligence functions to long-term corporate governance and decision processes. Vigfússon, and colleagues (2021) highlight the numerous obstacles to strategy implementation, including organisational inertia, communication gaps, and lack of analytical capacity, while simultaneously identifying success factors that strengthen execution. Similarly, research on the strategic involvement of corporate boards emphasises the growing demand for intelligence-driven models of governance that can effectively address uncertainty and systemic risks (Bozhinovska, 2024). These insights converge with earlier contributions in Strategic Management that explicitly link corporate political activities and strategic communication (Mitrović, 2019), as well as the synergistic evaluation of corporate success through combined political and responsibility dimensions (Taillard & Mitrović, 2020). Together, these works provide a conceptual foundation for situating BI and corporate intelligence not only as support tools but as critical components of strategic management systems.

The literature further suggests that modern BI frameworks are inseparable from risk management and security considerations. Integrating open-source intelligence (OSINT), social media intelligence (SOCMINT), and predictive analytics enables organisations to anticipate market disruptions, reputational crises, and hybrid security threats (Hayes & Cappa, 2018; Zuech, Khoshgoftaar, & Wald, 2015). At the same time, ethical and legal frameworks such as the General Data Protection Regulation (GDPR) and international corporate governance standards require intelligence activities to adhere to principles of transparency, legitimacy, and responsibility (Voigt & Von dem Bussche, 2017). The convergence of these factors positions BI as a multidimensional construct: simultaneously technical, strategic, and normative.

Against this backdrop, this paper seeks to advance the debate by examining the integrative role of Business Intelligence in strategic management and by introducing the SIDeARM model (Strategic Intelligence and Decision-centric Adaptive Risk Management) as a novel conceptual framework. Building upon prior research published in Strategic Management (Mitrović, 2019; Taillard & Mitrović, 2020; Vigfússon et al., 2021; Bozhinovska & Eftimov, 2024), as well as broader scholarship in intelligence studies and strategic management (Crump, 2015; Wilkinson & Kupers, 2013; Duchek, 2020), the study argues that intelligence-driven approaches represent not only an operational necessity but a strategic imperative for corporate resilience and long-term sustainability.

2. Methods

The methodological framework of this study integrates a combination of literature review, conceptual modelling, analytical tools, and illustrative case studies to explore the intersection between Business Intelligence (BI) and Strategic Management. A distinctive feature of the research design is the application of the SIDeARM model (Strategic Intelligence and Decision-centric Adaptive Risk Management) at both theoretical and practical levels, to demonstrate its relevance for enterprise risk management and corporate security.

2.1. Literature Review

The study is grounded in a comprehensive review of academic and professional literature addressing business intelligence, corporate security, and strategic decision-making. Key works by Crump (2015), Lowenthal (2020), and Fleisher and Bensoussan (2015) were examined to establish the theoretical basis for corporate and competitive intelligence.

Additionally, normative and regulatory frameworks, including ISO standards related to risk management and corporate governance, were examined to identify formalised approaches to intelligence functions. Special attention was given to recent contributions by Mitrović (2025), who advanced models linking intelligence, strategic communication, and adaptive decision-making.

 doi:10.20944/preprints202509.1321.v1

The literature review also incorporated relevant studies published in Strategic Management (Mitrović, 2019; Taillard & Mitrović, 2020; Vigfússon et al., 2021; Bozhinovska & Eftimov, 2024), thereby situating the analysis within the ongoing academic debate.

2.2. Conceptual Framework

The conceptual foundation of the paper builds upon the identification of four core domains of BI:

1. Strategic intelligence – monitoring macro-environmental trends and long-term scenarios;
2. Competitive intelligence – analysis of rivals, markets, and sectoral dynamics;
3. Security intelligence – safeguarding corporate assets against cyber, reputational, and hybrid threats;
4. Operational intelligence – real-time data analysis for tactical and managerial decision-making.

This four-domain framework provides a structured lens for linking intelligence activities with strategic management processes.

2.3. Analytical Methods

Several analytical methods were applied to operationalise the conceptual framework:

- SWOT (Strengths, Weaknesses, Opportunities, Threats) for internal and external situational assessment;
- PESTEL (Political, Economic, Social, Technological, Environmental, Legal) for macro-environmental analysis;
- Foresight techniques for scenario planning and strategic anticipation;
- OSINT/SOCMINT (open-source and social media intelligence) for data collection from digital ecosystems;
- Business Intelligence dashboards and SIEM systems for real-time visualisation and detection of risks.

These methods ensure both qualitative depth and quantitative rigour, enabling multidimensional insight into strategic challenges.

2.4. Case Study Method

The applicability of Business Intelligence (BI) and the SIDeARM model is best illustrated through sectoral case studies, where intelligence functions directly influence strategic decision-making and organisational resilience.

Three industries—energy, pharmaceuticals, and finance—were selected due to their exposure to systemic risks, regulatory constraints, and high reliance on adaptive intelligence capabilities.

2.4.1. Energy Sector

The energy sector exemplifies how BI supports the anticipation of geopolitical risks and supply-chain disruptions. The Russian–Ukrainian war (2022–) created unprecedented volatility in European gas markets, leading to a dramatic restructuring of supply chains. BI-enabled scenario planning and PESTEL analyses allowed European energy companies to diversify suppliers, rapidly expand investments in LNG terminals, and accelerate the integration of renewables (Goldthau & Sitter, 2020).

Companies such as BP and Shell utilised BI dashboards to monitor sanctions, regulatory changes, and operational bottlenecks, thereby ensuring the continuity of energy provision while realigning their portfolios toward sustainability targets (Van de Graaf & Colgan, 2016).

 doi:10.20944/preprints202509.1321.v1

Within this context, the SIDeARM model provided a systematic pathway to integrate environmental scanning, risk identification, and resilience assurance into corporate strategy, thereby strengthening critical infrastructure protection.

2.4.2. Pharmaceutical Sector

The pharmaceutical industry highlights the dual role of BI in competitive intelligence and regulatory adaptation. During the COVID-19 pandemic, companies such as Pfizer-BioNTech and Moderna leveraged intelligence-driven R&D decision-making, monitoring global clinical trial data and regulatory approvals from agencies like the FDA and EMA (Ball & Feigenbaum, 2022).

Competitive intelligence also enabled firms, such as Novartis, to anticipate the impact of biosimilars and generic competition, thereby adjusting their research portfolios accordingly (Pisano, 2019). These examples demonstrate how BI supported both short-term market entry strategies and long-term innovation pipelines. The SIDeARM model proved particularly relevant by recalibrating priorities in response to emerging threats and by linking risk mitigation with reputational management in times of crisis.

2.4.3. Financial Sector

The financial sector provides evidence of BI's role in systemic risk management and resilience-building. HSBC introduced SIEM systems and AI-driven fraud detection in response to compliance failures and money laundering scandals between 2019 and 2022, using BI to strengthen monitoring capacity across jurisdictions (Basel Committee on Banking Supervision, 2018).

Similarly, Deutsche Bank adopted BI frameworks and predictive analytics to anticipate regulatory sanctions and market volatility, embedding intelligence into risk governance. In the fintech domain, companies such as PayPal employed BI-enhanced security intelligence to identify cyber threats and prevent large-scale fraud attempts, thereby sustaining consumer trust in digital ecosystems (Gai, Qiu, & Sun, 2018).

These cases underscore how operational and security intelligence functions, when integrated through the SIDeARM model, facilitate adaptive responses to both cyber and systemic vulnerabilities.

2.4.4. Comparative Insights

Across all three industries, the empirical evidence confirms that BI, particularly when structured through adaptive models such as SIDeARM, serves as both a preventive mechanism and a strategic enabler.

In energy, it supports critical infrastructure continuity amid geopolitical shocks; in pharmaceuticals, it fosters adaptive research and development, as well as regulatory compliance, during crises; and in finance, it safeguards systemic trust and operational integrity.

Collectively, these findings underscore the universality of BI as a cross-sectoral strategic resource and its contribution to long-term sustainability and risk-informed decision-making.

2.5. Model Application and Comparative Insights

The final methodological step involves applying the SIDeARM model, which combines strategic intelligence and adaptive risk management in decision-centric processes. The model was analysed in both theoretical and practical contexts to demonstrate how intelligence can be institutionalised within enterprise risk management (ERM) frameworks. This approach bridges the gap between abstract theoretical concepts and operational practices in corporate security and governance.

The comparative overview presented in Table 1 illustrates that each industry operationalises distinct combinations of SIDeARM modules in response to its specific risk environment. Nevertheless, all three case studies converge on the principle of adaptive decision-making, confirming the model's integrative and flexible nature.

 doi:10.20944/preprints202509.1321.v1

In the energy sector, the emphasis is placed on environmental scanning and assurance of resilience. That reflects the need for continuous monitoring of geopolitical and regulatory contexts, as well as the capacity to secure critical infrastructure under conditions of systemic disruption. The sector demonstrates how early detection of exogenous shocks—such as sanctions and supply-chain disruptions—can be translated into strategic resilience through diversification and sustainability measures.

In the pharmaceutical sector, the application of the SIDeARM model is characterised by adaptive analysis and decision calibration. Faced with regulatory complexity and high demands for innovation, firms such as Pfizer, Moderna, and Novartis have employed BI-driven intelligence to dynamically reprioritise R&D pipelines and align them with emerging health crises or competitive pressures. The ability to recalibrate strategic decisions in real time underscores the model's relevance for innovation-intensive industries.

In the financial sector, the dominant modules are monitoring and feedback, as well as risk identification. Here, BI dashboards and SIEM systems provide continuous oversight of systemic vulnerabilities, while predictive analytics supports rapid detection of fraud and compliance risks. The emphasis on monitoring and identification highlights how intelligence not only supports adaptive decision-making but also institutionalises resilience as a permanent organisational capability.

Table 1. Empirical Case Studies Demonstrating the Application of the SIDeARM Model Across Industries.

Industry / Case	Key Risks / Challenges	BI & Intelligence Tools	SIDeARM Modules Applied	Observed Outcomes
Energy Sector (EU gas crisis, BP & Shell)	Geopolitical shocks (Russia–Ukraine war), supply-chain disruptions, sanctions, regulatory shifts	PESTEL, scenario planning, and BI dashboards for supply and sanctions monitoring	Environmental Scanning, Risk Identification, Resilience Assurance	Diversification of suppliers (LNG), accelerated renewables, protection of critical infrastructure
Pharmaceutical Sector (Pfizer-BioNTech, Moderna, Novartis)	Pandemic-driven R&D urgency, regulatory complexity, global supply-chain instability	Competitive intelligence (patent/R&D pipelines), regulatory intelligence (FDA, EMA), foresight methods	Adaptive Analysis, Decision Calibration, Risk Identification	Accelerated vaccine R&D, effective regulatory navigation, strategic reprioritisation of biosimilars and generics
Financial Sector (HSBC, Deutsche Bank, PayPal)	Fraud, cyberattack, systemic financial risks, regulatory sanctions	SIEM systems, BI dashboards, predictive analytics, security intelligence	Monitoring & Feedback, Risk Identification, Decision Calibration	Enhanced fraud detection, improved compliance, strengthened

 doi:10.20944/preprints202509.1321.v1

				systemic resilience and customer trust

Source: (Author).

Taken together, the three cases confirm that the SIDeARM model is a transferable and scalable framework, adaptable to the unique requirements of diverse industries. Its integration into ERM and corporate security demonstrates its potential to bridge abstract theoretical concepts with operational practices. In this sense, the model provides both analytical precision and strategic agility, establishing a foundation for risk-informed decision-making across sectors.

3. Results

The findings of this study highlight the multifaceted role of Business Intelligence (BI) in strategic management, demonstrating its relevance not only as a technical resource but also as a critical axis of organisational governance, resilience, and competitive sustainability.

Results are presented along six thematic dimensions: integration into strategic management, four intelligence domains, methodological application, legal and ethical constraints, the SIDeARM model, and illustrative case studies.

3.1. Integration of Business Intelligence into Strategic Management

The analysis reveals that BI serves as a connective hub between corporate management, information technology, and security sectors. By aligning strategic foresight with operational data, BI enables organisations to anticipate systemic risks and to translate complex information into actionable insights (Watson, 2018).

This integrative role strengthens decision-making by ensuring that managerial choices are informed by both macro-level intelligence and micro-level operational signals (Crump, 2015; Lowenthal, 2020).

3.2. The Four Domains of Business Intelligence

The conceptual framework was validated through the identification of four interdependent BI domains:

1. Strategic Intelligence – focused on monitoring long-term political, economic, and technological trends, thereby enabling proactive adaptation (Fleisher & Bensoussan, 2015).
2. Competitive Intelligence – dedicated to market and competitor dynamics, ensuring awareness of industry shifts and rival strategies (Taillard & Mitrović, 2020).
3. Security Intelligence – designed to identify cyber threats, reputational vulnerabilities, and hybrid risks, supporting corporate resilience (Hayes & Cappa, 2018; Zuech, Khoshgoftaar, & Wald, 2015).
4. Operational Intelligence – oriented toward real-time data and decision support, reinforcing tactical agility and crisis response (Dokman & Ivanjko, 2019).

These four domains form a coherent structure that situates BI as both a monitoring and decision-support mechanism across organisational levels.

3.3. Methodological Application

The findings demonstrate the methodological value of combining established analytical frameworks with emerging digital tools. SWOT and PESTEL analyses provide structured approaches

 doi:10.20944/preprints202509.1321.v1

to strategic foresight, while foresight methodologies allow the development of alternative future scenarios (Gordon et al., 2005; Wilkinson & Kupers, 2013).

On the technical side, the use of OSINT and SOCMINT expands the scope of intelligence collection beyond traditional datasets. At the same time, Security Information and Event Management (SIEM) systems and BI dashboards offer real-time visualisation of risks and anomalies (Zuech et al., 2015). Together, these methods ensure both qualitative depth and quantitative precision in intelligence operations.

3.4. Legal and Ethical Dimensions

The study confirms that the expansion of BI functions is inseparable from legal and ethical considerations. The European Union's General Data Protection Regulation (GDPR) establishes strict boundaries on the collection and processing of personal data (Voigt & Von dem Bussche, 2017), while professional codes such as the SCIP Code of Ethics regulate competitive intelligence practices.

Furthermore, national laws on unfair competition impose legal restrictions, underscoring the need for BI systems to be both practical and compliant with these regulations. These findings highlight that institutionalised BI functions must balance analytical efficiency with normative legitimacy.

3.5. The SIDeARM Model

A central finding is the validation of the SIDeARM model (Strategic Intelligence and Decision-centric Adaptive Risk Management) as a novel framework for integrating BI into corporate governance. The model comprises six modules: environmental scanning, risk identification, adaptive analysis, decision calibration, resilience assurance, and monitoring and feedback.

Together, these modules bridge intelligence collection with strategic decision-making, ensuring that managerial processes are adaptive and forward-looking (Mitrović, 2025). The SIDeARM model thus operationalises the intelligence–strategy nexus, providing a structured pathway from data acquisition to executive decisions.

3.6. Case Studies

Case study analysis across three industries confirmed the practical value of BI and the SIDeARM framework:

- Energy sector – BI-enabled anticipation of geopolitical risks, supply-chain disruptions, and regulatory shifts, ensuring continuity of critical infrastructure.
- Pharmaceutical sector – Competitive and regulatory intelligence supported R&D prioritisation, market entry decisions, and risk mitigation in global supply networks.
- Financial sector – Integration of SIEM systems and BI dashboards enhanced detection of systemic vulnerabilities, demonstrating the link between intelligence and organisational resilience.

These cases collectively demonstrate the adaptability of BI across various industries and highlight its role in promoting long-term sustainability and informed decision-making.

4. Discussion

The findings of this study reaffirm the shifting role of Business Intelligence (BI) from a narrowly defined technical tool into a comprehensive strategic resource. Earlier perspectives often conceptualised BI as an auxiliary mechanism for data processing and reporting (Watson, 2018). However, contemporary scholarship demonstrates that BI is increasingly positioned at the core of strategic management processes (Fleisher & Bensoussan, 2015). The results presented here show that the integration of BI with decision-making structures enables organisations not merely to observe

 doi:10.20944/preprints202509.1321.v1

their environment, but to shape strategic responses proactively and to sustain competitive advantage under conditions of heightened complexity.

A key contribution of the study is the introduction of the SIDeARM model, which provides a systematic pathway for embedding intelligence within adaptive decision-making processes. By combining structured data collection, risk identification, adaptive analysis, and feedback mechanisms, SIDeARM bridges analytical precision with strategic agility (Mitrović, 2024; 2025). This alignment corresponds to calls in the literature for organisations to move beyond static intelligence functions toward more dynamic, decision-centric models of strategic management (Lowenthal, 2020; Vigfússon, Jóhannsdóttir, & Ólafsson, 2021).

The study also highlights the conceptual and practical link between BI and organisational resilience. Resilience literature emphasises the need for organisations to anticipate, absorb, and recover from disruptive events (Duchek, 2020). The SIDeARM model, by integrating foresight methodologies (Gordon et al., 2005; Wilkinson & Kupers, 2013) and real-time monitoring tools (Dokman & Ivanjko, 2019), directly contributes to building resilience capacities. Moreover, the intersection of BI with reputation management and crisis response demonstrates its value beyond technical domains, reinforcing its position as a critical driver of trust, legitimacy, and stakeholder confidence (Bozhinovska & Eftimov, 2024).

From a normative perspective, the study underscores that the contribution of BI cannot be isolated from ethical and regulatory considerations. As shown in the results, compliance with the GDPR (Voigt & Von dem Bussche, 2017) and adherence to professional codes, such as the SCIP Code of Ethics (2014), constitute integral dimensions of legitimate intelligence practice. The integration of BI into strategic management, therefore, requires balancing analytical rigour with legal accountability and ethical transparency.

The main contribution of this research lies in its integration of Business Intelligence and Strategic Management through normative, ethical, and analytical dimensions. By situating intelligence at the crossroads of corporate governance, security, and adaptive strategy, the study provides a conceptual framework that can be further developed into practical guidelines for managers, security officers, and policy-makers.

However, the study is not without limitations. As a primarily conceptual and model-driven contribution, it requires empirical validation across industries with varying levels of exposure to uncertainty, regulation, and technological transformation. While the energy, pharmaceutical, and financial sectors illustrate the model's relevance, broader cross-sectoral studies are necessary to confirm its universal applicability. Future research should therefore combine quantitative assessments with qualitative case studies to evaluate the robustness of BI frameworks and the SIDeARM model in diverse organisational settings.

5. Conclusions

The findings of this study confirm that Business Intelligence (BI) and Strategic Management form an inseparable nexus in contemporary organisational contexts. In an environment marked by uncertainty, volatility, and systemic risks, the capacity to integrate intelligence functions into strategy is no longer optional but a structural necessity. Organisations that succeed in institutionalising BI as a core component of governance and decision-making establish a decisive competitive advantage while simultaneously enhancing their resilience against both predictable and unforeseen disruptions.

A central contribution of the research is the validation of the SIDeARM model (Strategic Intelligence and Decision-centric Adaptive Risk Management) as a novel and robust framework for risk management. By linking strategic intelligence with adaptive decision-making, SIDeARM bridges the divide between abstract theoretical constructs and operational practice. Its six interdependent modules—environmental scanning, risk identification, adaptive analysis, decision calibration, resilience assurance, and monitoring and feedback—enable organisations to transform information flows into structured, risk-informed strategic choices. This framework provides not only analytical

 doi:10.20944/preprints202509.1321.v1

precision but also strategic agility, which are essential for navigating increasingly complex business landscapes.

The study also demonstrates that BI, when ethically grounded and aligned with regulatory standards such as GDPR and professional codes of conduct, extends beyond technical and analytical functions to reinforce organisational legitimacy and trust. This dimension underscores that intelligence-driven strategy must be both practical and responsible, ensuring sustainability in a broad sense—economic, social, and reputational.

Nevertheless, the analysis acknowledges certain limitations. While the conceptual framework and illustrative case studies offer strong theoretical and practical insights, further empirical validation across a broader range of industries is necessary. Future research should incorporate both qualitative and quantitative methodologies to test the adaptability and scalability of the SIDeARM model rigorously.

In conclusion, this study positions BI not as a supportive function, but as a strategic cornerstone of modern management. By institutionalising intelligence practices and embracing adaptive models such as SIDeARM, organisations can secure resilience, sustain competitiveness, and strengthen their capacity for informed decision-making in the face of an uncertain and rapidly evolving global environment.

References

Bozhinovska, T., & Eftimov, L. (2024). Boards' strategic involvement models: Past, present, and future. *Strategic Management*, 29(1), 60–70. https://doi.org/10.5937/StraMan2300060B

Dokman, T., & Ivanjko, T. (2019). Open source intelligence (OSINT): Issues and trends. In INFuture2019: Knowledge in the Digital Age (pp. 191–196). https://doi.org/10.17234/INFUTURE.2019.23

Duchek, S. (2020). Organisational resilience: A capability-based conceptualisation. *Business Research*, 13(1), 215–246. https://doi.org/10.1007/s40685-019-0085-7

Fleisher, C. S., & Bensoussan, B. E. (2015). *Business and competitive analysis: Effective application of new and classic methods*. FT Press.

Gordon, T.J., Glenn, J.C., Jakil, A. (2005). Frontiers of futures research: What's next? *Technological Forecasting and Social Change*, 72(9):1064-1069. https://doi.org/10.1016/j.techfore.2004.11.008

Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. Business Horizons, 61(5), 689–697. https://doi.org/10.1016/j.bushor.2018.02.001

ISO. (2018). ISO 31000:2018 *Risk management – Guidelines.* International Organization for Standardization. https://www.iso.org/standard/65694.html

Lowenthal, M. M. (2020). *Intelligence: From secrets to policy* (8th ed.). CQ Press.

Mitrovic, M. (2019). Strategic communication concept implemented through the corporate political activities – suggested strategy modelling. *Strategic Management*, 24(4), 13–20. https://doi.org/10.5937/StraMan1904013M

Mitrovic, M. (2025). *Innovating strategy: Artificial intelligence and the future of management*. Independently published.

SCIP. (2014). *Code of Ethics*. Strategic and Competitive Intelligence Professionals. Retrieved from https://www.scip.org/page/Ethical-Intelligence

Taillard, M., & Mitrovic, M. (2020). Evaluation of corporate success using synergistic CPA and CPR corporate citizenship. *Strategic Management*, 25(4), 24–32. https://doi.org/10.5937/StraMan2004024T

Vigfússon, K., Jóhannsdóttir, L., & Ólafsson, S. (2021). Obstacles to Strategy Implementation and Success Factors: A Review of Empirical Literature. *Strategic Management*, 26(2), 12–30. https://doi.org/10.5937/StraMan2102012V

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer. https://doi.org/10.1007/978-3-319-57959-7

Watson, H. J. (2018). The evolution of business intelligence. *MIS Quarterly Executive*, 17(2), 155–174.

 doi:10.20944/preprints202509.1321.v1

Wilkinson, A., & Kupers, R. (2013). Living in the futures. *Harvard Business Review*, 91(5), 119–127. https://hbr.org/2013/05/living-in-the-futures

Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: A survey.

Journal of Big Data, 2(3), 1–41. https://doi.org/10.1186/s40537-015-0013-4