A Unified Ontological Framework Integrating StrategicAlignment,Governance,and Information Security

Youssef El marzak[1*], *Abdelilah Chahid* [2], Sophia Faris[3] and *Khalifa Mansouri*[4]

1M2S2I Laboratory, ENSET Mohammedia Hassan II University of Casablanca Mohammedia, Morocco
2M2S2I Laboratory, ENSET Mohammedia Hassan II University of Casablanca Mohammedia, Morocco
3M2S2I Laboratory, ENSET Mohammedia Hassan II University of Casablanca Mohammedia, Morocco
4M2S2I Laboratory, ENSET Mohammedia Hassan II University of Casablanca Mohammedia, Morocco

Abstract. The increasing complexity of organizational information systems highlights the need for a holistic approach that integrates strategic alignment, govern-ance, and information security. While these domains have been extensively studied independently, their fragmented treatment often leads to inefficien-cies, inconsistencies, and misaligned priorities within organizations. This pa-per proposes a unified ontological framework that bridges these dimensions into a coherent and interoperable model. The framework leverages ontologi-cal principles to formalize concepts, relationships, and constraints, thereby ensuring semantic consistency and traceability across strategic, governance, and security layers. By integrating strategic alignment theories, governance models such as COBIT, and security standards including NIST SP 800-53 and ISO/IEC 27001, the proposed ontology provides a common ground for decision-making, risk management, and compliance. The framework was validated through expert evaluation and a case study in an IT-intensive envi-ronment, demonstrating its capacity to improve alignment between business objectives, governance practices, and security requirements. The results un-derline the framework's potential to support organizations in achieving sus-tainable performance, regulatory compliance, and resilience in the face of emerging cyber threats.

Keywords: Ontological Framework;Strategic Alignment;IT Governance;Information Security;Risk Management;COBIT;NIST SP 800-53;ISO/IEC 27001;Cybersecurity

1 Introduction

The rapid growth and increasing complexity of organizational information systems have made it increasingly challenging to ensure the alignment of business strategy, governance, and security. Strategic alignment—the fit between an organization's IT and its business strategy—has long been recognized as a crucial factor for value creation[1]. However, misalignment persists, particularly when IT governance mechanisms, security requirements, and strategic objectives are treated in isolation.

* Corresponding author: youssef.elmarzak-etu@etu.univh2c.ma

Governance frameworks such as COBIT, along with information security standards like ISO/IEC 27001 and NIST SP 800-53, provide comprehensive guidelines for managing governance and security respectively. Yet, their application often remains fragmented, leading to inefficiencies, overlapping responsibilities, and gaps in organizational processes [2], [3]. Recent studies emphasize that while IT governance mechanisms are implemented, the underlying principles, leadership commitment, and integration with security management are frequently overlooked, resulting in limited effectiveness[4] .

This paper proposes an integrated ontological framework that unifies strategic alignment, IT governance, and information security into a coherent and interoperable model. By leveraging ontological principles, the framework formalizes concepts, relationships, and constraints, ensuring semantic consistency, improved risk management, compliance, and decision-making support across organizational layers.

2 Related Work

2.1 Strategic Alignment Theories

Strategic alignment refers to the degree to which information systems (IS) and business strategies support and complement each other [5]. The Strategic Alignment Model (SAM) proposed by Henderson and Venkatraman remains one of the most influential frameworks, emphasizing coherence between business strategy, IT strategy, organizational infrastructure, and IS infrastructure. Recent studies have extended the SAM by incorporating contemporary dimensions such as IT governance and knowledge management, demonstrating their combined impact on organizational performance [6], [7]. Furthermore, researchers have underscored the role of organizational culture and shared understanding between business and IT executives as critical enablers of sustainable alignment [8]. Despite these advancements, organizations continue to face persistent challenges in maintaining long-term alignment due to rapid technological change, digital transformation, and evolving business models [9].

2.2 IT Governance Models

IT governance provides a framework for decision rights, accountability, and performance measurement in managing information systems. COBIT, developed by ISACA, is one of the most widely used governance frameworks, offering a comprehensive set of processes, principles, and metrics for IT managemen[10]. Studies have shown that COBIT facilitates alignment between IT and business goals by establishing control objectives and governance structures[11] . However, research also notes that many organizations struggle with effective adoption, particularly in integrating governance principles with operational security and risk management [12].

2.3 Security Standards

Information security standards ensure the confidentiality, integrity, and availability of organizational data. ISO/IEC 27001 defines requirements for establishing and maintaining an Information Security Management System (ISMS) [13], while NIST SP 800-53 provides a comprehensive catalog of security and privacy controls [14]. Despite their robustness, implementation often remains fragmented, creating gaps between governance, compliance,

and risk management processes [15]. Integrating these standards within a holistic ontological framework can enhance semantic consistency, interoperability, and organizational resilience.

3 Proposed Ontological Framework

This paper introduces an integrated ontological framework that unifies strategic alignment, IT governance, and information security to provide a coherent basis for decision-making, risk management, and compliance. The framework addresses the need for comprehensive information security governance by aligning policies with organizational objectives through the integration of strategy, control, and regulation [16]. It supports continuous evaluation and compliance, safeguarding organizational assets and reputation in a rapidly evolving technological context [16], [17]. Leveraging machine learning methods, ontological modeling, and expert knowledge, the framework offers a multifaceted approach to risk management [17]. It also incorporates recent advances in AI management systems, such as ISO 42001:2023, enabling oversight of emerging technologies, including Large Language Models, within existing governance structures [18].

3.1 Ontological Principles and Modeling Approach

The framework is based on foundational ontological principles to ensure **semantic clarity, consistency, and interoperability**. Key concepts were formalized using **UML class diagrams**, which were subsequently transformed into an **OWL ontology** to enable machine-readability, reasoning, and integration with other systems[19].The ontology is modular, allowing flexibility for extensions and updates in dynamic organizational environments.

3.2 Representation of Concepts, Relationships, and Constraints

The proposed ontology formalizes the core components of an integrated information security governance framework: concepts such as business objectives, IT resources, governance processes, risks, and security requirements; relationships including dependencies, alignment, ownership, and mitigation links; and constraints defined by semantic and regulatory rules. These constraints ensure traceability, compliance with mandates such as the EU AI Act, and continuous performance monitoring [18]. This structured representation ensures consistency across strategic, operational, and technical layers, addressing gaps in current cybersecurity frameworks—particularly in human oversight, validation controls, and compliance. Furthermore, it supports responsible and transparent deployment of advanced AI systems, including Large Language Models (LLMs), by identifying vulnerabilities and ethical concerns [20].

3.3 Integration of Strategy, Governance, and Security Layers

The proposed framework integrates three interdependent layers—strategic, governance, and security—to ensure adaptive and holistic information security governance. The strategic layer aligns business and IT objectives with performance indicators; the governance layer, grounded in COBIT principles, defines policies, processes, and decision structures [18]; and the security layer incorporates controls, risk assessments, and compliance elements from ISO/IEC 27001 and NIST SP 800-53 [21]. This multi-layered integration provides end-to-end visibility and coherence across assurance levels [22], promoting a unified cybersecurity

posture suited to complex, interconnected systems [23]. It also addresses emerging risks from Large Language Models (LLMs) through specialized threat modeling and continuous, hybrid risk evaluation [24], [25], supported by adaptive intelligence and behavioral analytics for real-time control adjustments [26]. As shown in Figure 1, the ontology formalizes these interrelations, ensuring that strategic decisions are consistently guided by governance mechanisms and security imperatives [27], [17].

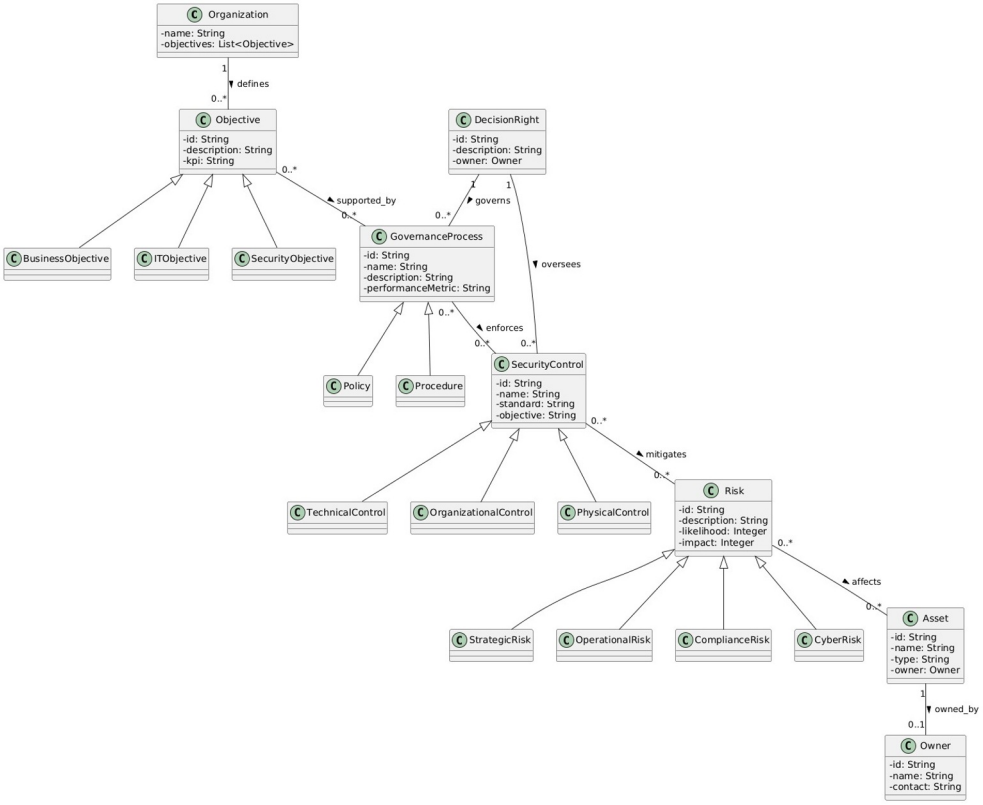

Fig. 1. Class diagram of the proposed ontology

The proposed ontology's class diagram was converted into RDF, exported in Turtle format, and validated via the W3C RDF validator to ensure compliance, quality, and interoperability. This process enabled the detection and correction of syntax and semantic inconsistencies, confirming the ontology's structural and semantic integrity for cybersecurity applications [19], [28]. The validation reinforces semantic interoperability, essential for integrating heterogeneous cybersecurity resources and achieving a unified threat perspective [29]. The RDF/XML representation Figure 2 enhances compatibility with Semantic Web technologies, enabling advanced reasoning and automated security verification through SPARQL, OWL, and SWRL [30].

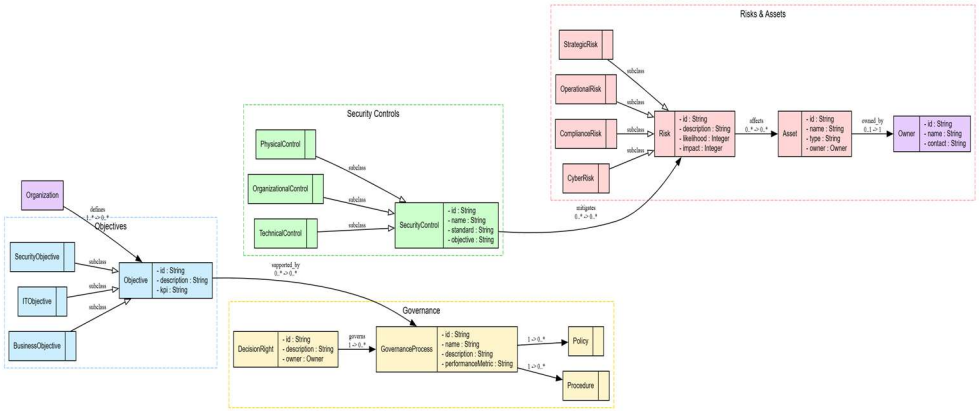

Fig. 2. Ontology of Risk Management Concepts including Governance, Objectives, Controls, and Risks

4 Results and Discussion

The ontology's class diagram was transformed into RDF, exported in Turtle format, and validated using the W3C RDF validator to ensure conformity and interoperability. This formal validation corrected syntax and semantic errors, confirming structural integrity and RDF compliance [19], [28]. Ensuring semantic interoperability supports the integration of heterogeneous cybersecurity resources and provides a unified threat perspective [29]. The RDF/XML model (Figure 2) extends the ontology's applicability, enabling reasoning and automated verification through SPARQL, OWL, and SWRL [30].

4.1 Alignment of Business, Governance, and Security

The ontology established clear traceability between business objectives, governance processes, and security controls, ensuring that security measures are strategically aligned with organizational goals and regulatory mandates [32]. This integration enhances resource allocation efficiency, linking security investments to measurable business value and compliance outcomes [33]. It also mitigates misalignments between strategic intent and IT security practices, providing managers with improved visibility and decision support.

4.2 B. Contributions to Risk Management

Risks were systematically associated with impacted assets and corresponding security controls, enhancing assessment accuracy and mitigation effectiveness through the ontology's semantic structure. The framework supports risk prioritization and accountability clarification, though broader empirical validation is required to assess its applicability across varied organizational contexts [17], [28]. Future research should address automation of ontology population and maintenance to ensure adaptability to evolving threats, positioning this model as a foundation for dynamic cybersecurity knowledge graph development [30].

4.3 Compliance and Resilience

Integration with ISO/IEC 27001 and NIST SP 800-53 enhanced regulatory compliance. The semantic framework allowed for mapping specific cloud security controls to these standards, thereby streamlining the implementation and maintenance of security measures [28].
Proactive identification of potential vulnerabilities improved organizational resilience. This comprehensive approach fosters a dynamic security posture that can adapt to emerging threats and regulatory changes, ultimately strengthening the organization's overall security assurance and trustworthiness [34] [28].
Future work could include quantitative metrics and longitudinal studies to better demonstrate measurable benefits.

4.4 Originality and Future Enhancements

The framework uniquely integrates strategic alignment, governance, and security into a coherent ontological model. Further enhancements will focus on extending its capabilities to incorporate real-time threat intelligence and automated policy enforcement, thereby transitioning towards a more adaptive and proactive security posture.
Its originality lies in the semantic representation and traceability across all layers, which is not commonly addressed in existing approaches. Future research could therefore focus on refining the ontology to include a broader spectrum of cyber threats and vulnerabilities, alongside an expanded set of control mechanisms to further bolster its comprehensiveness and practical applicability [35].
To reinforce its impact, empirical validation on multiple organizations, automation for real-time reasoning, and comparative evaluation with existing frameworks are recommended. The inclusion of an assurance context model is also essential for conducting effective and relevant system security assurance evaluations, ensuring that evaluations align with unique organizational requirements and objectives [34].

5 Conclusion and Future Work

The paper introduces an integrated ontological framework that unifies strategic objectives, IT governance, and information security to enhance organizational alignment and resilience. Expert evaluation and a case study confirmed its benefits in visibility, risk management, and regulatory compliance. Future work will focus on large-scale empirical validation, automation for real-time risk detection, comparative analysis with existing standards, and the integration of quantitative performance metrics. Overall, the framework establishes a strong foundation for advancing research and practice in governance, strategic alignment, and cybersecurity management.

References

1. Akbar, K. A., Rahman, F. I., Singhal, A., Khan, L., & Thuraisingham, B. (2023). The Design and Application of a Unified Ontology for Cyber Security. In Lecture notes in computer science (p. 23). Springer Science+Business Media.
2. AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers & Security, 99, 102030.
3. Alomari, Z., Wong, W., Lee, S., & Satti, M. I. (2024). Knowledge Graph to Facilitate Cloud SecurityCompliance with NIST Cybersecurity Framework. Research Square (Research Square).

4. Amara, O. B., Nicola, A. D., Kamissoko, D., & Benaben, F. (2022). Towards an Ontological Approach to Business Continuity Assessment. In Communications in computer and information science (p. 322). Springer Science+Business Media.
5. Antariksa, M. D. S., Angin, M. P., & Widodo, A. P. (2025). COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and Benefits Across Various Industry Sectors. Journal of Renewable Energy Electrical and Computer Engineering, 5(1), 99
6. Barbhuiya, I. A., Laroiya, S., & Singh, R. (2024). Holistic Cybersecurity Risk Management Framework. SSRN Electronic Journal.
7. Barlybayev, A., Sharipbay, A., Shakhmetova, G., & Zhumadillayeva, A. (2024). Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies. Applied Sciences, 14(21), 9858. https://doi.org/10.3390/app14219858
8. Bonar, J. R., & Hastings, J. D. (2024). Transforming Information Systems Management: A Reference Model for Digital Engineering Integration. arXiv (Cornell University).
9. Dairo, M., Adekola, J., Apostolopoulos, C., & Tsaramirsis, G. (2021). Benchmarking strategic alignment of business and IT strategies: opportunities, risks, challenges and solutions. International Journal of Information Technology, 13(6), 2191.
10. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 4(2), 92.
11. Faizi, S. M., & Rahman, S. M. (2019). Securing Cloud Computing Through IT Governance. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3360869
12. Fenz, S., & Neubauer, T. (2018). Ontology-based information security compliance determination and control selection on the example of ISO 27002. Information and Computer Security, 26(5), 551.
13. Gerek, Y., & Aydın, M. N. (2025). Management Frameworks and Management System Standards in the Context of Integration and Unification: A Review and Classification of Core Building Blocks for Consilience [Review of Management Frameworks and Management System Standards in the Context of Integration and Unification: A Review and Classification of Core Building Blocks for Consilience]. Systems, 13(4), 234. Multidisciplinary Digital Publishing Institute.
14. Haes, S. D., Grembergen, W. V., & Debreceny, R. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal of Information Systems, 27(1), 307
15. Ko, D., & Fink, D. (2010). Information technology governance: an evaluation of the theory-practice gap. Corporate Governance, 10(5), 662.
16. Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2020). Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective. IEEE Transactions on Engineering Management, 69(6), 3757.
17. Martins, B. F., Gil, L. J. S., Reyes, J. F., Panach, J. I., Pastor, Ó., & Rochwerger, B. (2020). Conceptual Characterization of Cybersecurity Ontologies. In Lecture notes in business information processing (p. 323). Springer Science+Business Media.
18. McIntosh, T. R., Liu, T., Sušnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. Computers & Security, 134, 103424.

19. McIntosh, T. R., Sušnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. Computers & Security, 144, 103964.
20. Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. Journal of Cybersecurity and Privacy, 3(3), 327.
21. Meriah, I., & Rabai, L. B. A. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards. Procedia Computer Science, 160, 85.
22. Narayanan, sundaraparipurnan, & Vishwakarma, S. K. (2024). GUARD-D-LLM: An LLM-Based Risk Assessment Engine for the Downstream uses of LLMs. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2406.11851
23. Nguyen, T. N. (2024). Ollabench: Evaluating LLMs' Reasoning for Human-centric Interdependent Cybersecurity. arXiv (Cornell University).
24. Orakzai, T. (2014). COBIT, ITIL and ISO 27002 Alignment for Information Security Governance in Modern Organisations. SSRN Electronic Journal.
25. Proceedings of the 19th Conference on Computer Science and Intelligence Systems (FedCSIS). (2024). Annals of Computer Science and Information Systems, 39.
26. Ross, R. S., Katzke, S., Johnson, L. A., Swanson, M., Stoneburner, G., & Rogers, G. O. (2006). Recommended security controls for federal information systems and organizations.
27. Sánchez-Zas, C., Villagrá, V. A., Vega-Barbas, M., Larriva-Novo, X., Moreno, J. I., & Berrocal, J. (2022). Ontology-based approach to real-time risk management and cyber-situational awareness. Future Generation Computer Systems, 141, 462.
28. Security and Privacy Controls for Federal Information Systems and Organizations. (2013).
29. Shariffuddin, N., & Mohamed, A. (2020). IT Security and IT Governance Alignment.
30. Sieber, M. R., Malý, M., & Liška, R. (2022). Conceptualizing organizational culture and business-IT alignment: a systematic literature review. SN Business & Economics, 2(9).
31. Slim, A. M., Sarah, O. S., Kadhim, K. G., Ali, B. J., Hammood, A. M., & Othman, B. (2020). he effect of information technology business alignment factors on performance of SMEs. Management Science Letters, 833. https://doi.org/10.5267/j.msl.2020.10.019
32. Tete, S. B. (2024). Threat Modelling and Risk Analysis for Large Language Model (LLM)-Powered Applications. arXiv (Cornell University).
33. Ullah, A., & Lai, R. (2013). A Systematic Review of Business and Information Technology Alignment [Review of A Systematic Review of Business and Information Technology Alignment]. ACM Transactions on Management Information Systems, 4(1), 1. Association for Computing Machinery. https://doi.org/10.1145/2445560.2445564
34. Wen, S.-F., & Katt, B. (2023). Exploring the role of assurance context in system security assurance evaluation: a conceptual model. Information and Computer Security, 32(2), 159
35. Zhang, J., Bu, H., Wen, H., Liu, Y., Fei, H., Xi, R., Li, L., Yang, Y., Zhu, H., & Meng, D. (2025). When LLMs meet cybersecurity: a systematic literature review. Cybersecurity, 8(1).