Developing a Unified Cyber Risk Management Framework Using Semantic Technologies and Structured Modeling Approaches

Youssef El Marzak
M2S2I Laboratory, ENSET Mohammedia, Hassan II University of Casablanca, Mohammedia, Morocco
youssef.elmarzak-etu@etu.univh2c.ma (corresponding author)

Abdelilah Chahid
M2S2I Laboratory, ENSET Mohammedia, Hassan II University of Casablanca, Mohammedia, Morocco
chahidabdelillah@gmail.com

Sophia Faris
M2S2I Laboratory, ENSET Mohammedia, Hassan II University of Casablanca, Mohammedia, Morocco
sophiafaris1989@gmail.com

Khalifa Mansouri
M2S2I Laboratory, ENSET Mohammedia, Hassan II University of Casablanca, Mohammedia, Morocco
khalifa.mansouri@enset-media.ac.ma

Received: 6 August 2025 | Revised: 11 September 2025, 5 October 2025, 14 October 2025, and 19 October 2025 | Accepted: 21 October 2025

 DOI: https://doi.org/10.48084/etasr.13844

ABSTRACT

Cybersecurity knowledge is often fragmented across heterogeneous ontologies and standards, limiting consistent and interoperable risk management. This study proposes a unified hybrid ontology by integrating ISO/IEC 27005 and the National Institute of Standards and Technology Special Publication 800-30 (NIST SP 800-30), selected for their complementary approaches to risk identification, assessment, and treatment. A Unified Modeling Language (UML) metamodel was designed, translated into the Resource Description Framework (RDF), enriched with Web Ontology Language (OWL) rules, and validated using the World Wide Web Consortium (W3C) RDF Validator. The resulting ontology (~200 RDF triples) achieved full syntactic conformity after resolving seven detected inconsistencies. Unlike previous static models, the framework reacts dynamically to real-time security events: when a vulnerability is reported, it is linked to affected assets and threats, triggering automatic risk recalculation and activation of treatment plans (avoidance, transfer, mitigation, or acceptance). Monitored by Key Performance Indicators (KPIs), the system ensures proactive, adaptive, and continuously aligned risk management, while remaining extensible to additional frameworks such as the Center for Internet Security (CIS) Controls and Control Objectives for Information and Related Technologies (COBIT).

Keywords-W3C RDF; cyber risk management; ISO/IEC 27005; NIST SP 800-30

I. INTRODUCTION

Software security is a particularly complex domain; ontologies based on knowledge representation and semantic technologies offer a structured means of managing its multiple facets [1]. These formal frameworks enable IT and security specialists to organize, share, and apply knowledge that is often scattered across projects heavily dependent on their context [2]. However, the current landscape consists of a patchwork of ontologies, each addressing a specific portion of the broader security field, without any systematic comparison of their respective contributions currently available in the literature [3]. This study, therefore, seeks to improve the accessibility and relevance of knowledge in software security by conducting a comparative evaluation of existing ontologies. Beyond merely compiling an inventory, the analysis identifies their strengths and limitations, proposes avenues for improvement, and emphasizes the importance of reliable and contextualized decision-making in an ever-evolving informational environment [4]. Specifically, this study enhances the effectiveness and usability of the reviewed ontologies through a rigorous evaluation framework [5]. The selected models, identified after an extensive review to ensure

representativeness [6], are evaluated for their ability to (i) simplify complex security data, (ii) contextualize knowledge according to project requirements, and (iii) promote interoperability across heterogeneous standards [7]. By comparing these approaches, the current study highlights their areas of excellence and aspects needing improvement, paving the way for the design of a more flexible, interoperable, and coherent hybrid ontology.

Information security is essential for all organizations [8]. Its effectiveness relies on integrated security practices, collectively applied to detect vulnerabilities, deploy defenses, and manage incidents [9]. Regulated sectors (such as finance, healthcare, government, and critical infrastructure) rely on dedicated standards [10] that establish a preventive approach to threats [11]. By combining assessments, policies, procedures, and a security-oriented culture, these standards reduce vulnerabilities and strengthen resilience [12], thus ensuring consistent protection of operations despite an ever-evolving regulatory and threat environment [13]. ISO/IEC 27001 defines a system for managing information security that focuses on the confidentiality, integrity, and availability of sensitive data [14, 15]. It establishes a structured approach: risk assessment to identify vulnerabilities and threats, selection of technical and organizational protective measures, and regular monitoring to maintain the resilience of information assets. Its framework remains voluntary and adaptable; it is suitable for both small businesses and multinational corporations, provided that its documentation requirements, internal audits, and continuous improvement logic are systematically applied [16,17].

The NIST Cybersecurity Framework, developed by the U.S. National Institute of Standards and Technology, offers a flexible reference model for managing cyber risk [18]. It covers five functions: identify, protect, detect, respond, and recover, and can be adapted to each organization's priorities, budget constraints, and maturity level, without prescribing specific technical solutions [19]. This flexibility enables the alignment of security objectives with overall strategy while ensuring preparedness, prevention, and post-incident recovery. The Center for Internet Security (CIS) Controls, published by the Center for Internet Security, comprises twenty-eight best practices organized into three tiers: basic, foundational, and organizational [20]. The basic controls focus on asset inventory and management, continuous vulnerability assessment, and privilege restriction. The foundational controls strengthen secure configuration, email and browser protection, and data backup [21]. Finally, the organizational controls cover risk management, staff awareness, training, and continuous monitoring. Their clear structure and gradual applicability make them an effective tool across various sectors and company sizes [21].

Table I compares three significant information security standards and frameworks: ISO/IEC 27001, the NIST Cybersecurity Framework, and CIS Controls. It summarizes their contributions, highlights areas where practical implementation details may be constrained, and suggests options for further study and development. Recent studies reveal an ongoing fragmentation in the field of security ontologies. These models often differ widely in terms of structure, scope, and expressiveness. Such inconsistencies make it increasingly difficult to align them effectively, thereby limiting their practical use in real-world applications, which emphasizes that there is no systematic framework available to facilitate the comparison of these diverse ontologies, resulting in overlapping definitions that still fail to form a complete conceptual picture [22]. In a similar vein, it is observed that many current ontologies fall short in capturing the complex, multi-layered nature of software security [23]. Moreover, they often struggle to support interoperability across varying environments. Together, these shortcomings point to a critical gap: the urgent need for a unified and thoroughly validated hybrid ontology that can provide a solid, reliable base for advancing software security practices.

II. METHODOLOGY: STANDARDS-INTEGRATED ONTOLOGY ENGINEERING

To build an ontology that unifies multiple information security frameworks, an organized pathway was followed, which starts with selecting complementary standards: ISO/IEC 27005, valued for its structured international scope, and National Institute of Standards and Technology Special Publication 800-30 (NIST SP 800-30), known for detailed risk-assessment guidance. Combining them yields a hybrid approach that draws on each framework's strengths, fitting our operational context of the study; the CIS Controls was added later to refine the model further.

TABLE I. COMPARATIVE ANALYSIS OF ISO/IEC 27001, NIST CYBERSECURITY FRAMEWORK, AND CIS CONTROLS

Aspect	ISO/IEC 27001	NIST Cybersecurity Framework	CIS Controls
What was achieved	Provides a thorough framework with a significant emphasis on risk assessment for information security management systems (ISMS) [16, 26]	Offers a methodical strategy for identification, defense, detection, response, and recovery [18]	Creates a list of tasks that are ranked in order of importance to strengthen the cybersecurity posture of an organization [27].
Contribution	Provides comprehensive principles for security measures, risk assessment, and ongoing development [17].	Establishes a voluntary framework with worldwide acceptance that is applicable to varied sectors [19].	Provides realistic and accessible controls that are relevant to a wide range of enterprises [28].
What was not achieved	There is a lack of attention to actual implementation details and particular technological controls [24].	Due to its non-mandatory nature, it may result in unequal adoption across organizations [26].	Simplicity may not sufficiently handle advanced risks or encompass the peculiarities of certain organizations [25].
What aspects need to be improved?	More study is needed on achievable ISO/IEC 27001 control implementation methodologies.	More comprehensive technical assistance within the NIST framework is required for uniform adoption.	Development of additional controls or changes to meet the demands of businesses with intricate security requirements is encouraged.

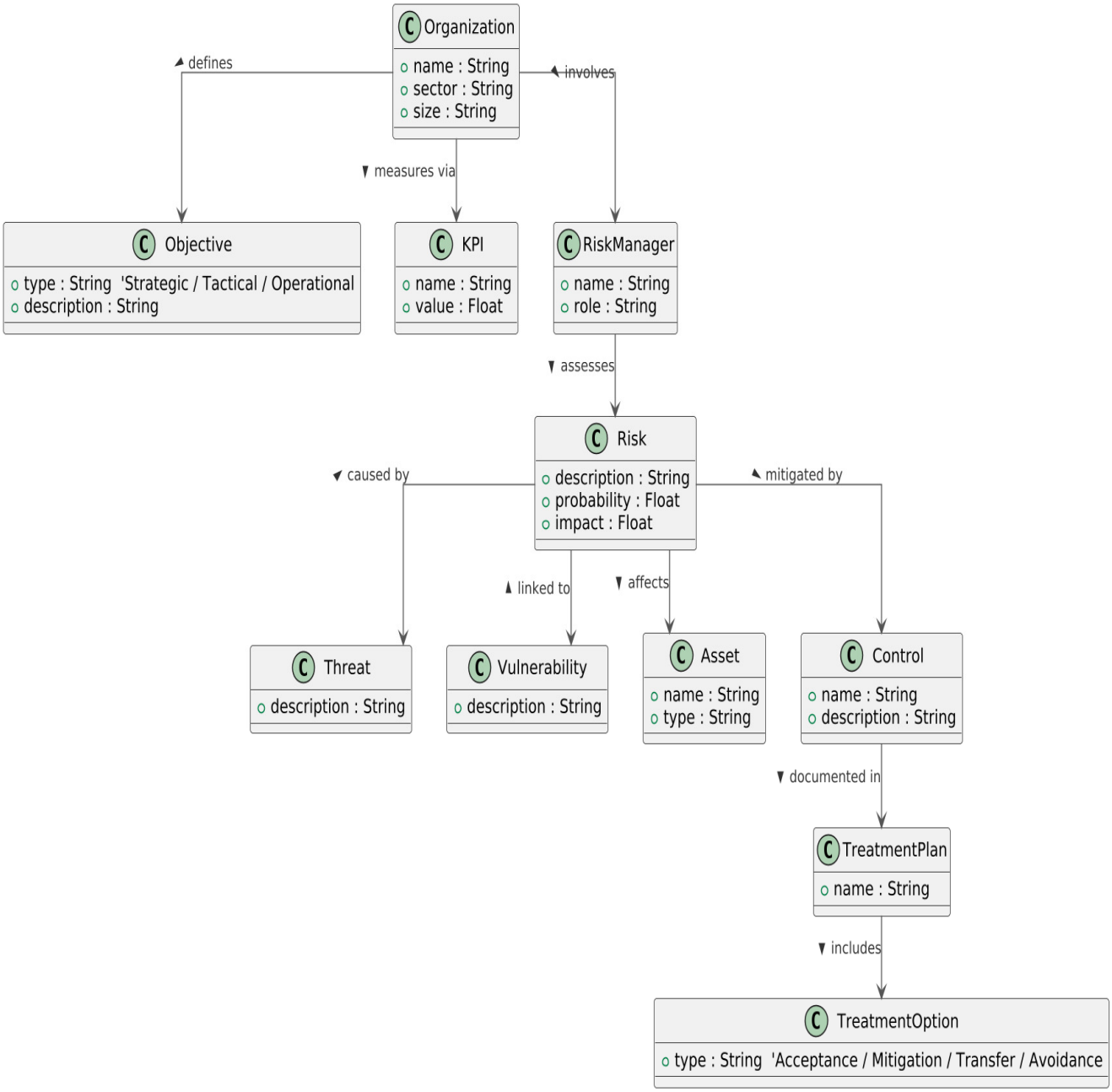

Fig. 1. UML Class Diagram for the Proposed ISO/IEC 27005 Risk Management Process.

Technically, concepts were first mapped in Unified Modeling Language (UML), then implemented with semantic-web tools: data were encoded in Resource Description Framework (RDF), relationships enriched in Web Ontology Language (OWL), and syntax verified using the World Wide Web Consortium (W3C) RDF Validator. This toolchain ensures the ontology remains coherent, adaptable, and extensible, making it easier to merge diverse viewpoints within the information-security domain.

III. CREATING THE HYBRID ONTOLOGY

A hybrid cybersecurity ontology combines different frameworks to unify assets, risks, threats, and controls within a structured model. It can react in real-time: when a vulnerability is reported, it automatically links it to the affected assets, reassesses the risk, and proposes appropriate measures. By integrating multiple data sources, it supports automated analysis, facilitating the identification of security gaps and missing controls. This flexible and adaptive approach strengthens organizational cybersecurity strategy.

A. ISO/IEC 27005 Risk Management Process Proposed Metamodel

The ISO/IEC 27005 standard offers a structured risk management approach by linking assets, threats, vulnerabilities, and treatments in a continuous process. The proposed metamodel depicts the organization through actors who manage security events, apply controls, and track key indicators aligned with strategic objectives. Risk is modeled by combining likelihood and impact, while treatment plans select appropriate responses: avoidance, transfer, mitigation, or acceptance, each tied to specific controls. Class relationships and stereotypes (e.g., <<actor>>, <<Abstract>>) clarify the model structure [29], as visualized in the UML diagram in Figure 1, embedded within the ISMS.

B. NIST SP 800-30 Risk Assessment Proposed Metamodel

The NIST SP 800-30 risk assessment metamodel begins by mapping assets, the threats that could harm them, and the vulnerabilities that expose them; each risk is then quantified by analyzing the likelihood of a threat exploiting a vulnerability and the resulting impact [30]. The model's core classes reflect this process: Asset (id, name, owner), Threat, Vulnerability, and Risk, all interconnected through a RiskAssessment object that compiles data across assets, threats, and vulnerabilities. Mitigation options (avoid, transfer, mitigate, and accept) are defined in Control Selection and assigned to an owner, while the objective class ensures treatments remain aligned with business goals. Continuous risk communication keeps stakeholders informed, and ongoing monitoring detects changes in exposure so that controls can be updated promptly [31]. The UML diagram shown in Figure 2 visualizes these relationships, illustrating how systematic assessment and targeted controls support informed decision-making and strengthen the organization's overall cybersecurity posture.

C. Proposed Hybrid UML Metamodel Integrating ISO/IEC 27005 and NIST SP 800-30 Frameworks

Table II presents key entities of ISO/IEC 27005 and NIST SP 800-30, presenting a hybrid UML metamodel that combines their strengths. The metamodel includes common entities such as risk, threat, vulnerability, asset, control, owner, and stakeholder, as well as specific entities from each standard, such as risk assessment, control plan, risk treatment, and risk communication. Integrating these elements into a single metamodel can provide a comprehensive risk management framework leveraging the strengths of both standards. e.g., a customer data server (asset) exposed to ransomware attacks (threat) is protected by strong encryption (control) defined in a risk treatment plan compliant with the hybrid metamodel. The Perspectives column offers insight into how each entity is regarded and evaluated in the risk management process.

TABLE II. KEY ENTITIES AND INTEGRATION IN THE HYBRID UML METAMODEL OF ISO/IEC 27005 AND NIST SP 800-30

Entity	ISO/IEC 27005	NIST SP 800-30	Perspectives
Asset	Information Asset	Information/System	Asset Value to the organization, criticality
Threat	Threat Source	Threat Source	Potential impact, likelihood of occurrence
Vulnerability	Vulnerability	Vulnerability	Weaknesses, exposure to threats
Risk	Risk	Risk	A combination of threat, vulnerability, and impact
Risk Assessment	Risk Assessment	Risk Assessment	Process of identifying and evaluating risks
Risk Treatment Plan	Risk Treatment Plan	Risk Response Plan	Strategies for risk mitigation, acceptance, or transfer
Communication	Communication and Consultation	Risk Communication	Involvement of stakeholders, transparency
Owner	Asset Owner	Asset/System Owner	Responsibility for the asset or system
Stakeholder	Interested Party	Stakeholder	Influence, interest, or impact on risk decisions
Control	Control Measure	Security Control	Measures to reduce or manage risk
Review	Risk Monitoring and Review	Risk Monitoring	Continuous evaluation of risk and effectiveness of controls

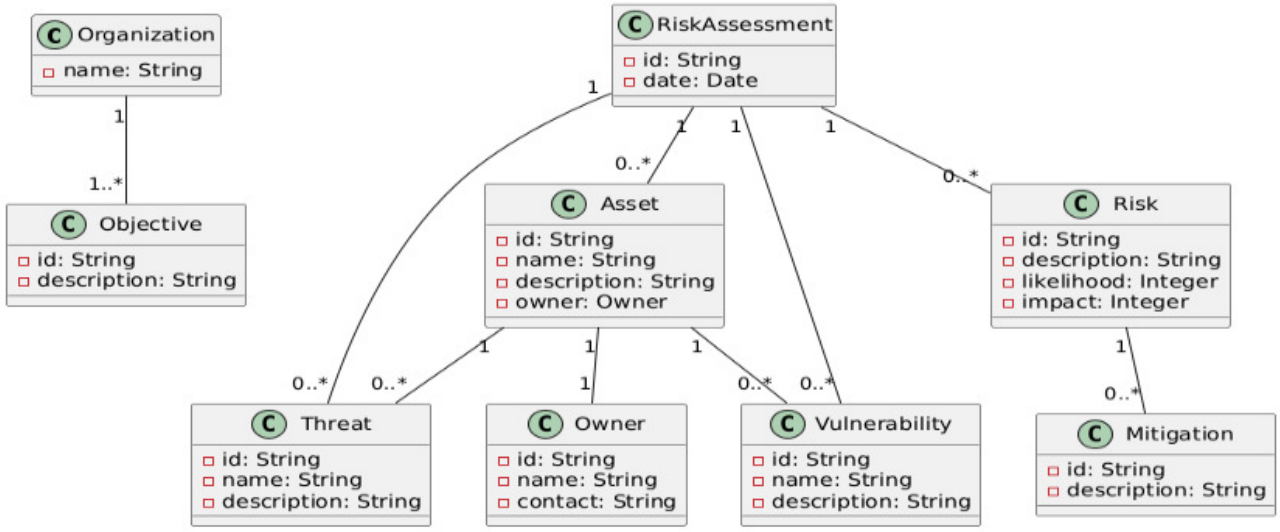

Fig. 2. UML class diagram for the proposed NIST SP 800-30 risk assessment metamodel.

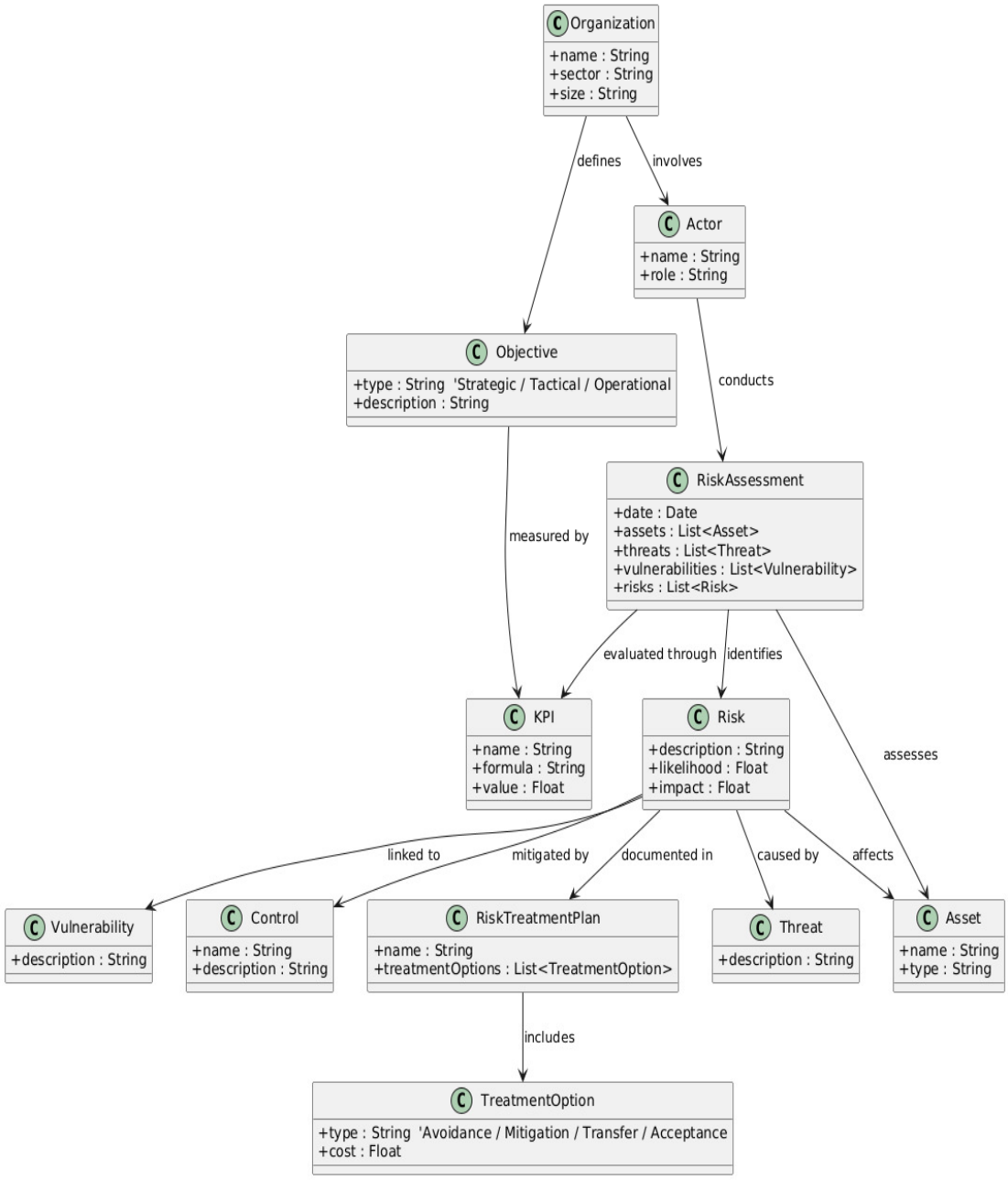

Fig. 3. Hybrid UML metamodel integrating ISO/IEC 27005 and NIST SP 800-30 framework.

This metamodel serves as a foundation for creating risk management processes that adhere to standards and may be customized to suit an organization's specific requirements. The focus is on integrating ISO/IEC 27005 and NIST SP 800-30 into a single UML class diagram, as shown in Figure 3. This diagram demonstrates the representation and interconnection of important components and processes in information security risk management. The hybrid metamodel provides a clear representation of both the systematic approach and specific guidance offered by these standards, demonstrating their contribution to an organization's ISMS. This visual representation facilitates comprehension of the organized yet flexible framework for controlling cybersecurity threats.

The application of the integration method of ISO/IEC 27005 and NIST SP 800-30 standards into a UML metamodel has led to several significant outcomes. First, the resulting metamodel facilitates the harmonization of concepts by reducing terminological redundancies and semantic ambiguities between the two standards. Second, it enables better traceability between threats, vulnerabilities, and treatment measures, thanks to the explicit formalization of relationships within the UML class diagram. Unlike prior works such as [32, 33], which propose risk ontologies without aligning with

ISO/IEC or NIST standards, our model integrates both frameworks into a formal RDF/OWL structure. Authors in [4] focused on scenario modeling but did not cover the full risk lifecycle or standard compliance. This study offers a unified, standards-based, and machine-readable ontology for enhanced risk traceability and automation. The hybrid metamodel, integrating ISO/IEC 27005 and NIST SP 800-30, was converted into an RDF representation, where all entities and relationships were organized into triples to facilitate interoperability and automated cybersecurity analysis. Validation with the W3C RDF Validator was performed on ~200 triples and three thematic modules (Asset–Threat–Vulnerability, Risk–Likelihood–Impact, Treatment–Control), ensuring well-formed syntax, correct prefixes, IRI compliance, and valid lexical values. Seven initial inconsistencies (four prefix errors, two datatype mismatches, one incorrect Control–Asset relation) were corrected, after which the ontology achieved full syntactic conformity, as shown in Figure 4. This robust RDF implementation guarantees compatibility for future extensions and supports dynamic behaviour. As seen in Figure 5, when a vulnerability is reported, it is linked to affected assets and threats, risks are recalculated, and risk treatment plans (avoidance, transfer, mitigation, acceptance) are triggered and monitored through key performance indicators (KPIs). The system thus ensures proactive, real-time, and continuously aligned risk management. Table III presents a segment on future advancements, highlighting the use of advanced technologies and approaches to improve the adaptability and effectiveness of the model.

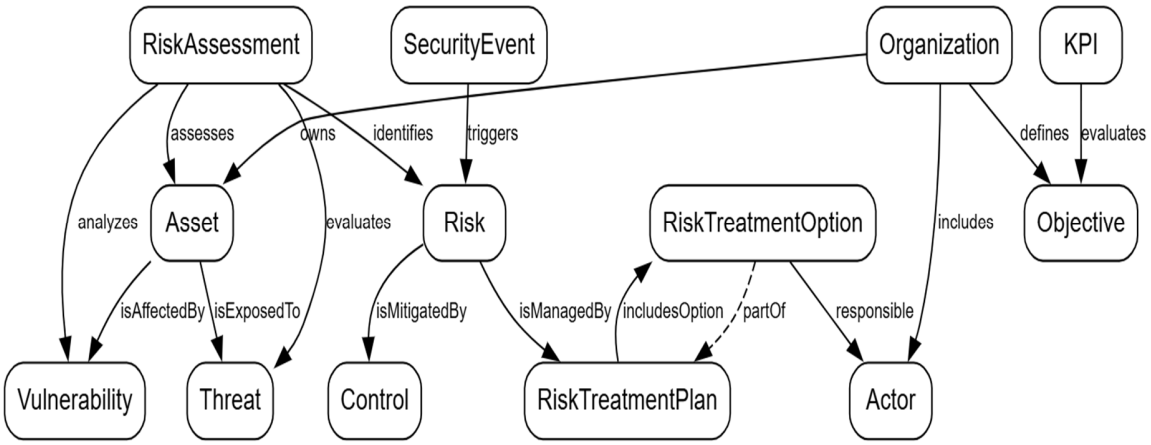

Fig. 4. RDF Graph Model for the proposed hybrid UML metamodel integrating ISO/IEC 27005 and NIST SP 800-30 framework.

TABLE III. OUTLINE OF THE RDF METAMODEL INTEGRATING ISO/IEC 27005 AND NIST SP 800-30 FRAMEWORKS

Aspect	Summary and Outlook
Key Entities	The RDF metamodel encompasses several entities, including Asset, Threat, Vulnerability, Risk, Risk Assessment, Risk Treatment Plan, Risk Communication, Control, Owner, and Stakeholder. It conforms to both ISO/IEC 27005 and NIST SP 800-30 standards.
Strengths	Comprehensive Framework: Encompasses fundamental aspects of risk management outlined in both ISO/IEC 27005 and NIST SP 800-30, offering a comprehensive perspective on risk assessment and mitigation.
	Explicit Relationships: Establishes connections between entities (e.g., Asset is susceptible to Threat, Risk may be reduced by Control), hence improving comprehension of risk dynamics and management procedures.
	The integration of standards involves incorporating components from ISO/IEC 27005 and NIST SP 800-30. This enables a cohesive approach to risk management that aligns with global best practices.
Areas for Improvement	Detail and Granularity: It may be beneficial to include more intricate features and attributes for each entity in order to effectively encompass certain risk situations and management mechanisms.
	Dynamic Risk Management: Requires methods to continually update and adjust to emerging risks, vulnerabilities, and controls, ensuring that the model stays applicable and up-to-date.
	Enhancing stakeholder engagement by improving the portrayal of stakeholder roles and their interactions in risk communication and decision-making might make the model more applicable.
	Future Work: Additional efforts should prioritize the integration of automated tools and procedures to continuously analyze and respond to risks, including sophisticated analytics, and improve compatibility with other risk management systems.
Practical Applications	Risk Assessment and Management: Offers a systematic method for identifying, evaluating, and controlling risks in accordance with ISO/IEC 27005 and NIST SP 800-30 standards.
	Security Planning and Implementation: Assists in formulating and executing efficient strategies to address and mitigate risks by developing customized plans and controls based on identified threats and vulnerabilities.
	Compliance and Integration: Assists organizations in meeting compliance requirements and integrating risk management.

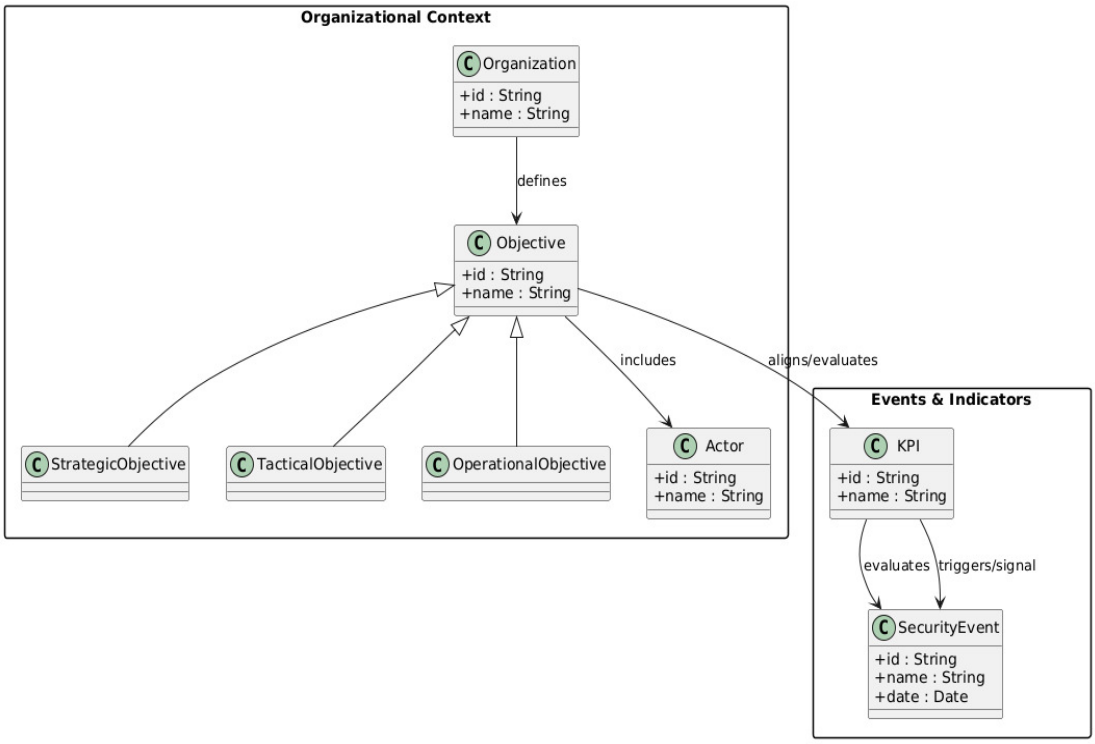

Fig. 5. Hybrid UML metamodel integrating ISO/IEC 27005 and NIST SP 800-30 for dynamic risk management (part 1).

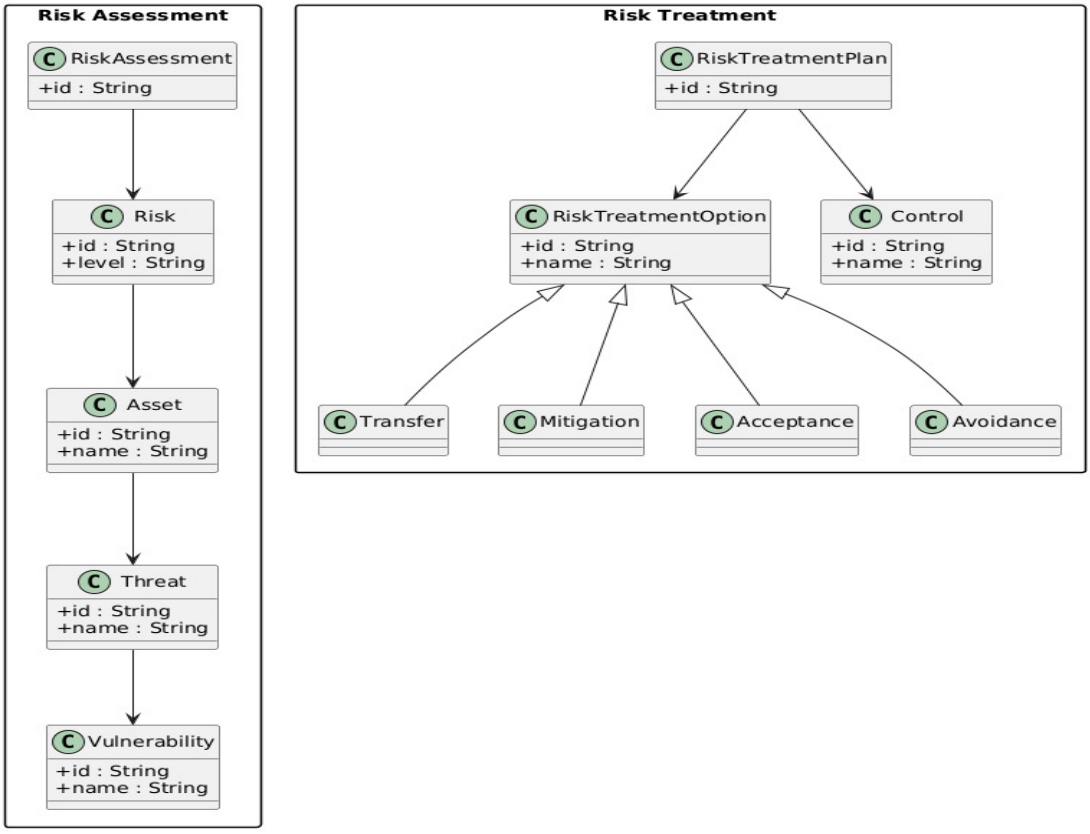

Fig. 6. Hybrid UML metamodel integrating ISO/IEC 27005 and NIST SP 800-30 for dynamic risk management (part 2).

IV. CONCLUSION AND FUTURE WORK

This study presents a strategic effort to merge the ISO/IEC 27005 and National Institute of Standards and Technology Special Publication 800-30 (NIST SP 800-30) frameworks into a unified, semantically rich ontology. By employing a validated Resource Description Framework (RDF) model, the study crafts a cohesive architecture that intricately links key cybersecurity components: assets, threats, vulnerabilities, and safeguards. The result is a system that supports traceability and automated reasoning and simplifies compliance across various regulatory standards, cutting down on administrative burdens. More than just a technical consolidation, the unified ontology acts as a shared repository of knowledge. It elevates risk assessment capabilities, shapes more effective mitigation strategies, and reinforces essential governance functions such as auditing and strategic planning. Thanks to its semantic interoperability, the model integrates effortlessly with current IT systems and compliance platforms, removing the need for labor-intensive data alignment or custom-built connectors. Future work could include complementary frameworks such as the Center for Internet Security (CIS) Controls and Control Objectives for Information and Related Technologies (COBIT) to broaden the framework's applicability. The study also advocates for enhanced automation, such as RDF-powered dashboards and semantic queries that could streamline reporting and real-time alerts. With practical applications in fields such as finance and healthcare on the horizon, this study marks a step forward in crafting intelligent, machine-actionable cybersecurity models that adhere to standards while empowering informed decision-making.

REFERENCES

[1] S. R. Mashwani and S. Khusro, "The Design and Development of a Semantic File System Ontology," *Engineering, Technology & Applied Science Research*, vol. 8, no. 2, pp. 2827–2833, Apr. 2018, https://doi.org/10.48084/etasr.1898.

[2] M. A. Ullah and S. A. Hossain, "Ontology-Based Information Retrieval System for University: Methods and Reasoning," in *Emerging Technologies in Data Mining and Information Security*, vol. 814, A. Abraham, P. Dutta, J. K. Mandal, A. Bhattacharya, and S. Dutta, Eds. Singapore: Springer Singapore, 2019, pp. 119–128.

[3] M. Alenezi, H. A. Basit, F. I. Khan, and M. A. Beg, "A Comparison Study of Available Software Security Ontologies," in *Proceedings of the Evaluation and Assessment in Software Engineering*, Trondheim Norway, Apr. 2020, pp. 499–504, https://doi.org/10.1145/3383219.3383292.

[4] S.-F. Wen, M. M. Yamin, and B. Katt, "Ontology-Based Scenario Modeling for Cyber Security Exercise," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria, Sept. 2021, pp. 249–258, https://doi.org/10.1109/EuroSPW54576.2021.00032.

[5] T. E. Abioye, O. T. Arogundade, S. Misra, A. T. Akinwale, and O. J. Adeniran, "Toward Ontology-based Risk Management Framework for Software Projects: An Empirical Study," *Journal of Software: Evolution and Process*, vol. 32, no. 12, Dec. 2020, Art. no. e2269, https://doi.org/10.1002/smr.2269.

[6] S. F. Wen, "Context-Based Support to Enhance Developers' Learning of Software Security," *Education Sciences*, vol. 13, no. 7, Jun. 2023, Art. no. 631, https://doi.org/10.3390/educsci13070631.

[7] B. Amini, R. Ibrahim, M. S. Othman, and M. A. Nematbakhsh, "A Reference Ontology for Profiling Scholar's Background Knowledge in Recommender Systems," *Expert Systems with Applications*, vol. 42, no. 2, pp. 913–928, Feb. 2015, https://doi.org/10.1016/j.eswa.2014.08.031.

[8] A. Sattar, E. Salwana, M. Nazir, M. Ahmad, and A. Kamil, "Comparative Analysis of Methodologies for Domain Ontology Development: A Systematic Review," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 5, 2020, https://doi.org/10.14569/IJACSA.2020.0110515.

[9] D. Wu, J. Dong, Y. Tang, and R. Capra, "Understanding Task Preparation and Resumption Behaviors in Cross-device Search," *Journal of the Association for Information Science and Technology*, vol. 71, no. 8, pp. 887–901, Aug. 2020, https://doi.org/10.1002/asi.24307.

[10] E. Humphreys, "Information Security Management Standards: Compliance, Governance and Risk Management," *Information Security Technical Report*, vol. 13, no. 4, pp. 247–255, Nov. 2008, https://doi.org/10.1016/j.istr.2008.10.010.

[11] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of Cybersecurity Standard and Framework Components," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 12, no. 3, Apr. 2022, https://doi.org/10.17762/ijcnis.v12i3.4817.

[12] F. Ullah, S. Qayyum, M. J. Thaheem, F. Al-Turjman, and S. M. E. Sepasgozar, "Risk Management in Sustainable Smart Cities Governance: A TOE Framework," *Technological Forecasting and Social Change*, vol. 167, Jun. 2021, Art. no. 120743, https://doi.org/10.1016/j.techfore.2021.120743.

[13] C. J. Ashley and M. Preiksaitis, "Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises," *Business Management Research and Applications: A Cross-Disciplinary Journal*, vol. 1, no. 2, pp. 109–157, 2022.

[14] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," *Sustainability*, vol. 15, no. 7, Mar. 2023, Art. no. 5828, https://doi.org/10.3390/su15075828.

[15] M. Suorsa and P. Helo, "Information Security Failures Identified and Measured – ISO/IEC 27001:2013 Controls Ranked based on GDPR Penalty Case Analysis," *Information Security Journal: A Global Perspective*, vol. 33, no. 3, pp. 285–306, May 2024, https://doi.org/10.1080/19393555.2023.2270984.

[16] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis, and V. Stantchev, "A Process Framework for Information Security Management," *International Journal of Information Systems and Project Management*, vol. 4, no. 4, pp. 27–47, 2016, https://doi.org/10.12821/ijispm040402.

[17] M. Podrecca, G. Culot, G. Nassimbeni, and M. Sartor, "Information Security and Value Creation: The Performance Implications of ISO/IEC 27001," *Computers in Industry*, vol. 142, Nov. 2022, Art. no. 103744, https://doi.org/10.1016/j.compind.2022.103744.

[18] N. Lungu *et al.*, "NIST CSF-2.0 Compliant GPU Shader Execution," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15187–15193, Aug. 2024, https://doi.org/10.48084/etasr.7351.

[19] A. D. Khaleefah, and H. M. Al-Mashhadi, "Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review," *International Journal of Wireless and Microwave Technologies*, vol. 13, no. 1, pp. 1–13, Feb. 2023, https://doi.org/10.5815/ijwmt.2023.01.01.

[20] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," in *2020 Resilience Week (RWS)*, Salt Lake City, ID, USA, Oct. 2020, pp. 106–112, https://doi.org/10.1109/RWS50334.2020.9241271.

[21] S. Gros, "A Critical View on CIS Controls," in *2021 16th International Conference on Telecommunications (ConTEL)*, Zagreb, Croatia, Jun. 2021, pp. 122–128, https://doi.org/10.23919/ConTEL52528.2021.9495982.

[22] M. Adach, K. Hänninen, and K. Lundqvist, "Security Ontologies: A Systematic Literature Review," in *Enterprise Design, Operations, and Computing*, vol. 13585, J. P. A. Almeida, D. Karastoyanova, G. Guizzardi, M. Montali, F. M. Maggi, and C. M. Fonseca, Eds. Cham, Switzerland: Springer International Publishing, 2022, pp. 36–53.

[23] A. K. Mishra, N. C. Debnath, and A. Patel, "Evaluating Richness of Security Ontologies for Semantic Web," in *Data Science with Semantic*

Technologies, 1st ed., A. Patel, N. C. Debnath, and B. Bhusan, Eds. Hoboken, NJ, USA: Wiley, 2022, pp. 277–297.

[24] L. Hertteli, "Improving IT Administration Security by Using Security Controls Based on Security Frameworks," Master's thesis, JAMK University of Applied Sciences, Jyväskylä, Finland, 2022.

[25] R. S. Alves, J. P. B. D. Silva, L. A. Ribeiro Junior, and R. R. Nunes, "Enhancing cybersecurity in the judiciary: Integrating additional controls into the CIS framework," *Computers & Security*, vol. 157, Oct. 2025, Art. no. 104584, https://doi.org/10.1016/j.cose.2025.104584.

[26] A. Alshammari, "A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11445–11450, Aug. 2023, https://doi.org/10.48084/etasr.6091.

[27] B. Shamma, "Implementing CIS Critical Security Controls for Organizations on a Low-Budget," M. S. Thesis, University of Houston College of Technology, Houston, TX, USA, 2018.

[28] R. Sasidharan, "A Case Study to Implement Windows System Hardening using CIS Controls," *International Journal of Computer Trends and Technology*, vol. 70, no. 7, pp. 1–7, July 2022, https://doi.org/10.14445/22312803/IJCTT-V70I7P101.

[29] L. Moudoubah, A. El Yamami, K. Mansouri, and M. Qbadou, "From IT service management to IT service governance: An ontological approach for integrated use of ITIL and COBIT frameworks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, Dec. 2021, Art. no. 5292, https://doi.org/10.11591/ijece.v11i6.pp5292-5300.

[30] "Validation service," *W3C RDF Validation Service*, 2006. https://www.w3.org/RDF/Validator/.

[31] M. A. Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency," *Procedia Computer Science*, vol. 161, pp. 1206–1215, 2019, https://doi.org/10.1016/j.procs.2019.11.234.

[32] C. Sánchez-Zas, V. A. Villagrá, M. Vega-Barbas, X. Larriva-Novo, J. I. Moreno, and J. Berrocal, "Ontology-based Approach to Real-time Risk Management and Cyber-situational Awareness," *Future Generation Computer Systems*, vol. 141, pp. 462–472, Apr. 2023, https://doi.org/10.1016/j.future.2022.12.006.

[33] Í. Oliveira, T. P. Sales, J. P. A. Almeida, R. Baratella, M. Fumagalli, and G. Guizzardi, "Ontology-based security modeling in ArchiMate," *Software and Systems Modeling*, vol. 23, no. 4, pp. 925–952, Aug. 2024, https://doi.org/10.1007/s10270-024-01149-1.