Enhancing a NIST SP 800-53-Based Cybersecurity Risk Metamodel with COBIT 2019: A Governance-Centric Perspective

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: 22 December 2025 | Revised: 26 January 2026 and 7 February 2026 | Accepted: 13 February 2026

 DOI: https://doi.org/10.48084/etasr.17097

ABSTRACT

As cybersecurity threats continue to increase in complexity and impact, organizations face challenges in aligning technical security controls with enterprise governance objectives. This paper represents a continuation of prior work on cybersecurity metamodeling and ontological integration. An enhanced hybrid cybersecurity risk metamodel is proposed, which integrates the Control Objectives for Information and Related Technologies (COBIT) 2019 governance framework into an existing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53–based structure. The proposed model combines governance objectives, organizational design factors, and performance indicators with technical security controls using Unified Modeling Language (UML) class diagrams, the Resource Description Framework (RDF), and Web Ontology Language (OWL) ontologies to ensure semantic consistency and end-to-end traceability. Design factors enable contextual adaptability by influencing the selection and prioritization of governance objectives and security controls according to organizational and regulatory environments. In addition, performance indicators establish monitoring and feedback loops that support continuous performance evaluation and dynamic risk management. Future work will focus on empirical validation and the integration of quantitative risk assessment approaches such as Factor Analysis of Information Risk (FAIR).

Keywords-cybersecurity; risk management; governance; NIST SP 800-53; COBIT 2019; UML; RDF/OWL; metamodel

I. INTRODUCTION

Cybersecurity threats continue to increase in frequency, scale, and sophistication, exposing organizations to significant risks affecting assets, operations, and strategic objectives. Consequently, organizations must not only deploy effective technical security controls but also ensure that cybersecurity initiatives are aligned with enterprise governance and value creation goals. Traditional cybersecurity risk management approaches, such as those defined in NIST SP 800-53 Revision 5, mainly focus on the identification and implementation of technical and operational controls [1]. While effective at the operational level, these approaches often provide limited support for aligning cybersecurity decisions with strategic business priorities. Enterprise governance of information and technology is significant for ensuring that cybersecurity investments contribute to organizational objectives, risk optimization, and regulatory compliance [2]. COBIT 2019 addresses this challenge by offering governance and management objectives, performance measurement

mechanisms, and contextual design factors. However, it lacks the technical granularity required for detailed security control implementation compared to NIST SP 800-53 [3]. This gap underscores the need for an integrated approach that combines the technical rigor of NIST SP 800-53 with the governance-oriented capabilities of COBIT 2019. Thus, the present study proposes an ontological integration framework that aligns information system governance with technical cybersecurity controls. The main contribution of this research lies in introducing a formal integration mechanism between COBIT 2019 governance objectives and NIST SP 800-53 controls using UML modeling and semantic formalization through RDF and OWL. The proposed approach incorporates design factors to enable context-aware control selection and prioritization based on organizational characteristics, regulatory constraints, and risk appetite. In addition, a performance-driven governance loop is established through the integration of Key Performance Indicators (KPIs) and Key Goal Indicators (KGIs), ensuring continuous feedback between operational control effectiveness and strategic objectives. Building on previous work, which introduced a NIST SP 800-53–based cybersecurity metamodel [4] and a governance-oriented ontological framework for strategic alignment [5], the current study presents a hybrid governance–control metamodel that formally integrates COBIT 2019 and NIST SP 800-53 through explicit bidirectional mappings. By providing semantic interoperability, end-to-end traceability, and performance-driven feedback, the proposed model bridges top-down governance objectives with bottom-up technical implementation.

II. BACKGROUND AND MATERIALS

A. Data Sources and Reference Frameworks

Table I presents the main datasets, normative frameworks, and ontological standards used as reference sources for the design and implementation of the proposed metamodel.

B. NIST SP 800-53 Revision 5

NIST SP 800-53 Revision 5 provides a comprehensive catalog of security and privacy controls organized into twenty control families. It is widely adopted across federal agencies, critical infrastructures, and private-sector organizations [1]. The framework emphasizes control selection, tailoring, and implementation based on organizational risk profiles and impact levels. While highly detailed and technically robust, NIST SP 800-53 primarily supports operational risk mitigation and compliance, offering limited native mechanisms for enterprise governance alignment [6].

TABLE I. REFERENCE DATASETS, STANDARDS, AND FRAMEWORKS USED FOR METAMODEL DESIGN

Catalog / framework	Source	Official URLS	Access conditions	Format
NIST SP 800-53 Rev. 5	NIST	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final	Publicly available	PDF, XML, JSON
COBIT 2019 Framework	Information Systems Audit and Control Association (ISACA)	https://www.isaca.org/	Documentation requires ISACA membership	PDF, online
RDF Schema (RDFS)	World Wide Web Consortium (W3C)	https://www.w3.org/TR/rdf-schema/	Open standard	RDF/XML, Turtle
OWL 2	World Wide Web Consortium (W3C)	https://www.w3.org/TR/owl2-overview/	Open standard	RDF/XML, OWL/XML
SPARQL 1.1 Query Language	World Wide Web Consortium (W3C)	https://www.w3.org/TR/sparql11-overview/	Open standard	Text

TABLE II. COMPARISON OF NIST SP 800-53 AND COBIT 2019 FRAMEWORKS ACROSS KEY CRITERIA

Criteria	NIST SP 800-53	COBIT 2019
Primary objective	Technical and privacy risk management [9, 10]	Enterprise governance of information and technology [11]
Scope of application	U.S. federal agencies, critical sectors [1, 12], and increasingly across various industries [9]	All types of organizations, regardless of size or industry [13, 14]
Structure	Catalog security and privacy controls into 20 control families by functional domain [6, 10]	Comprises 40 core governance and management objectives grouped into five domains [13, 14]
Approach	Control-based, focused on tactical and technical implementation [9]	Goal-driven, incorporating design factors and strategic customization [15, 16]
Granularity level	Highly detailed control requirements [10]	Higher-level, strategic objectives adaptable to organizational context [16]
Performance measurement	Based on control compliance and auditability; lacks integrated performance metrics [10]	Integrates KPIs/KGIs and capability levels for maturity and performance monitoring [7]
Governance integration	Minimal native governance linkage; requires external alignment [17]	Native governance layer via EDM and APO domains [15, 18]
Interoperability	Strong – aligns with ISO/IEC 27001, RMF, FISMA, etc. [6]	Designed for compatibility with other frameworks [19]
Target users	Security analysts, technical teams, compliance auditors [6]	Executives, IT managers, governance professionals [20]

C. COBIT 2019

COBIT 2019 is a comprehensive framework for the enterprise governance and management of information and technology [7]. It defines 40 governance and management objectives organized into 5 domains: Evaluate, Direct and Monitor (EDM); Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA) [8]. COBIT 2019 adopts a goal-driven approach that integrates design factors, capability levels, and performance metrics to support strategic alignment and continuous improvement.

D. Comparative Analysis of NIST SP 800-53 and COBIT 2019

Table II presents a comparison of NIST SP 800-53 and COBIT 2019 across key criteria, highlighting their complementary technical and governance orientations.

III. RESEARCH METHODOLOGY

This study adopts a Design Science Research (DSR) methodology, building upon an existing cybersecurity risk metamodel derived from NIST SP 800-53 [4]. The methodological framework is structured into 4 phases:

- Phase I: Analysis of the existing metamodel to identify structural limitations.
- Phase II: Extension of the model through the integration of COBIT 2019 governance constructs and identification of relevant integration points.
- Phase III: Formalization of the resulting hybrid metamodel using UML class diagrams and RDF/OWL-based semantic modeling.
- Phase IV: To ensure semantic consistency, logical coherence, and practical applicability of the proposed ontology and conduct a comprehensive validation using industry standard tools and methodologies.

IV. THE PROPOSED HYBRID METAMODEL

A. Integration of COBIT 2019 into the NIST SP 800-53–Based Metamodel

The proposed metamodel integrates COBIT 2019 governance principles into an existing NIST SP 800-53–based structure to enable explicit alignment between strategic objectives and technical controls. The integration of COBIT 2019 into the proposed metamodel has been a significant element of prior work [4], in which key governance components from COBIT 2019, including governance objectives, processes (e.g., APO12 (Managed Risk) and EDM03 (Ensured Risk Optimisation), and design factors, were meticulously mapped to the structural and behavioral elements of an existing NIST SP 800-53–based metamodel. This initial integration was aimed at establishing clear traceability between high-level governance intent and specific technical implementation controls, thereby supporting alignment with enterprise objectives and regulatory requirements. The present research systematically extends this foundation by further refining semantic consistency, introducing dynamic adaptability mechanisms, and formalizing the resultant hybrid model through advanced ontological and model-driven engineering techniques.

B. UML Classes and Relationships

The metamodel is extended with new UML classes—GovernanceObjective, GovernanceProcess, DesignFactor, and PerformanceIndicator—to integrate COBIT 2019 principles by capturing governance objectives, decision-making processes, contextual design factors, and performance metrics for evaluating both technical controls and governance effectiveness. Figure 1 illustrates the UML class diagram of the proposed hybrid metamodel, integrating COBIT 2019 governance constructs with NIST SP 800-53 security and privacy controls. This integration aims to ensure traceability between strategic governance objectives, operational processes, technical controls, and performance measurement.

The metamodel is organized around several core classes. The GovernanceObjective class represents COBIT governance and management objectives (e.g., EDM03, APO13), characterized by identifiers, descriptions, and domains. These objectives are operationalized through the GovernanceProcess class, which models COBIT processes and associates them with organizational actors using RACI relationships to explicitly define roles and responsibilities. The contextual adaptation is supported by the DesignFactor class, which captures elements such as regulatory environment, organizational size, industry sector, risk appetite, and technology maturity. These factors influence both governance processes and control selection.

The Control class represents NIST SP 800-53 security and privacy controls, defined by attributes such as control identifier, family, baseline, and implementation guidance. Controls are linked to the risk class, which models threats and vulnerabilities affecting organizational assets, including information systems, data, and infrastructure components. Performance monitoring is addressed through the PerformanceIndicator class, which includes KPIs and KGIs used to evaluate governance effectiveness and control performance. Key relationships within the metamodel ensure end-to-end traceability. Governance objectives are linked to controls through the ImplementedBy relationship, design factors influence processes and controls via Influences, performance indicators support continuous evaluation through Monitors, and accountability is established using the ExecutedBy relationship.

An illustrative traceability example is: EDM03 → APO12 → RA-5 → risk assessment → vulnerability scan results, demonstrating the alignment between governance objectives, technical controls, and measurable outcomes. Figure 2 shows the block diagram of the proposed hybrid model, emphasizing the iterative alignment between governance objectives, control implementation, and performance-driven improvement. Figure 3 depicts the equivalent semantic schema of Figure 1, namely the RDF/OWL graph model of the proposed cybersecurity governance ontology. Figure 4 illustrates the system architecture diagram of the proposed hybrid ontological model, highlighting its layered structure and the interactions between governance objectives, technical controls, and semantic processing components. Figure 5 displays the classes that constitute the proposed ontology, while Figure 6 presents the relationships between the ObjectProperty classes.

C. Mapping Between COBIT and NIST

A crucial aspect of this integration involves linking each instance of a GovernanceObjective to one or more Control instances derived from NIST SP 800-53. This mapping is supported by contemporary research and mapping studies focused on aligning strategic governance intent with practical technical implementation [4, 6, 21]. For example, the COBIT governance process APO13 is directly associated with specific NIST SP 800-53 controls, such as AC-2 and CA-7, enabling traceability from high-level objectives to tactical measures [21].

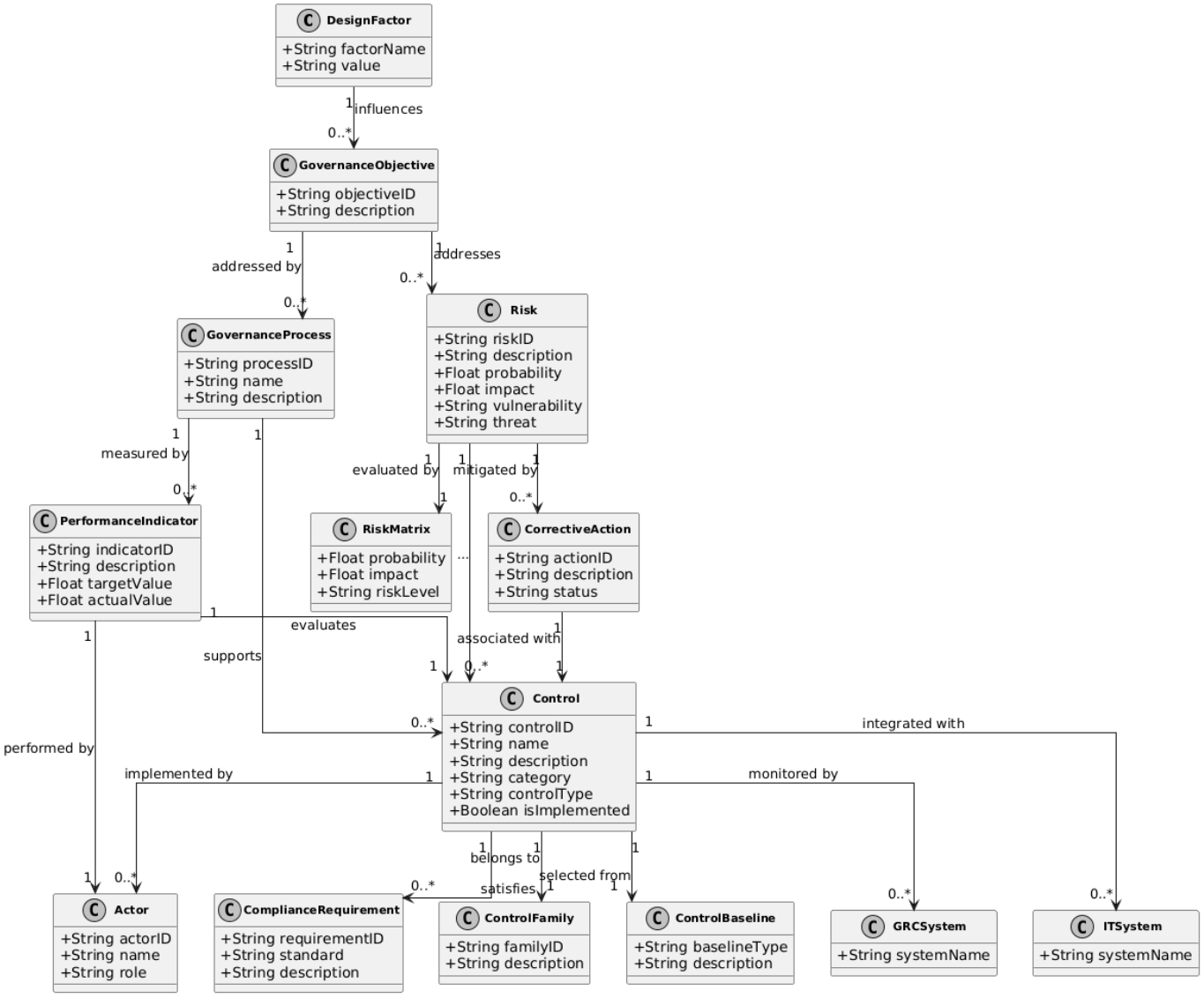

Fig. 1. UML Class diagram integrating COBIT 2019 elements into the NIST SP 800-53-based metamodel.

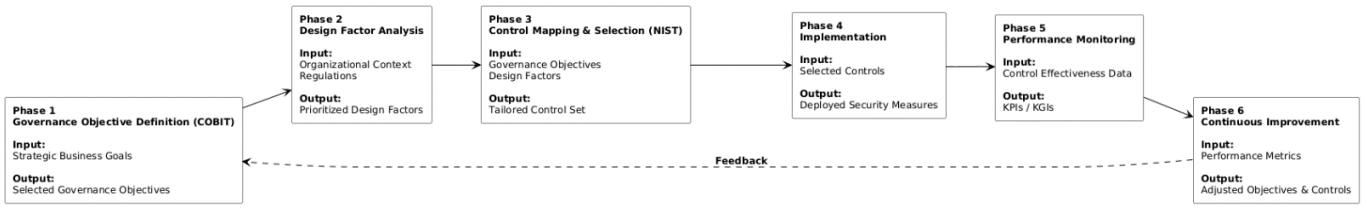

Fig. 2. Block diagram of the integrated COBIT–NIST governance and security process.

Furthermore, GovernanceProcess instances are linked to actor classes, representing key roles, such as the Chief Information Security Officer, Compliance Officer, or Risk Manager, who bear responsibility for executing and overseeing these processes in alignment with COBIT's RACI matrices [11, 20]. This explicit linkage ensures accountability and operationalizes the governance framework, making it actionable within the enterprise [15]. These connections are further reinforced by the integration of DesignFactor instances, which contextually modify how GovernanceProcesses are implemented and how PerformanceIndicators are interpreted, thereby ensuring that the hybrid metamodel remains adaptive to diverse organizational environments [15].

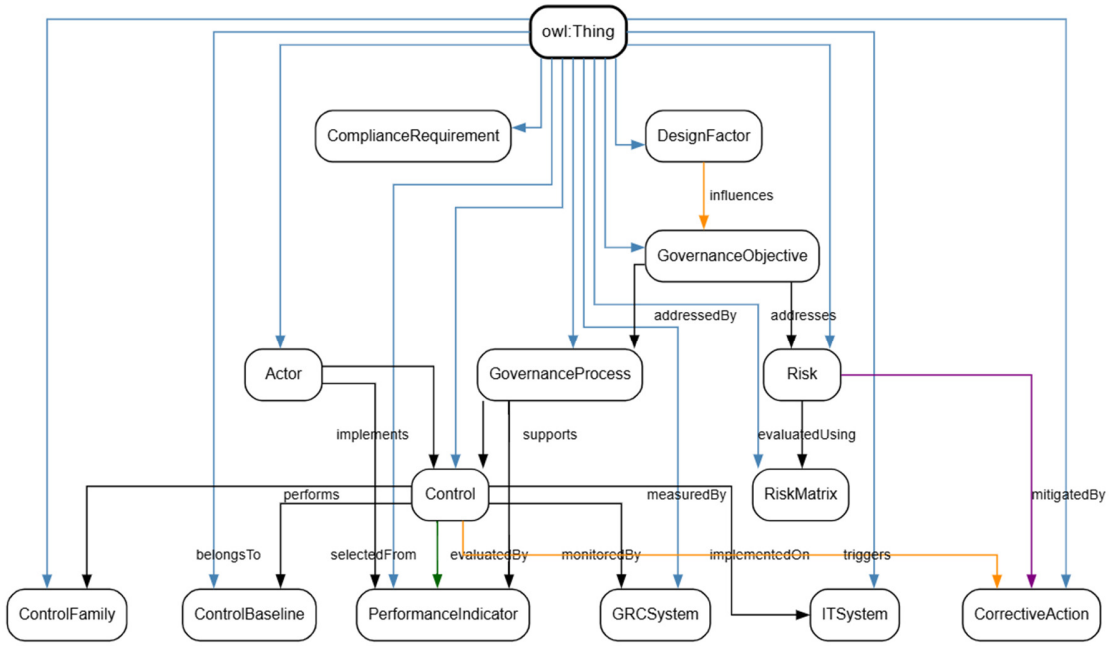

Fig. 3. RDF/OWL graph model for the proposed cybersecurity governance ontology.

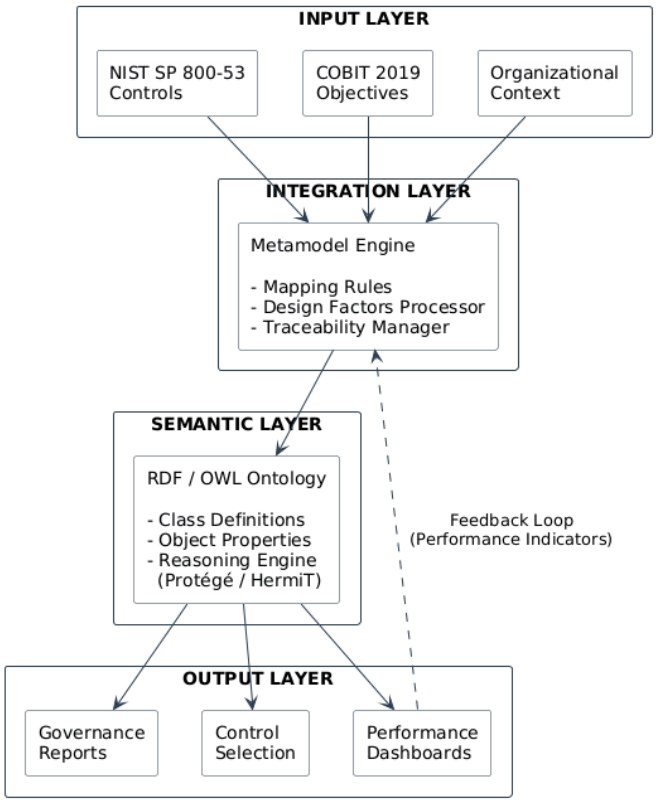

Fig. 4. System architecture diagram of the proposed hybrid ontological model.

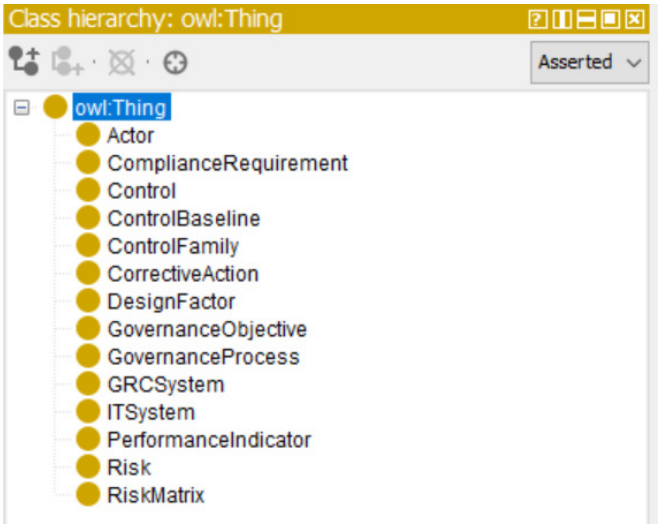

Fig. 5. Hierarchy of classes of the proposed ontology.

D. Adaptability via Design Factors

The DesignFactor class is significant in enabling the metamodel's inherent adaptability. By capturing organizational context, these factors influence the selection and prioritization of relevant governance objectives and technical controls. For example, an organization operating within a highly regulated sector, such as healthcare or finance, may prioritize GovernanceObjectives explicitly linked to rigorous compliance enforcement, thus necessitating a greater emphasis on specific NIST controls that directly support these stringent regulatory requirements.

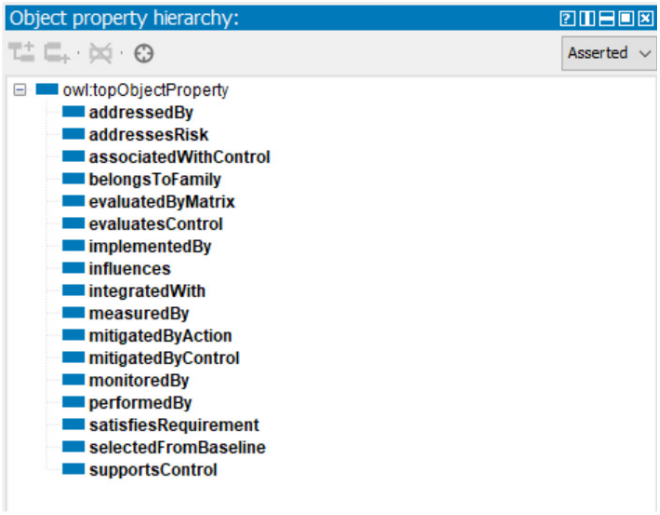

Fig. 6. Relationships between ObjectProperty classes in the proposed ontology.

E. Monitoring and Feedback Loops

The PerformanceIndicator class establishes crucial monitoring capabilities by associating directly with GovernanceObjective, control, and risk elements. This interconnectedness enables end-to-end traceability, spanning from strategic planning through to operational outcomes. Such robust feedback loops contribute to supporting continuous improvement, facilitating comprehensive performance evaluation, and enabling dynamic, responsive risk management strategies.

F. Implementation and Validation

The proposed ontology was validated for logical consistency and semantic coherence using Protégé 5.6.1 with OWL 2 description logic. Reasoning with HermiT confirmed class satisfiability and the absence of logical inconsistencies. Six SPARQL 1.1 competency questions verified governance-to-control traceability, design factor influence, and performance monitoring. Inference testing and performance evaluation demonstrated effective automated reasoning with acceptable response times.

V. DISCUSSION

The proposed metamodel addresses key shortcomings noted in prior studies by delivering a structured, governance-informed synthesis of technical controls and enterprise objectives, particularly those evident in disjointed framework alignments that lack semantic interoperability [4, 6, 21]. In contrast to conventional document-centric methodologies, the model augments traceability, adaptability, and performance oversight through its formalized UML and RDF/OWL representations, thereby enabling automated inference and evidence-driven decision processes [15]. Nonetheless, its efficacy depends on organizational governance maturity alongside access to dependable performance metrics [11, 20]. Moreover, effective implementation of this framework requires understanding the organization's operational context and strategic priorities [15, 21].

TABLE III. EXAMPLES OF COBIT 2019 AND NIST SP 800-53 ALIGNMENT AND TRACEABILITY

COBIT 2019 objective	NIST SP 800-53 controls	Justification	Traceability mechanism	Design factor influence
EDM03 – Ensure risk optimization	RA-1, RA-5, CA-2	Enterprise-wide risk visibility and remediation	EDM03 → APO12 → RA-* via risk assessment	Regulatory pressure increases RA-5 frequency
APO12 – Manage risk	RA-3, RA-7, PM-9	Risk assessment and continuous monitoring	APO12 → RA-3 via ERM processes	Risk tolerance shapes RA-3 methodology
APO13 – Manage security	AC-1, AC-2, SC-7	Core security control implementation	APO13 → DSS05 → AC-* via operations	Organization size affects AC-2 complexity
BAI09 – Manage assets	CM-8, PM-5	Asset and configuration control	BAI09 → DSS01 → CM-8 lifecycle	Industry sector determines CM-8 granularity
DSS05 – Manage security services	IR-4, AU-6, CP-2	Incident response and security operations	DSS05 → IR-4 via IR processes	Risk appetite affects IR-4 response time
MEA01 – Monitor performance	CA-7, AU-11	Continuous control effectiveness monitoring	MEA01 → CA-7 continuous monitoring	Compliance drives CA-7 scope
EDM01 – Ensure governance framework	PM-1, PL-1	Governance structure and policies	EDM01 → PM-1 policy framework	Governance maturity defines PM-1 detail

Table III further illustrates the alignment between enterprise governance objectives and technical cybersecurity controls by providing representative mappings between COBIT 2019 objectives and NIST SP 800-53 controls. This mapping demonstrates how high-level governance goals, such as risk optimization, security management, and performance monitoring, can be systematically operationalized through concrete control selection, thereby reinforcing the traceability and governance-driven nature of the proposed metamodel. However, this mapping is illustrative rather than exhaustive and may require contextual adaptation based on organizational characteristics, regulatory constraints, and governance maturity.

VI. CONCLUSION

This study introduced a governance-oriented cybersecurity risk metamodel that integrates Control Objectives for Information and Related Technologies (COBIT) 2019 governance principles into a National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53–based structure, bridging the gap between high-level enterprise governance objectives and detailed technical security controls.

By explicitly linking governance intent to operational implementation, the proposed metamodel provides a structured and semantically coherent approach to integrated cybersecurity governance. This integration enables organizations to better align cybersecurity investments with business objectives while enhancing traceability, adaptability, and performance monitoring capabilities. Unlike traditional document-centric or loosely coupled framework mappings, the proposed approach formalizes relationships between governance objectives, risks, controls, and performance indicators within a unified modeling framework. This governance-aware integration supports continuous monitoring and evidence-based decision-making, contributing to a more resilient and strategically aligned cybersecurity posture. Future work will focus on empirically validating the proposed metamodel across diverse organizational contexts and industry sectors to assess its practical applicability and effectiveness. Additional research directions include the integration of quantitative risk assessment methods, such as the Factor Analysis of Information Risk (FAIR) model, as well as the development of automated reasoning, compliance validation, and governance decision-support tools based on the underlying ontology.

REFERENCES

[1] D. Innomesanghan, E. Kiwamu, S. Butakov, and E. G. AbdAllah, "Streamlining Security: Mapping NIST SP 800-53, SOC 2, and US CJIS Policy to ISO/IEC 27001:2022 for Service Provider SMEs," presented at the 11th World Congress on Electrical Engineering and Computer Systems and Science, Paris, France, Aug. 2025, https://doi.org/10.11159/cist25.112.

[2] H. Alzaabi, "Strategic Cyber-Risk Alignment: A New Framework for Financial Institutions Facing the Digital Future." Research Square (Pre-Print), Apr. 30, 2025, https://doi.org/10.21203/rs.3.rs-6560364/v1.

[3] M. Fadya and D. N. Utama, "Towards Secure Information Systems: Developing and Implementing an Information Security Evaluation Model Using NIST CSF and COBIT 2019," *TEM Journal*, pp. 182–191, Feb. 2025, https://doi.org/10.18421/TEM141-17.

[4] Y. El Marzak, K. Mansouri, and S. Faris, "A Comprehensive Metamodel for Cybersecurity: Based on NIST SP 800-53 Revision 5 Security and Privacy Controls," in *Innovative Technologies on Electrical Power Systems for Smart Cities Infrastructure*, I. Aboudrar, F. Ilahi Bakhsh, A. Nayyar, and I. Ouachtouk, Eds. Cham, Switzerland: Springer Nature Switzerland, 2025, pp. 268–280.

[5] Y. El Marzak, A. Chahid, S. Faris, and K. Mansouri, "A Unified Ontological Framework Integrating Strategic Alignment, Governance, and Information Security," *E3S Web of Conferences*, vol. 680, 2025, Art. no. 00082, https://doi.org/10.1051/e3sconf/202568000082.

[6] Y. Kurii and I. Opirskyy, "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013," in *Cybersecurity Providing in Information and Telecommunication Systems*, Kyiv, Ukraine, Oct. 2022, vol. 3288, pp. 21–32.

[7] J. Y. Mambu, C. Lumingkewas, and G. M. W. Tangka, "IT Governance Maturity Assessment Using COBIT 2019 for System Enhancement and Strategic Decision Support," *CogITo Smart Journal*, vol. 11, no. 1, pp. 193–206, June 2025, https://doi.org/10.31154/cogito.v11i1.998.193-206.

[8] W. Mangoki, D. Manongga, and A. Iriani, "IT Governance Design in XY University Using COBIT 2019 Framework," *Jurnal Sistem Informasi Bisnis*, vol. 14, no. 2, pp. 111–122, Apr. 2024, https://doi.org/10.21456/vol14iss2pp111-122.

[9] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, "Cybersecurity Supply Chain Risk Management for Systems and Organizations," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, USA, NIST SP 800-161r1, May 2022. https://doi.org/10.6028/NIST.SP.800-161r1.

[10] J. Edwards, A Comprehensive Guide to the NIST Cybersecurity Framework 2.0: Strategies, Implementation, and Best Practice, 1st ed. Hoboken, NJ, USA: Wiley, 2024.

[11] "Enterprise Governance and Management of Information Technology Based on COBIT 2019," *Economic and Social Alternatives*, vol. 28, no. 2, pp. 144–150, June 2022, https://doi.org/10.37075/ISA.2022.2.13.

[12] T. J. Olorunlana, "Securing Healthcare Data in the Cloud under HIPAA and NIST Frameworks," *International Journal of Science, Architecture, Technology and Environment*, pp. 61–80, June 2024, https://doi.org/10.63680/ijsate032528.07.

[13] T. Huygh, D. Steuperaert, S. De Haes, and A. Joshi, "The Role of Compliance Requirements in IT Governance Implementation: An Empirical Study Based on COBIT 2019," in *Hawaii International Conference on System Sciences*, Virtual Event, Jan. 2022, https://doi.org/10.24251/HICSS.2022.806.

[14] Sahrul and E. L. Hadisaputro, "Evaluation of Yankel Services Using DSS and MEA Domains Based on the 2019 COBIT Framework (Case Study of Kelurahan Manggar)," *Seminastika*, vol. 3, no. 1, pp. 138–145, Nov. 2021, https://doi.org/10.47002/seminastika.v3i1.264.

[15] M. D. S. Antariksa, M. P. Angin, and A. P. Widodo, "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*, vol. 5, no. 1, pp. 99–105, Mar. 2025, https://doi.org/10.29103/jreece.v5i1.19501.

[16] D. Utomo, M. Wijaya, S. Suzanna, E. Efendi, and N. T. M. Sagala, "Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A," *Communication and Information Technology Journal*, vol. 16, no. 2, pp. 129–141, June 2022, https://doi.org/10.21512/commit.v16i2.8172.

[17] 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.

[18] Abhivardhan, "Data Governance," in *Handbook of Human-Centered Artificial Intelligence*, W. Xu, Ed. Singapore: Springer Nature Singapore, 2025, pp. 1–61.

[19] S. Almuhammadi and M. Alsaleh, "Information Security Maturity Model for NIST Cyber Security Framework," in *Computer Science & Information Technology*, Sydney, Australia, Feb. 2017, pp. 51–62, https://doi.org/10.5121/csit.2017.70305.

[20] R. S. Hidayat, R. E. Indrajit, and E. Dazki, "Evaluation of Information Technology Governance Maturity Using COBIT 2019: A Case Study on the IT Security Industry," *Journal La Multiapp*, vol. 5, no. 4, pp. 478–487, Aug. 2024, https://doi.org/10.37899/journallamultiapp.v5i4.1514.

[21] I. A. Essien *et al.*, "Optimizing Cyber Risk Governance Using Global Frameworks: ISO, NIST, and COBIT Alignment," *Journal of Frontiers in Multidisciplinary Research*, vol. 3, no. 1, pp. 618–629, 2022, https://doi.org/10.54660/.JFMR.2022.3.1.618-629.