Designing an Ontology-Based Framework for ISO 27002-Based Information Security Risk Management

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

Lamia Moudoubah
M2S2I Laboratory, ENSET Mohammedia, Hassan II University of Casablanca, Morocco
Lamiae.modobah@gmail.com

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

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

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

Received: 27 October 2025 | Revised: 3 December 2025 | Accepted: 10 December 2025

 DOI: https://doi.org/10.48084/etasr.15794

ABSTRACT

Information Security Risk Management (ISRM) is an essential requirement for organizations seeking to ensure the governance and protection of their information assets. Ontology-based knowledge representation has emerged as a promising solution to address information security challenges, as it enables the formalization of concepts, relationships, and constraints within a given domain. This paper proposes an ontology-based framework aligned with the ISO/IEC 27002 standard. The approach consists of extracting relevant concepts from textual sources using UML modeling and TF-IDF filtering, and representing them in OWL using the Protégé environment. The resulting ontology formally captures key ISRM entities—including assets, threats, vulnerabilities, risks, controls, and monitoring mechanisms. The ontology was validated using the FACT++ reasoner to assess consistency and semantic completeness. The results show that the proposed model ensures traceability across ISO/IEC 27002 control families, supports governance alignment, and improves visibility across risk treatment processes.

Keywords-ISRM; ISO 27002; ONTOLOGY; TF-IDF; OWL;UML

I. INTRODUCTION

Information security governance has become an increasingly important challenge for all levels of management in organizations [1]. Security must be addressed throughout the system design process, before entering the development and maintenance phases, to ensure effective risk management. Proper risk management protects organizations against threats and helps implement relevant controls within their information systems [2].

As security breaches and information leaks increase, organizations face substantial operational and financial risks [3]. Conducting a risk assessment is an essential component of risk management, allowing organizations to evaluate their security posture, identify vulnerabilities, and implement appropriate controls [4]. However, many organizations lack sufficient information security experts, making it difficult to assess and improve the security of their systems effectively.

To address this gap, the development of a security ontology based on the ISO 27002 standard has been recognized as a significant challenge and an active research area [5]. Such an ontology acts as a knowledge management tool, enabling organizations to formalize concepts and relationships shared by the community, and supporting effective risk assessment and management.

Several ontology-based approaches have been proposed to formalize information security knowledge and support risk management. For instance, in [6], ISO 27002 controls were mapped into an OWL-based security ontology, enriching existing models with formally accepted knowledge. Similarly, in [7], a comprehensive security ontology was aligned with ISO/IEC 27001, covering key concepts such as threats, vulnerabilities, assets, and controls, implemented in OWL-DL for automated reasoning [8]. Although these studies provide valuable foundations, they mainly address partial aspects of information security and do not fully integrate traceability from organizational goals to risk treatment and control implementation.

To address these gaps, this paper proposes a comprehensive security ontology based on the ISO 27002 framework. The proposed ontology formalizes and extracts knowledge from textual sources, using TF-IDF to identify relevant terms, UML to model relationships, and OWL to enable automated reasoning. This approach facilitates automated formulation and validation of security controls, improves governance and traceability, and enhances decision-making within enterprise information systems.

II. MATERIALS USED

A. The ISO 27002 Standard

ISO/IEC 27002 is an international standard for information security, published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005 and most recently revised in 2022 [6]. The current title of the standard is Information security, cybersecurity, and privacy protection - Information security controls, and is part of the ISO/IEC 27000 suite. It provides guidance on organizational standards for information security and good information security management practices, including the selection, implementation, and management of security measures that take into account the organization's information security risk environment(s) [9].

It is developed for organizations that wish to select the measures required as part of the process of implementing an Information Security Management System (ISMS) according to ISO/IEC 27001, implement widely recognized information security measures, and develop their own information security management guidelines [9]. The standard now contains 93 security controls categorized into four thematic clauses (Organizational, People, Physical, and Technological) [9]. Each control has a purpose and is associated with several attributes that provide more detailed information to support its implementation and achieve its objective. They also include implementation guidance, which provides discrete steps (Guideline Steps). The guideline ends with an "Other Information" section that provides additional information that may need to be considered, such as legal considerations or references to other standards [10]. Table I lists the terms and their definitions applied in the international standard ISO 27002.

TABLE I. ISO 27002 CONCEPTS [10]

Term	Definition
Asset	Anything that has value to the organization. (ISO/IEC 13335-1:2004)
Control	Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be administrative, technical, management, or legal. (ISO/IEC 13335-1:2004)
Guideline	A description that clarifies what should be done and how to achieve objectives set in policies. (ISO/IEC 13335-1:2004)
Information processing facilities	Any information processing system, service, infrastructure, or physical locations housing them.
Information security	Preservation of confidentiality, integrity, and availability of information; may also include authenticity, accountability, non-repudiation, and reliability. (ISO/IEC 13335-1:2004)
Information security event	An identified occurrence of a system, service, or network state indicating a possible breach or failure of security safeguards. (ISO/IEC TR 18044:2004)
Informations ecurity incident	One or a series of unwanted or unexpected events with a significant probability of compromising business operations or information security. (ISO/IEC TR 18044:2004)
Policy	Overall intention and direction as formally expressed by management.
Risk	Combination of the probability of an event and its consequence. (ISO Guide 73:2002)
Risk analysis	Systematic use of information to identify sources of risk. (ISO Guide 73:2002)
Risk evaluation	Process of comparing the estimated risk against criteria to determine its significance. (ISO Guide 73:2002)
Risk assessment	Overall process of risk analysis and risk evaluation. (ISO Guide 73:2002)
Risk management	Coordinated activities to direct and control an organization with regard to risks. (ISO/IEC 13335:2002)
Risk treatment	Selection and implementation of options to modify risks. (ISO/IEC 13335:2002)
Third party	Recognized body that is independent of the parties involved, as an organization or individual. (ISO Guide 2:1996)
Threat	Potential cause of an unwanted incident that may result in harm. (ISO/IEC 13335-1:2004)
Vulnerability	Weakness of an asset or group of assets that can be exploited by a threat. (ISO/IEC 13335-1:2004)

B. Presentation of Ontologies

An ontology is a specification of a conceptualization. It represents knowledge in a formal and structured form, providing better communication, reusability, and organization of knowledge, and improving computational inference [11]. Ontology in computer and information science is a hierarchically structured set of concepts describing a specific domain of knowledge that can be used to create a knowledge base. Ontology is an important component of the semantic web and contains concepts, a sub-assumption hierarchy, relations between concepts, and axioms. It may also contain other constraints and functions [11]. An ontology includes a vocabulary common to users, materialized by concepts and relations between them. The notion of ontology is used in different contexts involving philosophy, where the term was initially introduced, and Artificial Intelligence (AI) [12].

The security field needs an ontology to provide a well-known basis to support the development of methods, processes, and appropriate methodologies [7]. This study employed ontologies to benefit from the following advantages:

- Organize and transmit knowledge;
- Check and report risks effectively;
- Share data and information through the organization and reuse communication among people;
- Reuse domain knowledge;
- Make domain knowledge explicit.

The proposed method is particularly intended for organizations seeking compliance with ISO 27002-based security ontologies.

III. RESEARCH METHODOLOGY

A. *Methodologies for Acquiring Ontologies from Texts*

In recent years, ontology engineering has been marked by text-based ontology construction approaches. The acquisition of ontology from unstructured text typically combines Natural Language Processing (NLP), text mining, and machine learning techniques to identify domain concepts and their semantic relationships. Traditional methods are generally categorized into three major families: linguistic approaches (term extraction and lexico-syntactic pattern identification), statistical approaches (co-occurrence and association measures), and machine learning-based approaches (supervised or unsupervised models) [13]. The well-known layer-cake model—comprising term extraction, concept formation, relation extraction, and axiom formulation—remains a foundational methodological framework for ontology learning from textual corpora. Recent research trends emphasize hybrid methods that integrate deep learning with ontology engineering [14]. For example, in [15], an ontology-based deep learning-driven approach was proposed for extracting legal facts from textual data, demonstrating the scalability of ontology learning across complex domains.

In [16], an approach was presented to support automatic acquisition of ontologies from textual data. This approach combines linguistic methods—such as segmentation, lemmatization, and grammatical analysis—with machine learning techniques. Linguistic analysis is employed to extract ontology building blocks, while machine learning algorithms are used to assess their relevance. This process is iterative, allowing the ontology to be progressively refined and enriched prior to expert validation. A tool named Text2Onto was developed to implement this methodology, consisting of a suite of Java-based modules that extract primitives from text, each integrating one or more algorithms such as RTF (Relative Term Frequency) and TF-IDF (Term Frequency–Inverse Document Frequency) [17].

The proposed ontology assists security administrators in learning from past security incidents to prevent and mitigate future ones. It models key information security concepts—such as assets, vulnerabilities, threats, and controls—to structure organization-specific knowledge. This framework supports both strategic decision-making and risk assessment by aligning security activities with business objectives. Moreover, it enables IT managers to justify their security-related decisions to senior leadership based on structured reasoning rather than intuition. The ontology also provides a formal mechanism to organize, document, and communicate security decisions within the organization. The figure below illustrates the main steps followed in its development.

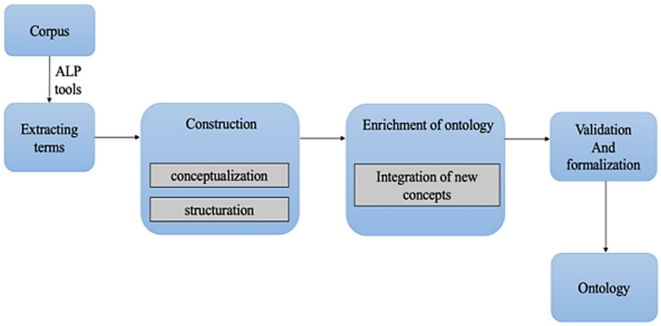

Fig. 1. Architecture of the proposed method for ontology construction.

B. *Term Frequency-Inverse Document Frequency (TF-IDF)*

The TF-IDF technique has been widely applied in the fields of information retrieval and text mining to evaluate the importance of each word within a collection of documents [18]. The TF-IDF method determines the relative frequency of a word in a specific document compared to its inverse frequency across the entire corpus [19]. The first step in the TF-IDF process is the computation of the Term Frequency (TF), which represents the number of times a given term appears in the document. Before this computation, the document must be preprocessed: stop words are removed, and stemming is performed on the remaining words. The Inverse Document Frequency (IDF) is then calculated by considering the number of documents in which the term appears relative to the total number of documents in the corpus. The formula for calculating the inverse document frequency is [20] given by:

$$idf_i = \log \frac{\|D\|}{\|\{d_j : t_i \in d_j\}\|} \quad (1)$$

$$TF - IDF(t_i) = TF(t_i) \times IDf(t_i) \quad (2)$$

A high TF-IDF weight is obtained with a high frequency of a term in a given document and a low occurrence of this term in the documents of the corpus. TF-IDF tends to filter out common terms. This study used a textual corpus composed of 37 documents to compute TF-IDF for ontology construction. In addition, a systematic review of the literature began by defining key research questions. Relevant articles were identified and retrieved using targeted keywords across multiple online databases. Inclusion and exclusion criteria were applied to ensure that only pertinent studies were considered. Data from the selected studies were then extracted, analyzed, and synthesized to provide a comprehensive understanding of the domain. Finally, a detailed discussion was conducted, and conclusions were drawn based on the synthesized evidence. Table II shows the TF-IDF results.

TABLE II. TF-IDF RESULTS

Term	TF	IDF	TF-IDF
Business objectives	5	log(37/5) = 0.86	4.3
Asset	452	log(37/30) = 0.09	40.68
Confidentiality	52	log(37/20) = 0.26	13.52
Availability	102	log(37/24) = 0.18	18.36
Integrity	72	log(37/21) = 0.24	17.28
Vulnerability	403	log(37/28) = 0.12	48.36
Severityscale	3	log(37/3) = 1.09	3.27
Threat	645	log(37/26) = 0.15	96.75
Threat agent	16	log(37/6) = 0.79	12.64
Risk	1670	log(37/35) = 0.02	33.4
Control	641	log(37/33) = 0.04	25.64
Standard control	11	log(37/11) = 0.52	5.72
Policy	265	log(37/22) = 0.22	58.3
procedure	21	log(37/10) = 0.56	11.76
Process	567	log(37/35) = 0.02	11.34

IV. PROPOSED APPROACH

The main contribution of this study is that it proposes an ontology based on the ISO 27002 standard, developed through the text analysis method described in the previous section. In this phase, the relationships among the previously identified security concepts are modeled using a UML class diagram. This diagram is subsequently transformed into an ontology represented in OWL (Web Ontology Language). The choice of a UML-based conceptual modeling approach, followed by OWL ontology development, was motivated by the need for a structured and formal representation of security knowledge. UML provides clear visualization and organization of the relationships between security concepts, whereas OWL enables semantic formalization, automated reasoning, and interoperability with other systems. This combination bridges human understanding and machine processing, supports incremental updates, and ensures alignment with widely recognized security best practices. The following figure presents the class diagram of the proposed ontology.

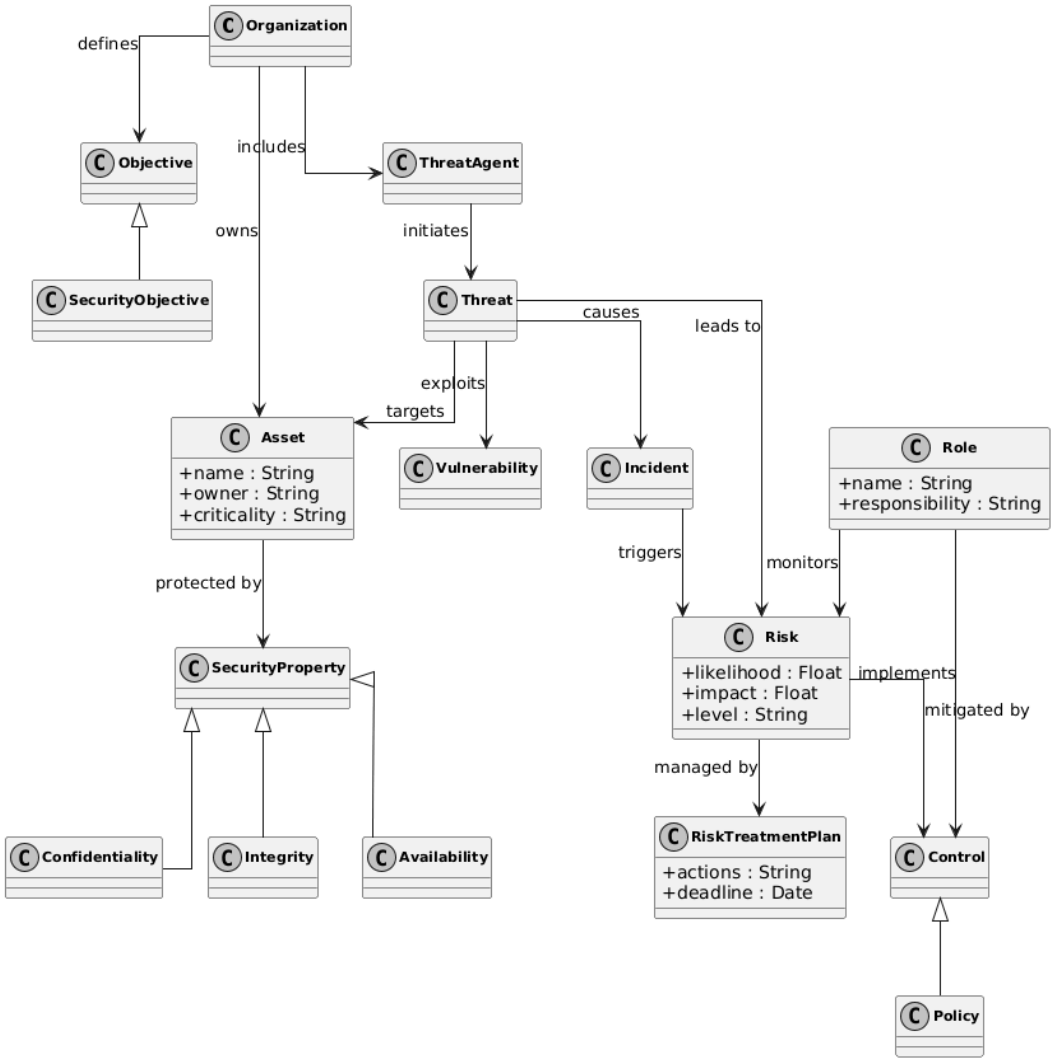

Fig. 2. Class diagram of the proposed ontology.

UML is a language for visualizing, specifying, building, and documenting all aspects and artifacts of a software system [21]. OWL was recommended by the W3C in 2001, and its version 2 in 2009 is designed for use by applications that need to process the content of information instead of just presenting information to humans [22]. OWL provides a level of modeling abstraction that allows structuring and grouping resources with common characteristics into classes. These resources, which belong to the factual level of a modeling, are called assertions, instances, or individuals. The classes belong to the structural level of modeling. A class constitutes a type for a set of individuals; this set constitutes an extension of the class. Since there is no specific modeling language for modeling a knowledge base, the use of the UML class diagram was extended for this purpose. The concepts of the class diagram in Figure 2 were transformed into OWL. UML and OWL have different goals and approaches; however, they have some overlaps and similarities, especially for structure representation [23]. UML and OWL comprise some components that are similar in several regards, such as classes, associations, properties, packages, types, generalization, and instances [23]. UML is a notation for modeling the artifacts of object-oriented software, whereas OWL is a notation for knowledge representation, but both are modeling languages. The UML class diagram (Figure 2) was transformed into OWL according to the following rules.

- Rule 1: A UML class is transformed into an OWL class, with the class name being preserved.

```
<owl :Class rdf :Id="ClassName"/>
```

- Rule 2: In UML, an association can be unidirectional or bidirectional and can be transformed into an object property in OWL. For bidirectional associations, the two attributes are converted into two object properties for each direction [21].

Figure 3 shows an overview of the classes and relations that make up the ontology, and Figure 4 visualizes it graphically. These figures were made with Protégé.

Fig. 3. Classes and relations of the proposed ontology.

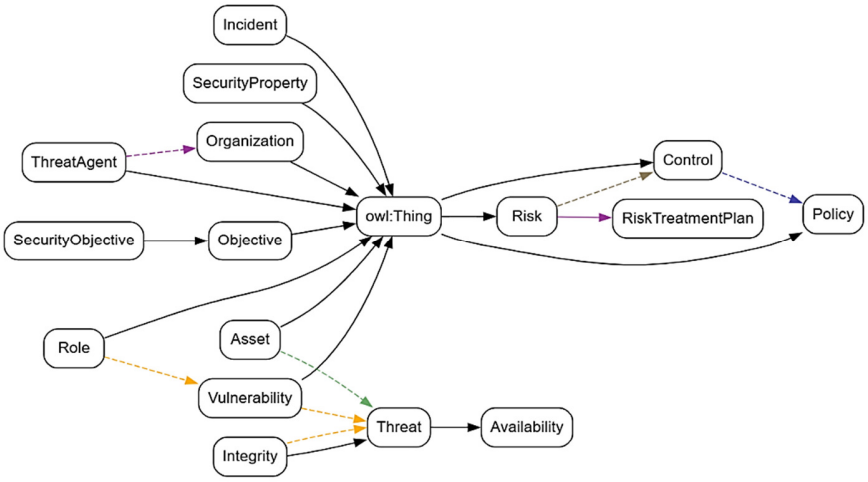

Fig. 4. Graph of the proposed ontology.

V. RESULTS AND DISCUSSION

The validation of ontology structure has attracted the interest of many studies and applications. The FACT++ reasoner [24] allows us to check the consistency and coherence of an ontological model and thus to answer the questions: "does a world exist that is represented by the ontology?", or "are all classes satisfied?" [25]. This approach used the FACT++ inference engine integrated as a plug-in in the protected software to validate the consistency of the proposed ontology.

A quantitative evaluation was conducted to assess the coverage and completeness of the proposed ontology compared to well-established information security ontologies. Table III summarizes the presence or absence of key ISRM concepts across three ontologies: the proposed ISO 27002-based ontology, the ISO-mapping ontology of [7], and the comprehensive domain ontology of [8]. The results show that the proposed ontology provides broader operational coverage, particularly in risk treatment, incidents, roles, and automated knowledge extraction, while maintaining alignment with ISO

27002 controls. This confirms that the ontology is both consistent—validated using the FACT++ reasoner—and comparatively more complete in terms of ISRM process representation.

TABLE III. COMPARATIVE COVERAGE OF SECURITY ONTOLOGIES BASED ON ISO STANDARDS

Concept category	**Proposed ontology (ISO 27002-based)**	**[7]**	**[8]**
Assets	✓ Covered (detailed attributes)	✓ Covered	✓Covered
Threats	✓ Covered	✓Covered	✓Covered
Vulnerabilities	✓ Covered	✓ Covered	✓ Covered
Controls	✓ Fully aligned with ISO 27002	✓ Mapped from ISO 27002	✓ Derived from ISO 27001
Risk Assessment	✓ Likelihood, impact, level	✕ Not explicitly modeled	✓ Included
Risk Treatment	✓ Treatment plans included	✕ Not covered	✕ Not detailed
Incidents	✓ Explicit modeling	✕ Not included	✓ Included
Roles & Responsibilities	✓Organizational roles included	✕ Not included	✓ Partially covered
Governance / Compliance	✓Supported through ISO 27002 alignment	✓ Supported	✓ Supported
Reasoning Support	✓ OWL + FACT++	✓ OWL	✓ OWL-DL
Knowledge Extraction (TF-IDF)	✓ Integrated in methodology	✕ Not included	✕ Not included

The ontology encompasses all crucial elements within the management of information security risks: management, assets, threats, vulnerabilities, risks, controls, roles, compliance, and monitoring. Its relational structure allows for traceability from organizational goals to the treatment of risks and the implementation of controls. This ontology also connects risks to security requirements and legal risks, reinforcing and improving the governance and auditability of risks, thanks to its compatibility with ISO/IEC 27002 and associated frameworks. The inclusion of actors, incidents, KPIs, and audits within risk management workflows demonstrates practical operational workflows and captures the essence of what operational workflows should entail. Nevertheless, this ontology does not address complex patterns of risk propagation, risk maturity, and emerging threats such as AI. The continuity of the challenges is beneficial, as complex compliance tools, automation, and decision support systems can still be developed, along with systems within the spheres of governance, risk, and security management.

VI. CONCLUSION

Information security concept modeling has advantages and challenges. The main challenge is to develop an information security ontology capable of analyzing the impact of risk that can affect all the resources of the organization. This paper proposes an ontology for modeling information security based on the ISO 27002 framework, which allows effective information security management. This ontology was developed in OWL using the Protégé tool. It encapsulates security concepts in accordance with the ISO27002 standard and provides a tool to help information security managers make decisions about which controls to implement to mitigate the risk to the organization's assets. The basic concept of the proposed ontology is based on assets, threats, vulnerabilities, controls, risks, etc. The main advantage is that the semantic knowledge base ensures that all the decision options generated are compliant with the ISO 27002 standard and take into consideration the characteristics of the organization.

Future work plans involve extending the capabilities of this ontology to include other security standards and repositories so that it can contribute significantly to the construction of a theoretical core for information security research and to reduce the ambiguity of terminology.

REFERENCES

[1] 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.

[2] J. Bonar and J. Hastings, "Transforming Information Systems Management: A Reference Model for Digital Engineering Integration," 2024, https://doi.org/10.48550/ARXIV.2405.19576.

[3] Y. Chen, "Information security management: compliance challenges and new directions," *Journal of Information Technology Case and Application Research*, vol. 24, no. 4, pp. 243–249, Oct. 2022, https://doi.org/10.1080/15228053.2022.2148979.

[4] A. Santos-Olmo *et al.*, "Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals," *Frontiers of Computer Science*, vol. 18, no. 3, June 2024, Art. no. 183808, https://doi.org/10.1007/s11704-023-1582-6.

[5] D. Preuveneers and W. Joosen, "An Ontology-Based Cybersecurity Framework for AI-Enabled Systems and Applications," *Future Internet*, vol. 16, no. 3, Feb. 2024, Art. no. 69, https://doi.org/10.3390/fi16030069.

[6] S. Fenz, S. Plieschnegger, and H. Hobel, "Mapping information security standard ISO 27002 to an ontological structure," *Information & Computer Security*, vol. 24, no. 5, pp. 452–473, Nov. 2016, https://doi.org/10.1108/ICS-07-2015-0030.

[7] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, Sydney, Australia, Mar. 2009, pp. 183–194, https://doi.org/10.1145/1533057.1533084.

[8] A. Herzog, N. Shahmehri, and C. Duma, "An Ontology of Information Security," *International Journal of Information Security and Privacy*, vol. 1, no. 4, pp. 1–23, Oct. 2007, https://doi.org/10.4018/jisp.2007100101.

[9] 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.

[10] F. A. Vargas and S. Fenz, *Mapping iso 27002 into security ontology*. 2012. [Online]. Available: https://upcommons.upc.edu/bitstream/2099.1/17302/4/memoria.pdf.

[11] E. Alatrish, D. Tosic, and N. Milenkovic, "Building ontologies for different natural languages," *Computer Science and Information Systems*, vol. 11, no. 2, pp. 623–644, 2014, https://doi.org/10.2298/CSIS130429023A.

[12] R. J. Rovetto, "The ethics of conceptual, ontological, semantic and knowledge modeling," *AI & SOCIETY*, vol. 39, no. 4, pp. 1547–1568, Aug. 2024, https://doi.org/10.1007/s00146-022-01563-3.

[13] J. M. Banda, M. Seneviratne, T. Hernandez-Boussard, and N. H. Shah, "Advances in Electronic Phenotyping: From Rule-Based Definitions to Machine Learning Models," *Annual Review of Biomedical Data Science*, vol. 1, no. 1, pp. 53–68, July 2018, https://doi.org/10.1146/annurev-biodatasci-080917-013315.

[14] R. Du, H. An, K. Wang, and W. Liu, "A Short Review for Ontology Learning: Stride to Large Language Models Trend." arXiv, 2024, https://doi.org/10.48550/ARXIV.2404.14991.

[15] Y. Ren, J. Han, Y. Lin, X. Mei, and L. Zhang, "An Ontology-Based and Deep Learning-Driven Method for Extracting Legal Facts from Chinese Legal Texts," *Electronics*, vol. 11, no. 12, June 2022, Art. no. 1821, https://doi.org/10.3390/electronics11121821.

[16] P. Cimiano and J. Völker, "Text2Onto," in *Natural Language Processing and Information Systems*, vol. 3513, A. Montoyo, R. Muńoz, and E. Métais, Eds. Springer Berlin Heidelberg, 2005, pp. 227–238.

[17] S. Azzi, "A methodology for building a medical ontology a with a limited domain experts' involvement." In Review, Nov. 11, 2024, https://doi.org/10.21203/rs.3.rs-5305559/v1.

[18] K. Sarawan, J. Polpinij, G. Somprasertsri, and B. Luaphol, "Analyzing Hybrid Feature Representations for Improved Multiclass Bug Severity Classification," *Engineering, Technology & Applied Science Research*, vol. 15, no. 4, pp. 24561–24569, Aug. 2025, https://doi.org/10.48084/etasr.11090.

[19] A. Mishra and S. Vishwakarma, "Analysis of TF-IDF Model and its Variant for Document Retrieval," in *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, Jabalpur, India, Dec. 2015, pp. 772–776, https://doi.org/10.1109/CICN.2015.157.

[20] M. Mujahid *et al.*, "Data oversampling and imbalanced datasets: an investigation of performance for machine learning and feature engineering," *Journal of Big Data*, vol. 11, no. 1, June 2024, Art. no. 87, https://doi.org/10.1186/s40537-024-00943-4.

[21] M. H. L. Vo and Q. Hoang, "Transformation of UML class diagram into OWL Ontology," *Journal of Information and Telecommunication*, vol. 4, no. 1, pp. 1–16, Jan. 2020, https://doi.org/10.1080/24751839.2019.1686681.

[22] G. Antoniou and F. V. Harmelen, "Web Ontology Language: OWL," in *Handbook on Ontologies*, S. Staab and R. Studer, Eds. Springer Berlin Heidelberg, 2009, pp. 91–110.

[23] A. Belghiat, "An Approach based AToM3 for the Generation of OWL Ontologies from UML Diagrams," *International Journal of Computer Applications*, vol. 41, no. 3, pp. 41–48, Mar. 2012.

[24] A. Chatterjee, N. Pahari, A. Prinz, and M. Riegler, "Machine learning and ontology in eCoaching for personalized activity level monitoring and recommendation generation," *Scientific Reports*, vol. 12, no. 1, Nov. 2022, Art. no. 19825, https://doi.org/10.1038/s41598-022-24118-4.

[25] M. Richard, X. Aimé, M. O. Krebs, and J. Charlet, "LOVMI : vers une méthode interactive pour la validation d'ontologies," in *26es journées francophones d'Ingénierie des Connaissances (IC)*, Rennes, France, Apr. 2015.