Methodology for Formalizing Knowledge of Business Process Risks and Making Decisions on Countermeasures

Katarina Samoylova
Institute of Physics and Mathematics
Perm State University (PSU)
Perm, Russia
e-mail: katarinasamoilova@yandex.ru
ORCID: 0000-0002-6867-076X

Elena Zamyatina
Department of Information Technologies in Business
HSE University
Perm, Russia
e-mail: e_zamyatina@mail.ru
ORCID: 0000-0001-8123-598

***Abstract*—Effective risk management requires not only the anticipation and prevention of threats but also the formulation of timely and context-aware countermeasures once a risk has materialized. However, many existing approaches lack a transparent, explainable, and formal mechanism for linking risks to actionable responses. This paper proposes an ontology-based expert system designed to support decision-making in risk treatment scenarios. The core of the system is a formal OWL ontology constructed using the MASK (Method for Analysing and Structuring Knowledge) methodology, which facilitates structured capture of expert knowledge, including risks, causes, consequences, and countermeasures. The system applies logical inference through recursive analysis of cause–risk relationships, using annotated diagnostic questions and verification methods. A demonstration scenario illustrates how the system identifies deep-rooted organizational issues and recommends both technical and managerial actions.**

***Keywords*—Expert systems, ontologies, risk management, business process modeling**

I. Introduction

Modern organizations face the challenge of not only anticipating potential risks but also responding effectively to incidents that have already occurred. It is essential to take into account the specifics of business processes, the roles involved, and the contextual factors surrounding each issue. Despite the existence of international standards and advanced risk management systems, the task of developing justified, transparent, and adaptive countermeasures that are directly linked to the underlying causes of risks remains unresolved.

This paper proposes a method for building a decision support expert system based on a risk ontology constructed using the MASK methodology. Unlike traditional approaches that rely on manually generated recommendations or neglect the structure of business processes, the proposed system uses a formalized knowledge structure. It identifies causal relationships, determines confirmed root causes through diagnostic questioning, and suggests actions aligned with both the internal context and corporate policies. The knowledge base is built upon an OWL ontology that integrates risks, causes, consequences, and countermeasures.

The goal of this study is to demonstrate an approach in which expert knowledge is gradually transformed into a formal ontology, and subsequently into a functioning expert system capable of producing explainable and adaptive recommendations in response to risk events. The approach is illustrated through a real-world case involving a marketplace business process, where the system identifies deep organizational issues and proposes context-aware mitigation strategies.

II. Related Works

This section reviews existing methodologies for risk management, with a particular focus on the selection and justification of countermeasures. Special attention is given to models and systems designed to support decision-making, including classical risk assessment and treatment procedures, as well as innovative approaches based on artificial intelligence (AI), machine learning (ML), ontological modeling, and international standards.

In the work of H.-P. Berg [1], risk management is presented as a multi-stage process: establishing context, identification, analysis, evaluation, treatment, and monitoring. The treatment phase includes four classical strategies: avoidance, mitigation, transfer, and acceptance. While analysis methods such as FMEA, HAZOP, and risk matrices are widely used, the actual choice of countermeasures often relies on expert judgment, intuition, or consensus among stakeholders. The study emphasizes that such decisions should consider context, cost, impact, and residual risk, but does not provide a formal system linking specific causes to actions. This limitation underlines the need for approaches that explicitly represent causal structures of risks and derive countermeasures systematically.

Aziz and Dowling [2] analyze the role of AI and machine learning in financial risk management, showing their effectiveness in tasks such as credit scoring, fraud detection, and market modeling. However, the authors emphasize key limitations: lack of structured data, weak integration of expert knowledge, shortage of professionals, and the “black box” nature of neural networks. These issues are critical in risk management, where not only forecasting but also explainable and justified responses are required. While AI/ML approaches

https://doi.org/10.51408/csit2025_69

are valuable for prediction, they do not address the generation of countermeasures, leaving a gap that ontology-based reasoning can fill.

Qin [3] proposes an Intelligent Decision Support System combining machine learning with expert knowledge, but its case-based reasoning approach does not establish explicit causal links between risks and actions. Interpretability and policy alignment remain unresolved, limiting its practical use. Engelberg et al. [4] apply ontologies to model risk propagation in cyber-physical systems, enabling analysis of dependencies between assets and processes. However, their approach remains analytical and does not provide mechanisms for selecting countermeasures.

Vadivel et al. [5] review Governance, Risk, and Compliance (GRC) practices, noting their strategic role in integrating risk management with digital transformation, but also highlighting gaps in formalizing risk causes and decision logic. Sánchez-García et al. [6] survey taxonomies of countermeasures based on ISO/IEC 27005 [7] and NIST SP 800-53 [8], which provide structured catalogs of controls. However, these frameworks rarely link specific causes to context-aware actions, leaving users to select measures manually.

Despite the availability of catalogs and standards, existing approaches rarely provide a unified causal model linking risks to specific countermeasures. As a result, measures are often chosen manually or without regard to business process logic. To address this gap, our study develops a risk ontology that explicitly connects causes and actions, forming the basis for an expert system capable of transparent and context-aware decision support.

III. The Ontology-Based Decision Support System

Modern risk management approaches place significant emphasis on threat forecasting, regulatory compliance, and general recommendations for damage mitigation. However, in many real-world scenarios, the central question remains: what actions should be taken once a risk has already materialized, and how can those actions be justified, transparent, and aligned with organizational policies?

Based on the analysis of existing solutions, several unresolved challenges can be identified:

- Insufficient linkage between specific root causes and relevant countermeasures.
- Lack of explainable reasoning logic.
- Limited capacity for knowledge accumulation and adaptation.
- Difficulty in applying solutions to specific business contexts.

To address these challenges, we propose an ontology-based approach grounded in expert knowledge elicited using the MASK methodology [9]. This approach is implemented in the form of an expert system that performs logical inference based on a structured representation of cause-and-effect relationships.

A. The MASK Method as a Basis for Knowledge Acquisition

MASK (Method for Analysing and Structuring Knowledge) [9] is applied to formalize risk-related knowledge by capturing incidents, identifying root causes, and linking them with consequences and countermeasures. Unlike checklist-based methods, MASK supports collaborative modeling and produces structured representations that can be directly transformed into an ontology for logical inference. Based on these components, an ontology is constructed — a formalized knowledge representation suitable for automated logical inference.

B. Ontology Structure

The result of applying the MASK methodology is an ontology that includes the following key classes:

- Risk – a threat that compromises the objectives of a process;
- Cause – a factor that contributes to the emergence of a risk;
- Consequence – an outcome that occurs if the risk materializes;
- Countermeasure – an action aimed at reducing the likelihood or impact of the risk.

Semantic relationships are defined between these classes:

- hasCause (Risk → Cause): a cause that leads to a specific risk;
- leadTo (Cause → Risk): a cause that, if realized, triggers a new risk;
- mitigatedBy (Cause → Countermeasure): a measure that eliminates or weakens a cause.

In addition, each instance of the Cause class is assigned annotated properties:

- diagnosticQuestion — a question used to clarify whether the cause is present;
- checkMethod — a method or source for obtaining an answer.

Thus, the resulting ontology serves as a structured, explainable, and extensible knowledge model, capable not only of storing information but also of supporting logical inference for decision-making.

C. Architecture and Inference Logic of the Expert System

Based on the described ontology, we implemented an ontology-driven expert system [11], where:

- The knowledge base is structured as an OWL ontology constructed using the MASK methodology;
- The inference mechanism performs a depth-first traversal of the semantic graph formed by risk–cause–countermeasure relationships;
- The user interface supports an interactive diagnostic dialog (a prototype is implemented in Python).

Unlike classical production systems that operate on rule-based "if–then" logic, this system relies on semantic relationships defined in the ontology (e.g., hasCause, leadTo, mitigatedBy) and annotated properties such as diagnostic questions and verification methods.

The expert system, implemented on an OWL ontology, performs depth-first reasoning along risk–cause–countermeasure relations. The user selects a risk, the system verifies causes through diagnostic questions, explores nested risks, and retrieves relevant countermeasures. This ensures knowledge accumulation, context adaptation, and transparent traceability of decisions.

Although implemented in Python, the architecture is compatible with any platform that supports OWL ontologies, SPARQL queries, or similar semantic technologies.

To validate the proposed architecture, we developed a prototype system and tested it on a real-world business process scenario.

IV. Demonstration of the Proposed Ontology-Based System

As a demonstration of the proposed approach, a prototype expert system was developed for selecting countermeasures in the context of a typical business process — marketplace operations. This process involves multiple stakeholders (suppliers, warehouse staff, administrators, etc.) and is subject to various operational risks, such as shipping delays, incorrect product labeling, and insufficient staff training.

In accordance with the MASK methodology, a knowledge engineer collaborated with a subject-matter expert to formalize accumulated expertise. During this process, the following key models were developed:

- History model — descriptions of real incidents, process violations, and common errors;
- Phenomenal model — observable external phenomena and contextual conditions influencing risk realization;
- Task model — the structure of tasks, roles, and actions performed by process participants.

Based on these models, an ontology was constructed, containing classes and relationships that represent the logical structure of risk-related knowledge. This ontology served as the knowledge base of the expert system.

Figure 1 shows a fragment of the ontology graph, including the core concepts: Risk, Cause, Countermeasure, and Consequence, as well as the semantic relationships between them: hasCause, leadTo, and mitigatedBy. Each instance of the Cause class also includes annotated properties: diagnosticQuestion (a question to clarify the presence of a cause) and checkMethod (a way to obtain or confirm the information).

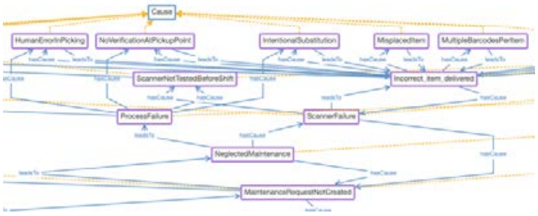


Fig. 1. Ontology graph fragment

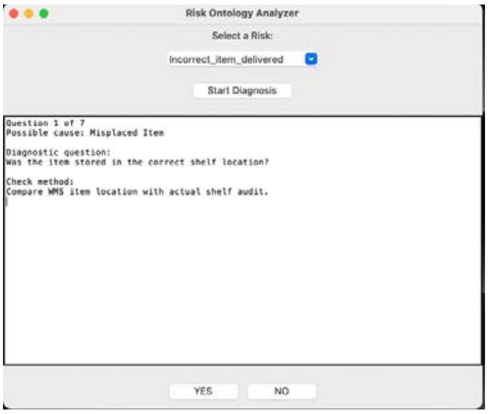
The resulting ontology, which captures the relationships between risks, causes, and countermeasures, was saved in OWL format and used as the knowledge base for the expert system. To demonstrate the proposed method, a prototype was developed in Python using the Owlready2 library [10], which supports ontology loading, access to class structures, and navigation through semantic relationships.

After loading the ontology, the system initializes an interactive interface that allows the user to select a specific risk of interest. The system then automatically retrieves the associated causes and presents diagnostic questions to confirm or rule them out. Confirmed causes are checked for nested risks via the leadTo relation, after which the system generates a list of corresponding countermeasures (via mitigatedBy) and presents them in a final window along with explanations.

For demonstration purposes, a simple graphical user interface (GUI) was implemented using tkinter, providing accessible visualization of the reasoning logic and user interaction.

Suppose that during the marketplace operation, a risk occurs involving the delivery of an incorrect item to the customer. In the expert system, this corresponds to the risk "Incorrect_item_delivered". The user selects this risk from a dropdown list in the system interface.

Once the risk "Incorrect_item_delivered" is selected, the system activates the reasoning module and automatically retrieves the related causes. One of the first causes proposed for verification is "MisplacedItem" (see Fig. 2).



```
Question 1 of 7
Possible cause: Misplaced Item

Diagnostic question:
Was the item stored in the correct shelf location?

Check method:
Compare WMS item location with actual shelf audit.
```

Fig. 2. Diagnostic question generated by the system to verify the cause "Misplaced Item"

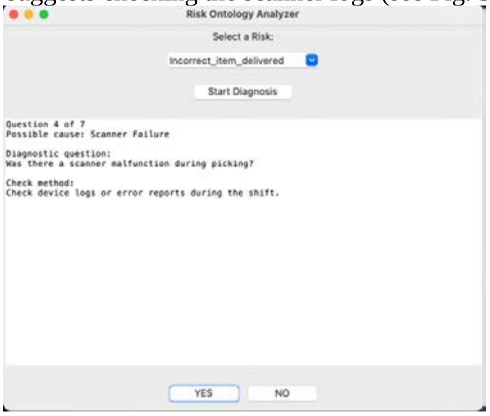
The system formulates the following diagnostic question:

Question: Was the item stored in the correct shelf location?

Check method: Compare the WMS item location with the actual shelf audit.

At this stage, the decision-maker can verify whether the data in the Warehouse Management System (WMS) matches the actual physical placement of the item on the shelf. If the answer is "Yes," the expert system will discard this cause and proceed to the next possibilities.

On the fourth question, the system asks whether the scanner was malfunctioning during item picking. To obtain the answer, it suggests checking the scanner logs (see Fig. 3).



```
Question 4 of 7
Possible cause: Scanner Failure

Diagnostic question:
Was there a scanner malfunction during picking?

Check method:
Check device logs or error reports during the shift.
```

Fig. 3. Possible cause: ScannerFailure

Since the answer is "No" (i.e., the scanner was indeed not working), the cause is considered confirmed. The system retrieves causes related to ScannerFailure via the hasCause relation and continues the diagnostic process (see Fig. 4):

Maintenance Request Not Created: Did the employee report the scanner malfunction to IT (see Fig. 5)?

Scanner Not Tested Before Shift: Was the scanner tested before the shift started?

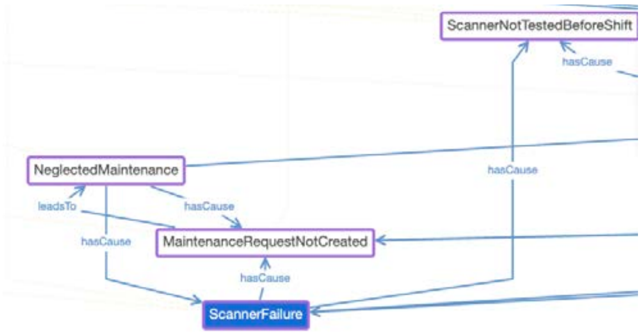
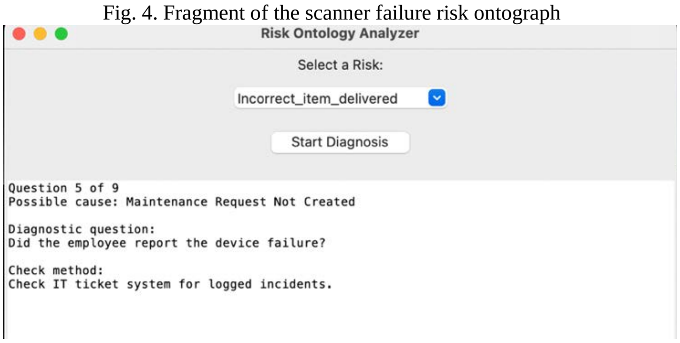


Fig. 4. Fragment of the scanner failure risk ontograph



Select a Risk:

Incorrect_item_delivered

```
Question 5 of 9
Possible cause: Maintenance Request Not Created

Diagnostic question:
Did the employee report the device failure?

Check method:
Check IT ticket system for logged incidents.
```

Fig. 5. Possible cause: MaintenanceRequestNotCreated

In this case, a single incident (Incorrect item delivered) revealed a chain of four underlying causes, including scanner malfunction and outdated staff training. As a result, the system generated both technical and organizational countermeasures — such as equipment repair requests, staff training audits, and process accountability measures.

This shows that the system not only suggests immediate corrective actions, but also uncovers deeper organizational weaknesses, such as gaps in training procedures and maintenance protocols. Such insights are valuable for preventing repeated incidents and improving the overall process resilience.

This example demonstrates how the proposed ontology-driven expert system enables the identification of not only surface-level causes of incidents, but also deeper organizational issues that arise in a specific business context. Thanks to the formalized knowledge structure based on the MASK method, the system ensures transparent and explainable reasoning, provides relevant countermeasures, and contributes not only to localized responses but also to the systematic prevention of repeated failures. In this way, it serves not merely as a diagnostic tool but as a full-fledged decision-support assistant in the field of risk management.

V. Conclusion

This paper presented an ontology-based expert system for risk management using the MASK methodology. The model captures risks, causes, and countermeasures, enabling causal reasoning and transparent decision support. Unlike traditional approaches, it provides context-specific recommendations and can be easily extended as processes evolve. A case study showed that a single incident can reveal deeper organizational problems, demonstrating the value of this approach for both local response and long-term knowledge management. Future work will include integrating the ontology with ISO/NIST standards, extending it with additional business process elements, and experimenting with hybrid inference that combines ontological reasoning with machine learning techniques.

References

[1] H.-P. Berg, "Risk management: Procedures, methods and experiences," *Risk Management*, vol. 22, no. 1, pp. 1–18, 2010.

[2] S. Aziz and M. Dowling, "AI and machine learning for risk management," *SSRN Electron. J.*, 2018.

[3] H. Qin, "Research on machine learning and intelligent decision support system based on risk prediction," *Proc. Int. Conf. Big Data Eng. Intell. Manag. Syst. (ICBDEIMS)*, Atlantis Highlights in Engineering, vol. 4, pp. 582–587, 2023.

[4] S. Engelberg, M. Díaz, M. Klenner, and M. van der Linden, "Towards an ontology-driven approach for process-aware risk propagation," *Proc. 20th Int. Conf. Business Process Management Workshops (BPM 2022 Workshops)*, Utrecht, The Netherlands, CEUR-WS, vol. 3395, pp. 327–338, 2023.

[5] K. Vadivel, J. Prabhakaran, P. Banu, and U. S. Senthil Kumar, "Systematic literature review on GRC – A study on best practices and implementation strategy in GRC," *Samdarshi: J. Electron. Commun. Eng.*, vol. 16, no. 4, pp. 431–440, 2023.

[6] A. Sánchez-García, J. García-Galán, and E. Pimentel, "Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic literature review," *Computers & Security*, vol. 130, 103179, 2023, doi: 10.1016/j.cose.2023.103179.

[7] ISO/IEC, *Information Technology — Security Techniques — Information Security Risk Management*, ISO/IEC 27005:2018, Int. Org. Standardization, 2018.

[8] NIST, *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*, Nat. Inst. Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-53r5.

[9] N. Matta and J. L. Ermine, "Towards a knowledge modelling approach adapted to communities of practice," *Advances in Knowledge Management*, 2007.

[10] J.-B. Lamy, "Owlready: Ontology-oriented programming in Python with automatic classification and high level constructs for biomedical ontologies," *Artif. Intell. Med.*, vol. 80, pp. 11–28, 2017.

[11] P. Jackson, *Introduction to Expert Systems*, 3rd ed., Addison-Wesley, 1999.