Advanced Framework for Integrating Risks into an Organizational Setting

Marina Yancey
Faculty of Humanities, Ulyanovsk State Technical University, Ulyanovsk, Ulyanovsk Oblast, Russia, 432027.
may@ulstu.ru

Correspondence should be addressed to **Marina Yancey** : may@ulstu.ru.

Article Info
Journal of Journal of Enterprise and Business Intelligence (http://anapub.co.ke/journals/jebi/jebi.html)
Doi: https://doi.org/10.53759/5181/JEBI202404005
Received 10 January 2023; Revised from 18 July 2023; Accepted 12 August 2023.
Available online 05 January 2024.

Abstract – Enterprise risk management (ERM) is a systematic approach that strategically assesses risk management from a holistic standpoint, including the whole company or enterprise. The aforementioned approach is a top-down strategic methodology designed to detect, evaluate, and proactively address possible risks, threats, hazards, and other sources of damage that have the potential to impede an organization's operations and goals, or result in negative outcomes. ERM is a prominent framework that assists businesses in the identification, evaluation, and management of hazards at the enterprise level. Scholars identified many elements that serve as motivators for enterprises to participate in the process of ERM. These reasons include the likelihood of encountering financial hardship and the subsequent expenses, subpar profits performance, potential development prospects, and the autonomy of the board. The implementation of an effective risk management plan might potentially serve as a competitive advantage for organizations, facilitating their growth. This elucidates the extensive corpus of research devoted to ERM. This paper examines the fundamental connections between Enterprise Architecture and Risk Management and presents a proposed architectural framework for effectively incorporating risk considerations within the broader organizational context. This article presents a proposed strategy for attaining a comprehensive and shared perspective on hazards throughout an organization.

Keywords – Enterprise Risk Management, Risk Analysis, Enterprise Architecture, Environmental Assessment, Enterprise Architecture Implementation Methodology.

I. INTRODUCTION

Enterprise risk management (ERM), which adopts a comprehensive approach and necessitates management-level decision-making, may not have goals or objectives that are consistent with those of a business unit or sector. Therefore, developing firm-wide monitoring is prioritized rather than giving individual business units the responsibility of controlling their own risks. Additionally, it often involves communicating the risk management plan to all relevant stakeholders and including it in the annual report. A broad number of sectors have embraced the use of ERM, including banking, insurance, public health, international development, and aviation. While also seeing unique possibilities that emerge at the organizational level, ERM has the ability to reduce risks across the board for the whole business. Efficient cooperation and communication between various business units is crucial for effective implementation of ERM.

The objective of an ERM method is to cultivate a comprehensive comprehension of the primary risks that management, as a collective, deems to be the most crucial dangers now, posing a potential threat to the strategic triumph of the organization. Many firms place emphasis on identifying and prioritizing the top 10 risks deemed significant by management. Zieba, Durst, and Gonsiorowska [1], presents more insights into the various methods used by organizations to prioritize their most critical risks. Typically, the board's presentation of the top 10 risks emphasizes significant risk themes, while management is responsible for monitoring more specific and detailed aspects. One illustrative risk factor that businesses may encounter is to the ability to recruit and retain essential personnel. The board of directors may engage in a high-level discussion on the risk problem, while management directs their attention towards the distinct issues associated with recruiting and keeping talent in certain functional areas of the business, such as IT, sales, operations, and so forth.

After acquiring an understanding of the most notable hazards that lie ahead for the organization, management proceeds to assess if the existing approach used by the organization in managing those risks is satisfactory and successful. In some instances, management may make the decision to accept a risk in collaboration with the board, while for other risks, they aim to react by implementing measures to mitigate or prevent the possible exposure to risk. When considering strategies to address risks, it is crucial to contemplate both preventive measures to mitigate the likelihood of a risk occurrence and responsive measures to mitigate the consequences in the event that the risk materializes. A widely used method for

facilitating the conceptualization of risk response strategies is referred to as a "Bow-Tie Analysis," [2] as seen in **Fig 1**. The left side of the "knot" represents the risk event and provides management with insights into potential measures that may be undertaken to mitigate the likelihood of the risk materializing. The right side of the "knot" facilitates managerial deliberation on potential measures that might be implemented to mitigate the consequences of a risk event in the event that prevention measures fail.

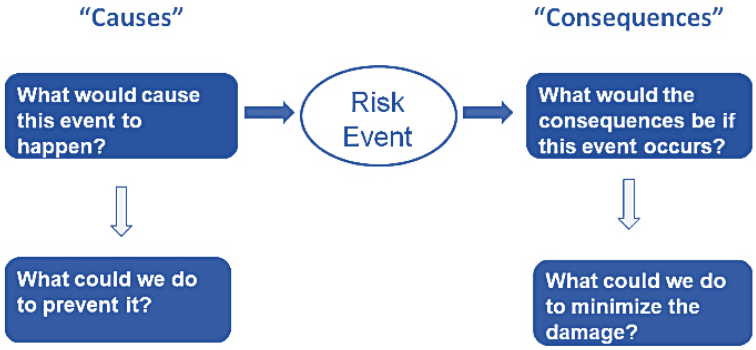

Fig 1. Bow-Tie Tool for Developing Responses to Risks

The risk management architecture serves as a comprehensive structure that facilitates the seamless integration of risk management practices across all facets of a company [3]. The architectural framework is primarily focused on the principles of leadership and dedication, including four key elements: design, execution, assessment, and enhancement. Given the rapid integration of computer systems into organizational processes that serve human, societal, and organizational objectives, it becomes imperative to adopt a comprehensive perspective of the overarching sociotechnical system. The ramifications arising from a malfunction within one layer of the sociotechnical system are amplified due to the interconnections and interdependencies between the many levels.

Therefore, it is essential for software components to possess trustworthiness, ensuring their availability as needed and their proper operation without generating any undesirable consequences. The degree of trustworthiness shown by a system of computer is often referred to as its dependability. Dependability may be seen as a collection of security criteria aimed at safeguarding systems against various abnormal occurrences, such as internal breakdowns and assaults. To establish comprehensive protection criteria, it is necessary to possess a thorough comprehension of the potential dangers that may impact the system and its surrounding habitat. The use of a risk-driven methodology is often employed in order to comprehend the potential occurrences that may result in harm and are deemed probable. In intricate and reliable systems characterized by interconnections and interdependencies among various components, the comprehensive perspective and dissemination of risk information emerge as crucial mechanisms for attaining optimal protection needs.

This article presents a proposal for aligning Governance, EA, and RM activities. The objective is to provide a systematic approach that enables the mapping and tracking of recognized risks to artifacts represented inside an EA. This alignment aims to support the overall strategic goals of organizations. In this study, we examine the correlations between EA and RM activities. Additionally, we provide a comprehensive architecture and suggest a solution for effectively managing risk data in an integrated manner. The rest of the paper is organized as follows: Section II presents a critical review of previous literature assumptions related to risk conceptualization, determinants of RM implementation within an enterprise, risk management, and enterprise architecture. Section III presents a detailed review of the proposed architecture and solution. Finally, Section IV presents concluding remarks to the article.

II. LITERATURE REVIEW

Risk Conceptualization

Numerous endeavors have been undertaken to develop widely acknowledged definitions of pivotal terminology associated with essential ideas in the field of risk. In order for a scientific field or discipline to establish a strong foundation, it is essential to rely on well-defined and widely comprehensible terminology and ideas. However, empirical evidence has shown that reaching a consensus on a singular, comprehensive collection of definitions is not feasible. The aforementioned statement served as the initial basis for a cognitive process undertaken in recent times by a group of esteemed professionals affiliated with the Society for Risk Analysis (SRA). This endeavor culminated in the development of a novel lexicon for the SRA [4]. The underlying premise of the glossary is rooted in the notion that it remains feasible to develop definitive definitions that carry authority. This may be achieved by accommodating diverse opinions on basic ideas and by differentiating between overarching qualitative definitions and the measures connected with them. The primary emphasis of this discussion will be on the idea of risk. However, it is important to note that the vocabulary also include other relevant concepts, including probability, vulnerability, robustness, and resilience. Incorporating diverse viewpoints does not imply the inclusion of all definitions available in the literature inside the glossary. The definitions that are included must adhere to some fundamental requirements, such as possessing a logical, well-defined, clear, and explicit explanation.

In the following section, we provide a condensed rendition of the risk definition excerpt sourced from SRA.The present analysis pertains to a forthcoming undertaking, which encompasses a broad scope including natural occurrences. Specifically, we examine the functioning of a system and establish the concept of risk in regard to the potential outcomes of this undertaking, considering its impact on aspects that have significance for human beings. The repercussions are often seen in connection to certain reference values, such as intended goals or aims. Typically, the emphasis is placed on negative and unwanted effects. In each given situation, it is certain that there exists a minimum of one outcome that is seen as bad or unpleasant.

In general, qualitative definitions of risk can be described as follows: (a) the likelihood of an unfavorable event occurring, (b) the potential for the realization of undesirable and negative outcomes resulting from an event, (c) the exposure to a proposition, such as the occurrence of a loss, in which one's level of certainty is uncertain, (d) the consequences of engaging in an activity along with the uncertainties associated with it, (e) the uncertainty and severity of the consequences of an activity in relation to something that is valued by humans, (f) the instances of specific consequences arising from the activity and the uncertainties associated with them, and (g) the deviation from a reference value accompanied by uncertainties. These definitions essentially convey a similar concept, including the element of uncertainty in relation to events and their outcomes. The International Organization for Standardization (ISO) [5] provides a definition of risk as the impact of uncertainty on goals. The interpretation of this definition may vary, with one potential interpretation being that it is a particular instance of the definitions previously discussed, such as (d) or (g). In order to characterize or quantify risk and assess its magnitude, determinants outlined in the following paragraph are used.

Determinants of RM implementation within an enterprise

Numerous empirical studies have been conducted to examine the factors that influence the adoption of ERM systems, focusing on various business characteristics. **Table 1** presents a comprehensive overview of the factors influencing investment decisions in an ERM program, as derived from existing scholarly literature.

Table 1. Factors affecting the investment decision in ERM

Factors	Formula	Projected relationship	Explanation	Literature
Size of the firm	Asset book value (log)	Positive	Larger organizations are capable of implementing an ERM program across multiple business divisions and have a thorough grasp of risk identification. Numerous results exist about the likelihood of major firms to engage in ERM projects.	Kim and Yoo [6]
Financial leverage	Equity market value/Liability book value	Negative/Positive	The findings exhibit a combination of favorable and negative associations. The adoption of ERM necessitates the allocation of financial resources, making it more feasible for companies with lower levels of debt to launch such a program. However, it should be noted that the implementation of the ERM program has been shown to have positive effects on risk assessment and a decrease in loan expenses. Consequently, firms may choose to enhance their financial leverage given these advantageous circumstances.	Jurdi and AlGhnaimat [7]
Book-to-market ratio	Equity market value/Equity book value	Positive	Since ERM systems help preserve franchise value, the adoption of ERM is often more appealing to businesses with high ratios of the book-to-market.	Celona, Driver, and Hall [8]
Managerial career	Market value1-market valuet-1/market valuet-1	Positive	The application of ERM has been shown to improve the quality and relevance of earnings information, serving as an indicator of the company`s managerial competencies.	Desir, Nam, and Pfeiffer [9]

Financial laxness	Marketable securities plus cash / total assets	Positive	Increased financial slack may persuade businesses to set aside money for the initial expenditure essential to develop an ERM initiative.	MacDonald and Moore [10]
Earnings volatility	The quarterly fluctuation in earnings before interest and taxes (EBIT)	Positive	There are potential advantages for companies with fluctuating revenues to start the implementation of an ERM framework.	Tola [11]
Capital invisibility	Intangible assets/ Value of Book Assets	Positive	High levels of capital opacity in companies make them more likely to take part in ERM arrangements, especially when they are struggling financially.	Currie and Williamson [12]
Profit from Assets	Net income/Value of Book Assets	Positive	The Return on Assets (ROA) is widely recognized as a measure of managerial efficiency. Consequently, organizations that exhibit greater ROA values are more inclined to invest their financial resources towards engaging in ERM activities.	Wijaya [13]
Acquisition and merger and acquisition (M&A) activities	Book value of all assets - intangible assets	Negative	There exists a negative correlation between recent merger and acquisition (M&A) activity and a firm's likelihood of initiating ERM adoption. This is attributed to the potential unavailability of extra money to allocate towards the implementation of such a program.	Edi, Basri, and Arafah [14]

Risk management

Numerous organizations are increasingly recognizing the need of using established efficient strategies and systematic procedures for managing their software projects. Therefore, the outcomes achieved are significant when project managers prioritize the effective management of associated risks, aiming to minimize their influence and vulnerability. This includes proactive measures to mitigate risks and, if they do arise, ensuring they are handled in a controlled manner. Risks inside a company include a range of potential threats, including security breaches, failures in human resource management, financial difficulties, challenges in the business environment, and project failures. As stated in the Project Management Body of Knowledge (PMBOK), a risk refers to an ambiguous occurrence or circumstance that, if materialized, would provide either a favorable outcome (opportunity) or an unfavorable outcome (threat) impacting at least one project goal. The factors that may be included in a project are time, cost, scope, and quality. Risk may arise from one or more factors and can result in various repercussions on the project. According to Bhat and Farooq [15], an event or condition may be characterized as a factor that has the potential to result in harm, loss, or a setback within the context of a software project.

Risk management is a systematic procedure that involves the identification, assessment, and mitigation of risks, with the ultimate goal of lowering them to a level that is deemed acceptable by companies. Projects often start with a heightened degree of risk exposure, which gradually diminishes as the project advances over time. This reduction in risk is attributed to the accumulation of more information, leading to a decrease in uncertainty. The field of risk management has had significant advancements in recent decades, becoming as a crucial component within the realm of project management. The aforementioned activities included under project management consist of control, planning, monitoring, identification, response, and analysis. Risk management is a scholarly subject that incorporates information from many business fields and using numerous approaches to address specific issues. Risk management is widely acknowledged and included as an essential component of project management by many project management organizations. Risk management encompasses a range of techniques, methodologies, and accompanying instruments that are used to detect and mitigate risk to a level that is deemed acceptable.

The foundational concepts of ERM, which form the basis of holistic risk management, were first formulated in the mid-1990s by the individuals responsible for the establishment of the Australian risk management standard. Subsequently, the Canadian risk management community made further contributions to these ideas. In response to a series of corporate crises characterized by unethical behavior, the COSO (Committee of Sponsoring Organizations of the Treadway Commission) made the decision to expand its internal audit framework to include ERM. Consequently, the first COSO ERM framework was released in 2004. Suparto and Lukmandono [16] has now become a widely accepted and often used resource in debates pertaining to the implementation of ERM, in conjunction with ISO 31000. ISO 31000 is an internationally recognized

standard that outlines the concepts and guidelines for effective risk management implementation. The primary objective of frameworks such as ISO 31000 is to facilitate adherence to established standards, provide confidence in organizational processes, and enhance the quality of decision-making.

According to the Committee of Sponsoring Organizations of the Treadway Commission [17], ERM is a systematic approach aimed at identifying potential events that may affect a company and effectively managing these risks to ensure they remain within the company`s predetermined tolerance of risk. By doing so, ERM provides a fair level of confidence that the organization's goals will be achieved. This procedure is to be executed by individuals at various hierarchical levels within the business, including the board of directors of the company. While there may be variations in definitions within the ERM community, the concept of risk appetite often refers to the level of risk that an organization is prepared to assume in order to pursue favorable and suitable opportunities for growth. In the context of ERM frameworks, risk is often understood as the potential for not attaining the predetermined objectives established by organizational management. The definition of risk as "the effect of uncertainty on objectives" is explicitly articulated in ISO 31000. Kulić [18] utilizes a metaphor of a thermostat to explain the COSO framework. Organizations endeavor to detect and assess all significant risks and establish appropriate control measures to mitigate them, resulting in a remaining level of risk that aligns with their predetermined risk tolerance. This process may be likened to the functioning of a thermostat, which adapts to variations in the surrounding conditions in order to maintain a desired temperature as per a predefined goal.

Enterprise Architecture

Enterprise Architecture (EA) is used by organizations to provide a cohesive environment that facilitates the harmonization of the IT (Information Technology) infrastructure and enterprise's business operations. The EA project has two primary methodologies, namely the EAIM (Enterprise Architecture Implementation Methodology) and the EAF (Enterprise Architecture Framework). The aforementioned techniques aim to facilitate the implementation of Enterprise Architecture (EA) by offering strategies for planning EA projects, creating models of EA artifacts, constructing organized artifacts, overseeing the implementation of EA, supporting EA governance, and ensuring the maintenance of the EA implementation. The purpose of the EA framework is to gather data from both the IT and business aspects of a company and create a model based on this knowledge. On the other hand, EAIM aims to use these models in order to develop suitable information systems and IT infrastructure for the firm. The acronym EAF stands for company Architecture Framework, which serves as a structural framework for modeling the business and IT units of a company. There are several models that include diverse viewpoints within the field of Enterprise Architecture Frameworks (EAF), each exhibiting distinct scopes and activities. The outputs of Enterprise Architecture (EA) are the artifacts produced by EA, which include models, diagrams, documentation, and reports.

Given that EA artifacts alone are inadequate for achieving alignment between business and IT in companies, organizations are actively seeking a methodology to effectively solve their competitiveness concerns via the use of EA artifacts. The EAIM (Enterprise Architecture Implementation Methodology) is a systematic technique used to address the requirements of implementation of EA and give a detailed strategy for enabling the EA artifacts. The Enterprise Architecture Integration Methodology should include all facets of the Enterprise Architecture (EA) lifecycle. This includes the strategic planning for comprehending enterprise projects, the thorough analysis of business needs, the meticulous systems design, the continuous development of systems, and the continual upgrades of all aforementioned components. There exist multiple Enterprise Architecture Integration Methods (EAIMs), each characterized by distinct approaches, practices, and perspectives. However, they share a common understanding of EAIM, which refers to a generic procedural framework encompassing the following aspects: (1) the existing systems state and structure, (2) the explanations and practices guiding the management of step-by-step guidelines for current architecture transitioning to the desired one, (3) the explanations and practices facilitating the maintenance and continuous updating of the enterprise to effectively adapt to forthcoming changes, and (4) the practices and explanations governing the supervision and control of systems and artifacts.

The approach used by Tambouris, Zotou, Kalampokis, and Tarabanis [19] is comprehensive and succinct, providing a cohesive framework for experts in the field. The efficacy of Enterprise Architecture (EA) is assessed based on the extent to which the outcomes of EA implementation contribute to the achievement of the enterprise's desired objectives. Moreover, the efficacy of the EA function may be defined as the extent to which company goals are achieved via the outputs of the function of EA. The measurement of effectiveness may be conducted in an objective manner by analyzing organizational performance data that is specifically relevant to the application of EA decision-making. The efficiency of the EA implementation technique used to facilitate the implementation of Enterprise Architecture is hindered by the intricate nature of the procedures, models, methodologies, and strategy employed in EAIM. As a result, EA initiatives may encounter challenges in several aspects of EA, including requirement analysis, governance and assessment, implementation guidance, and ongoing development of EA implementation.

The architecture of the risk management process refers to the underlying framework that encompasses the structural arrangement of its processes, including the many elements involved in the form of inputs, processing mechanisms, and outputs. This study examines the architecture of risk management processes, including an inventory and comprehensive description of each process, its constituent components, and their interconnections. Additionally, it explores the interplay between risk management processes and other corporate processes, highlighting how they collaborate and integrate. This

article presents an analysis of the links between EA and RM activities. Additionally, an architecture and solution are proposed for the integrated and comprehensive management of risk information.

III. PROPOSED ARCHITECTURE AND SOLUTION

Discussion of Architecture

This section provides an analysis of the connections b1/27/2024etween RM and EA. The initial step in establishing the external and internal context of risk management (RM) involves considering the legal environment, key values for stakeholders, organizational culture, and trends. These aspects are also addressed in the three phases of enterprise architecture (EA): requirements management, preliminary, and vision. During the requirements management phase, the overall requirements are defined and refined. In the preliminary phase, principles, constraints, and the main goals are established. Lastly, in the vision phase, an initial model is created to represent the company`s overall architectural vision. In this scenario, there exists a reciprocal relationship between Enterprise Architecture (EA) and Requirements Management (RM), since each process may serve as an input for the other process. For instance, the outcomes derived from a Requirements Management process can be used in the establishment of the Enterprise Architecture vision.

The identification of risks can be achieved through the application of a systematic analysis approach, which involves the technology architectures, information systems, and utilization of business. This approach allows for the identification of vulnerabilities in existing technology infrastructures, processes, information entities, or actors. These vulnerabilities are then assessed in relation to threats that arise from specific requirements and contextual factors. Risk assessment is a crucial tool used by investors, organizations, and governments to evaluate the likelihood of an unfavorable occurrence occurring and its potential to have an effect that is detrimental on project, company, investment, or economy. In order to determine the viability of a certain investment or project and to determine the most efficient ways to reduce such risks, risk appraisal is essential. Risk analysis encompasses many methodologies that may be used to evaluate the balance between risk and reward associated with a prospective investment opportunity. The first step undertaken by a risk analyst is the identification of prospective risks or hazards. The aforementioned drawbacks need to be taken into consideration in light of a probability meter that quantifies the possibility of the event taking place. Risk analysis is to assess the potential magnitude of the consequences that may arise in the case of an occurrence. Various risks, like currency risk, credit risk, and market risk, among others, may be mitigated by hedging strategies or the acquisition of insurance.

In addition, the detailed descriptions supplied by the EA may be used in risk analysis, which involves estimating the possibility and implications of potential risks, as well as in assessment, which entails identifying choices and establishing priorities. For example, one may do an analysis on the propagation of the exploitation of a vulnerability inside a particular technological component. This analysis may include several aspects such as the impact on stakeholders, information entities, business processes, and so on. The EA opportunities and solutions phase can utilize the risk plans and options of treatment offered by the treat risk process of RM to formulate an initial implementation plan for the overarching architecture. This plan may encompass activities such as business process redesign and hardware component replacement. Conversely, the pursuit of solutions within the environmental assessment (EA) process may provide valuable insights for assessing prospective risk mitigation strategies. This may be achieved via an inclusive strategy, which involves mitigating a particular set of risks. Conversely, an exclusive approach is also possible, when a treatment option is deemed unsuitable due to non-compliance with regulations or failure to address specific issues within the EA.

The results from the risk phase of treatment may also be used by the planning process of migration, in a way similar to the link between opportunities and risk treatment and solutions. Specifically, this entails outlining the procedures required to create, improve, and monitor the implementation of the architecture, as mentioned in the solutions and opportunities phase. It is evident that the governance implementation phase is seen as a management project effort, with a thorough risk management strategy especially designed for this goal. However, when focusing exclusively on the direct links, the risk plans developed during the risk treatment phase of the risk management process provide crucial insights for establishing the management and governance measures required to accomplish the intended design. This ensures adherence to the specified architecture while effectively managing risk. The goal of the change management phase of architecture is to assure the ongoing suitability of the architecture by identifying necessary modifications and evaluating its performance to the principles and framework established in earlier stages. This component has the capability to serve as a monitoring mechanism for detecting changes in enterprise architecture (EA) components. The tracking of risks associated with EA components allows for the discovery of potential new hazards or changes in the severity of previously recognized problems. This is shown by the impact of modifications on the risk identification process.

The monitoring component of this phase differs from the monitor and review process because of the mapping between risks and enterprise architecture components, which allows for bidirectional information flow. The management of EA requirements involves gathering information from other activities to assess the degree to which needs have been recognized and solutions have been put into place. Monitoring activities are closely tied to this process. Establishing efficient lines of communication with all pertinent stakeholders is the main goal of the RM communicates and consult procedure. Since enterprise architecture (EA) spans high-level planning through system implementation, with each step being intimately related to particular stakeholders, this activity is essential to all EA processes.

Proposed Solution

To effectively tackle the challenges surrounding interoperability and standardization in the realm of Risk Management (RM), as well as its integration with Governance and Enterprise Architecture (EA), we put up a proposal for a comprehensive RM Framework. This framework encompasses the use of a Risk-DL (Domain Specific Language) for RM, which is based on XML, and is further reinforced by a formal description of the fundamental concepts within RM. The suggested framework is underpinned by a system of information designed to effectively handle the identification and categorization of hazards. Furthermore, the implemented solution has been seamlessly connected with a MDR (Metadata Registry) in order to facilitate the inclusion and alignment of various risk representations inside the risk description language [20]. The use of a Metadata Registry (MDR) aims to guarantee the compatibility and exchangeability of diverse representations of risk, as suggested by IEC/ISO 11179. In this context, an information system assumes the responsibility of effectively storing and disseminating descriptive data pertaining to resources, specifically risk information.

It is crucial to identify the systems that impose limits on both semantics and system-specific factors, such as the maximum length of a string, in order to effectively store data using MDR. Additionally, documenting these constraints is of utmost importance. For instance, altering the string maximum length should not result in any alteration of the underlying data element's meaning. The ISO (International Organization for Standardization) has released a set of standards pertaining to a metadata registry known as ISO/IEC 11179. Additionally, ISO has published ISO15000-3 and ISO15000-4, which pertain to the exam registry and repository (regrep). The ebXML (Electronic Business using eXtensible Markup Language) RegRep (Registry and Repository). There are two well recognized international standards that are often known as metadata registry standards: ISO 15000-3 and ISO/IEC 11179. There exists a subset of individuals who hold the belief that ISO 15000-3 and ISO/IEC 11179 possess interchangeability or, at the very least, exhibit some similarities.

It is noteworthy that the ISO 11179 model had a significant role in the improvement of the ebXML RIM (registry model of information), resulting in substantial functional similarities between the "registry" section of the conceptual model of ISO 11179 and the ebXML RIM. Nevertheless, this assertion is inaccurate. The first section of the Design Objectives of the ebRIM v2.0 specification states the intention to maximize the use of the ISO 11179 and OASIS Registry models. By the release of ebRIM v3.0 on May 2, 2005, all mention to IEC/ISO 11179 has been significantly minimized, appearing only as an instructive reference on page 76 out of a total of 78 pages [21]. Some team members acknowledged that the ebXML RIM data model did not have a designated storage space for "fine grained artifacts". In IEC/ISO 11179, the fundamental components of data, often referred to as data elements, were not explicitly and definitively addressed by the team until 2009. The user's message is already academic and do not require to be rewritten.

According to IEC/ISO 11179 [22], its focus is on "traditional" metadata, specifically referring to descriptions of data in a conventional sense. The word is delimited within the scope of IEC/ISO 11179 to include the more customary use of metadata. Initially, the standard designated itself as a register for "data elements." The text delineates the concept of data elements, asserting that they serve as the basic entities of data. Furthermore, it elucidates that data elements include many forms of data, including characters, pictures, sound, and other similar entities. Additionally, the article provides an example to illustrate the concept of a registry: "This can be likened to the registries that governmental bodies maintain in order to monitor and manage motor vehicles." Each motor vehicle is described and recorded in the registration, however, the physical vehicle itself is not included.

By using a defined reference model to capture the descriptions of data and assuring semantic interoperability, a metadata registry (MDR) makes interoperability easier. Furthermore, it records the contextual data required for the proper use of the data, hence fostering pragmatic interoperability. Additionally, the MDR keeps track of the data object's version information, facilitating dynamic interchange. It also maintains relationships between several versions of the same or distinct data objects, fostering conceptual interoperability. The Risk-DL language's syntactic representation is unimportant for the primary objective of this strategy. The suggested solution also gives users access to a variety of decision-support tools that facilitate the creation of appropriate risk management strategies and facilitate the evaluation of the efficacy of different treatment options. The architectural design of the suggested solution is further upon in **Fig 2.**

Operator refers to the employee who takes responsibility for interacting with the system inside the organization. The Operator initially offers a comprehensive Risk Description, which is afterwards converted into the Risk-DL Specification of those hazards by utilizing the Risk Modeling component. The MDR component offers assistance with the conversion into the Risk-DL Specification. As a result, the architectural framework enables coexistence of many Risk-DL iterations and alternate risk representations. The user's text has gaps in it. Please provide the whole document that needs to be edited. The use of this strategy is justified by the notion that there shouldn't be any conflict between the services responsible for processing risk information.

The Plan Evaluator generates a range of statistical data to facilitate the assessment of various risk treatment plans and determine the optimal course of action for a given situation. The process of defining risks based on various scoring systems, such as semi-quantitative, qualitative, quantitative, or other scales, necessitates the use of a Risk Normalizer. This tool is responsible for standardizing scores, hence enabling the comparison and ranking of risks that have been identified using disparate methodologies. Ultimately, the Report Generator generates Risk reports that serve to facilitate the determination of the most suitable course of action to implement. Additionally, it is important to provide risk information to various stakeholders that possess distinct concerns. Given the aforementioned, the Report Generator is linked to the MDR in order

to give several representations for examining the risk data, taking into account the specific interests and concerns of each stakeholder.

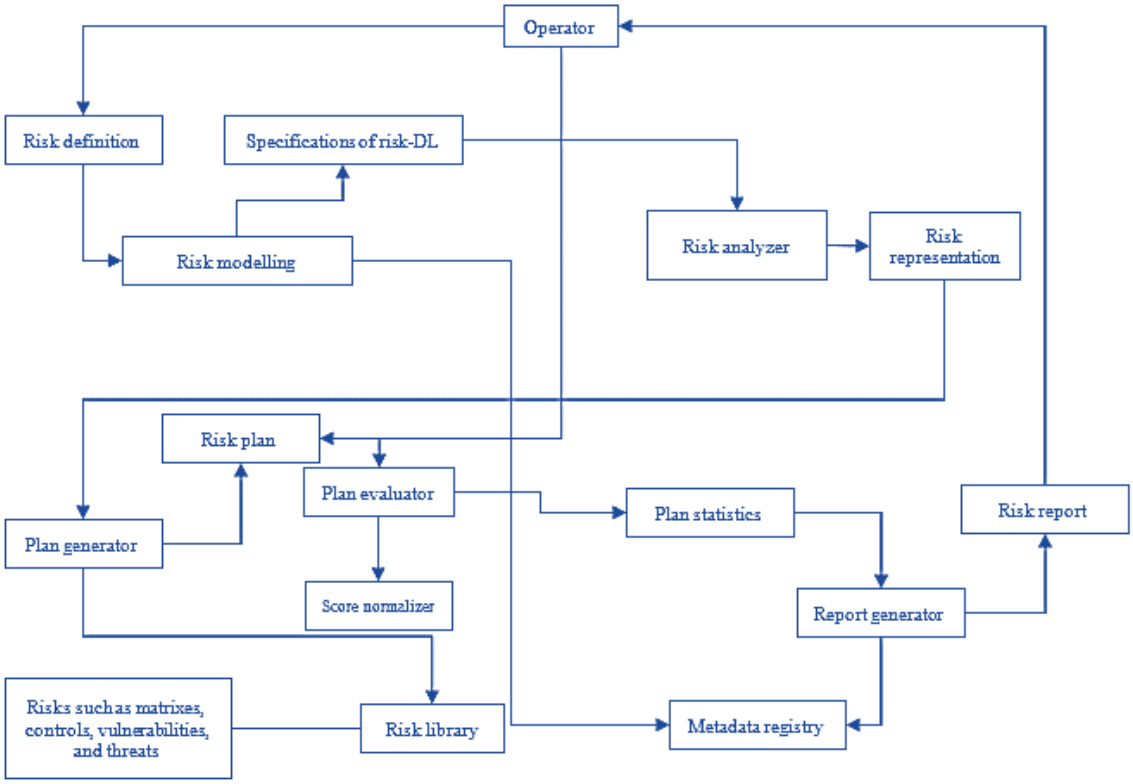

Fig 2. Architecture Overview

It is important to acknowledge that the suggested solution primarily emphasizes the risk aspect of the strategy outlined in section III. The connection between Enterprise Architecture (EA) and Governance is shown by the manner in which Risk-DL effectively associates risks with the specific artifacts outlined within the EA framework. Moreover, the manner in which risks are described facilitates interoperability, enabling the incorporation of risks from other organizational units. Typically, these risks are recognized in isolation, without any linkage to other risks within the business. This approach promotes a comprehensive perspective and cohesive risks management. The reporting systems provide measurements and reports that facilitate informed decision-making by assessing risks and providing alternative strategies to address them.

IV. CONCLUSIONS

Conventional risk management (RM) practices are characterized by compartmentalization, which hinders the exchange of risk-related information and the attainment of a comprehensive and up-to-date organizational perspective on risks. In recent times, a notable endeavor has been undertaken in the field of ERM. However, it is worth noting that existing solutions and frameworks in this domain do not conform to acknowledged and firmly established Enterprise Architecture (EA) frameworks such as the TOGAF or Zachman framework. Indeed, enterprise architecture (EA) descriptions provide a standardized approach for representing complex business systems, including many levels of abstraction ranging from strategic considerations to granular implementation specifics. This article provides a rationale for using enterprise architecture (EA) descriptions as a means of representing risk information. By employing EA descriptions, a more comprehensive comprehension of the value of assets may be achieved, particularly in relation to the components that may be impacted by the occurrence of certain risks. Indeed, it is worth noting that a risk that has a direct influence on an Enterprise Architecture (EA) component, such as a business process, will subsequently affect other components within the architecture, including other business processes and services.

In contrast, we examined the primary connections between the ISO 31000 RM and the TOGAF-ADM procedure, which serve as notable sources of reference within the domains of RM and EA, respectively. The present investigation has shown several interconnections among these activities, so providing a strong rationale for fostering collaborative endeavors aimed at attaining the same organizational goals. This article presents a proposed strategy for attaining a comprehensive and shared understanding of hazards throughout a company. The effectiveness of this approach is contingent upon the capacity of risk tools to interact with enterprise architecture (EA) specifications. This interaction involves using a metadata repository (MDR) and an XML-based language to convert various representations of risk into our proposed solution. In this manner, the suggested resolution is neither constrained by a particular range of tools, nor by a certain language for representing enterprise architecture artifacts (such as UML, BPMN, BPEL, etc.).

Data Availability
No data was used to support this study.

Conflicts of Interests
The author(s) declare(s) that they have no conflicts of interest.

Funding
No funding was received to assist with the preparation of this manuscript.

Competing Interests
There are no competing interests.

References

[1]. M. Zieba, S. Durst, and M. Gonsiorowska, "A New Critical Risk on the Block: Cyber Risks as an Example of Technical Knowledge Risks in Organizations," European Conference on Knowledge Management, vol. 23, no. 2, pp. 1269–1276, Aug. 2022, doi: 10.34190/eckm.23.2.654.
[2]. Q. Xu and K. Xu, "Mine safety assessment using gray relational analysis and bow tie model," PLOS ONE, vol. 13, no. 3, p. e0193576, Mar. 2018, doi: 10.1371/journal.pone.0193576.
[3]. N. A. Manab and N. A. A. Aziz, "Integrating knowledge management in sustainability risk management practices for company survival," Management Science Letters, pp. 585–594, 2019, doi: 10.5267/j.msl.2019.1.004.
[4]. C. Murphy and P. Gardoni, "The Role of Society in Engineering Risk Analysis: A Capabilities-Based Approach," Risk Analysis, vol. 26, no. 4, pp. 1073–1083, Aug. 2006, doi: 10.1111/j.1539-6924.2006.00801.x.
[5]. R. C. Rund, "International Organization for Standardization (ISO)," Journal of AOAC INTERNATIONAL, vol. 75, no. 1, pp. 196–199, Jan. 1992, doi: 10.1093/jaoac/75.1.196.
[6]. S. Kim and J. Yoo, "How Does LG Group Embed Enterprise Risk Management (ERM) System In Its Conglomerate Governance To Control Its Affiliated Firms' Risk Events?," Journal of Applied Business Research (JABR), vol. 33, no. 3, pp. 637–652, May 2017, doi: 10.19030/jabr.v33i3.9952.
[7]. D. J. Jurdi and S. M. AlGhnaimat, "The Effects of ERM Adoption on European Insurance Firms Performance and Risks," Journal of Risk and Financial Management, vol. 14, no. 11, p. 554, Nov. 2021, doi: 10.3390/jrfm14110554.
[8]. J. Celona, J. Driver, and E. Hall, "Value-driven ERM: Making ERM an engine for simultaneous value creation and value protection," Journal of Healthcare Risk Management, vol. 30, no. 4, pp. 15–33, 2011, doi: 10.1002/jhrm.20065.
[9]. R. Desir, J. Nam, and R. Pfeiffer, "Does Managerial Ability Improve the Predictability and Relevance of Earnings?," SSRN Electronic Journal, 2022, Published, doi: 10.2139/ssrn.4201596.
[10]. R. MacDonald and M. J. Moore, "The spot–forward relationship revisited: an ERM perspective," Journal of International Financial Markets, Institutions and Money, vol. 11, no. 1, pp. 29–52, Mar. 2001, doi: 10.1016/s1042-4431(00)00034-2.
[11]. A. Tola, "The Implementation of ERM in Non-Life Insurance Companies in Albania," European Journal of Business and Management Research, vol. 5, no. 6, Nov. 2020, doi: 10.24018/ejbmr.2020.5.6.570.
[12]. D. Currie and P. Williamson, "Will ERM entry make British companies more competitive?," Business Strategy Review, vol. 1, no. 3, pp. 1–16, Sep. 1990, doi: 10.1111/j.1467-8616.1990.tb00013.x.
[13]. R. Wijaya, "Analisis Perkembangan Return On Assets (ROA) dan Return On Equity (ROE) untuk Mengukur Kinerja Keuangan," Jurnal Ilmu Manajemen, vol. 9, no. 1, p. 40, Dec. 2019, doi: 10.32502/jimn.v9i1.2115.
[14]. Edi, Y. Z. Basri, and W. Arafah, "Ceo Characteristics, Firm Reputation And Firm Performance After Merger And Acquisition," Business: Theory and Practice, vol. 21, no. 2, pp. 850–858, Dec. 2020, doi: 10.3846/btp.2020.12782.
[15]. N. A. Bhat and S. U. Farooq, "An empirical evaluation of defect prediction approaches in within-project and cross-project context," Software Quality Journal, vol. 31, no. 3, pp. 917–946, Mar. 2023, doi: 10.1007/s11219-023-09615-7.
[16]. E. R. A. Suparto and L. Lukmandono, "Penilaian Maturity Level ERM (Enterprise Risk Management) Berbasis ISO 31000 : 2018," Prosiding SENIATI, vol. 6, no. 3, pp. 478–482, Jul. 2022, doi: 10.36040/seniati.v6i3.5079.
[17]. B. Masama, J. P. Bruwer, and L. Gwaka, "The feasibility of implementing the Committee of Sponsoring Organizations of the Treadway Commission enterprise risk management framework in South African small, medium and micro enterprises: a literature review," International Journal of Business Continuity and Risk Management, vol. 12, no. 3, p. 208, 2022, doi: 10.1504/ijbcrm.2022.125288.
[18]. S. Kulić, "COSO integrated framework and interactive connection elements of internal control," Ekonomski pogledi, vol. 20, no. 2, pp. 49–70, 2018, doi: 10.5937/ekopog1802049k.
[19]. E. Tambouris, M. Zotou, E. Kalampokis, and K. Tarabanis, "Fostering enterprise architecture education and training with the enterprise architecture competence framework," International Journal of Training and Development, vol. 16, no. 2, pp. 128–136, May 2012, doi: 10.1111/j.1468-2419.2012.00400.x.
[20]. S. Sumarni Hussein, M. Naz'ri Mahrin, and N. Maarop, "Sustainability through Innovations Of Enterprise Architecture (EA) in Public Sector's Management: Issues & Challenges," Journal of Southeast Asian Research, pp. 1–13, Jul. 2017, doi: 10.5171/2017.722027.
[21]. K. F. Best, "OASIS standards work," Markup Languages: Theory and Practice, vol. 3, no. 3, pp. 241–249, Dec. 2001, doi: 10.1162/109966201753750289.
[22]. H. Jung, "ISO/IEC 11179-based Blockchain System for Exchange Between CBDCs," The Journal of Korean Institute of Information Technology, vol. 18, no. 7, pp. 43–50, Jul. 2020, doi: 10.14801/jkiit.2020.18.7.43.