Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

The Missing Principles: A Systematic Literature Review of Risk Management Maturity Concepts

Eskil Kjemperud

eskil.kjemperud@dnv.com

University of South-Eastern Norway

Systematic Review

Keywords: systematic literature review, risk management, maturity assessment, risk process, risk principles, risk framework

Posted Date: November 25th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11592564/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Title Page

The Missing Principles: A Systematic Literature Review of Risk Management Maturity Concepts

Eskil Kjemperud[1,2], eskil.kjemperud@dnv.comPhone: +4791562856

[1] Institute for Nautical Operations, University of South-Eastern Norway, Raveien 215, 3184 Borre, Norway

[2] DNV, Veritasveien 1,1363 Høvik, Norway

Corresponding author

Eskil Kjemperud, Veritasveien 1, 1363 Høvik, email: eskil.kjemperud@dnv.com.

Author Note and funding:

This study is part of a PhD project sponsored by Det Norske Veritas (DNV) and the Norwegian Research Council (NFR).

Abstract

Research on risk management maturity assessments is growing because organizations need a documented record of how their ability to support risk management objectives evolves. However, it remains unclear whether they capture the full scope of risk management. This systematic literature review (SLR) synthesizes studies on risk management maturity assessment concepts, examining which risk management dimensions are emphasized by various maturity concepts, using ISO 31000 as the primary reference point. The literature search followed the PRISMA guidelines and identified 117 records from three major databases: Scopus, WoS, and EBSCO.

More than 94% of identified maturity concepts focused on governance, accountability, reporting systems, and risk management activities (in ISO 31000, this refers to the framework and process components). In contrast, only 2% of the maturity assessment concepts explicitly assessed risk management principles such as integration, adaptability, availability, and the effective use of information to support decision-making. Current maturity research emphasizes structural, procedural, and process aspects of risk management while paying limited attention to the principles that underpin the effectiveness of such an implementation.

This imbalance suggests that maturity assessments may overstate an organization's risk management capability by focusing on easily measurable aspects. A more balanced assessment of principles, framework, and process as interconnected risk management dimensions could improve maturity concepts to more accurately measure the performance of a risk management implementation.

Further empirical research is needed to clarify whether the observed gap reflects a true shortcoming in the proposed maturity concepts.

Keywords: systematic literature review, risk management, maturity assessment, risk process, risk principles, risk framework

Introduction

Risk has become a central concept in modern organizations, as evidenced by the widespread development and adoption of systematic risk management frameworks across industries. The field has advanced considerably over the past decades, with new theories, analytical methods, governance approaches, and practical tools for managing risk [1], [2], [3].

Alongside building knowledge on risk management, the complexity of the problems these systems (guidelines, frameworks, and methodologies) must solve is increasing due to technological advancement, business requirements, and environmental factors [2], [4], [5]. The "goodness" of a risk management system is difficult to measure [6], and many attempts have been made to find a solution to this issue; this is why maturity measurements for risk management implementations (frameworks, models, and concepts) have been part of the research since structured and centralized risk management emerged [7].

The institutionalization of risk management through international standards—for example, ISO 31000, enterprise risk management frameworks such as COSO ERM, and more specific frameworks such as NIST Cybersecurity Framework—reflects the importance attributed to risk management in organizations [8], [9]. At the same time, risk remains a multifaceted concept whose meaning varies across disciplines and organizational contexts [10].

The typical method for measuring maturity and performance is within an audit framework, such as an ISO audit. For example, in maritime, there is a concept called "a seamless audit," where the ISM Code (statutory company audit), ISO 27001, and ISO 9001 are audited within the same scope (and time), and ISO 31000 guidelines are used as the foundation for the risk management part of the assessment.

This indicates that risk management is a universal concept across various auditable schemes, though, depending on the organization, its implementation varies through a tailored, structured approach for the management of uncertain events and conditions, thereby supporting informed decision-making and helping organizations achieve their objectives [1].

The ISO 31000 and the other aforementioned guidelines, frameworks, and systems do not provide a specific implementation blueprint for organizations; one size does not fit all. Rather, they support and incorporate risk management into an organization's overall management system, leaving the individual organization to decide how to operate within that system [11]. This is why a maturity concept is perceived as extremely valuable, even though there remain several critiques regarding how it is implemented, especially in terms of organizational maturity.

Risk frameworks rely on three core dimensions, with ISO 31000 exemplifying a holistic risk management approach by dividing it into framework, principles, and process. This aligns with ISO's role in providing guidelines, simplifying complex ideas, and supporting cross-disciplinary risk science discussions. For this review, ISO 31000 is a reference point for understanding the components of risk management—namely, framework, principles, and process, as seen in Figure 1.

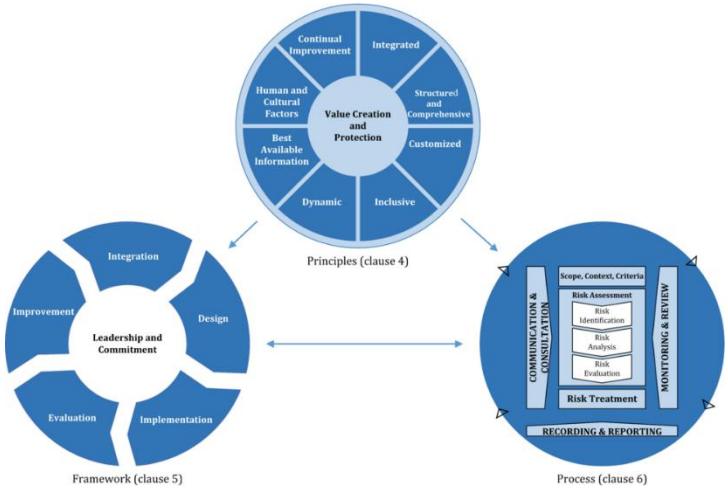


Figure 1: ISO 31000 framework for risk management showing the Framework (clause 5), Principles (clause 4), and the Process (clause 6). It is widely adopted and shapes the foundation for audits, risk models, and risk management documentation [1].

First, take ISO 31000 as an example: A concern within the organization, from its own review process, identified several areas where users require additional guidance. The ISO/TC 262 Task Group 5 report concluded that, as the top priority, the standard needs to "[p]rovide further guidance on the principles" as well as stronger guidance on implementation, organizational integration, risk culture, risk appetite, emerging risks, risk quantification, and practical examples [11]. The report also called for

clarification of the risk definition itself, suggesting that important aspects of the standard remain open to interpretation and may contribute to inconsistent implementation across organizations.

This can be seen as ISO's attempt to clarify the vague language that allows for multiple interpretations of the guidelines [12]. Effective implementation of a risk management system requires consistent understanding of these guidelines, and a risk management maturity concept could be part of this alignment across industries.

A second controversy relates to the definition of risk itself. ISO 31000 defines risk as the "effect of uncertainty on objectives," yet scholars argue that risk remains a contested concept and that different interpretations of uncertainty, probability, and consequences can lead to different risk management practices. Some researchers question whether ISO 31000 and similar frameworks adequately address highly uncertain, complex, or unforeseen events, prompting increased interest in complementary concepts such as resilience and adaptive management [1], [12], [13], [14].

Despite these criticisms of risk management frameworks, as well as in this review, which has used ISO 31000 guidelines as a backdrop, maturity models have been seen as an antidote to these challenges and as a concept for aligning risk management ambitions with organizational practice

Risk Maturity Models (RMMs), as introduced by Hillson [15], offer a structured approach for organizations to evaluate and enhance their risk management skills across four maturity levels. Later models expanded this idea by adding maturity attributes and levels, such as those developed by Hopkinson [16]. This concept of maturity has been adapted into various frameworks, notably within safety science, including much research on the very similar concept of Safety Culture maturity [17].

Risk maturity frameworks operationalize certain aspects of risk management theory into measurable organizational capabilities. As a result, examining how maturity is assessed may reveal which aspects of risk management are currently emphasized in both theory and practice, linking risk science with practice. The dimensions included in maturity models can therefore be viewed as indicators of the maturity of the "risk theory implemented into practice." In this sense, maturity frameworks offer a useful lens for understanding and describing how a risk management concept is translated into an organizational

practice [7]. As both Hillson and Hopkinson note, maturity models can show which parts of the risk definition are and are not included in the implementation of risk management.

This review examines contributions to developing maturity concepts for the implementation of future risk management frameworks, particularly as emerging technologies challenge our understanding of decision-making under uncertainty. As a result, risk management has become increasingly intertwined with safety management systems and procedural adaptations, resilience engineering, software engineering, and organizational learning, showing a need for risk management maturity concepts to span these areas to meet implementation objectives, and not just compliance checkboxes.

Risk management is more than compliance with standards, guidelines, and frameworks for risk management [10]. The availability of risk-related information has significantly increased since the introduction of Industry 4.0 and the digital transformation, both due to the availability of data and information and to the introduction of new technologies [18], [19].

These technological advances create opportunities for more dynamic and informed decision-making, challenging traditional risk management approaches often designed around periodic assessments and static reporting structures. Despite extensive research on decision-making under uncertainty and risk-informed decision support [2], [20], relatively little work has been found on whether this has been integrated into risk management maturity frameworks.

Therefore, the research question has become: What are the different research directions on risk management maturity concepts across industries?

This systematic literature review (SLR) addresses this question by synthesizing research on risk management maturity concepts across industries and professional domains. The review reveals differences in framework features, identifies research gaps, and emphasizes the link between maturity frameworks and ISO 31000 risk elements. It aims to guide future research and support the development of more holistic risk management maturity concepts.

This literature review of risk management maturity frameworks helps determine their effectiveness and initiates a discussion about what needs strengthening. For example, consider a Hazard

Identification Workshop (HAZID), a common way to work through the process part of ISO 31000. If the maturity performance concept only measures things such as a HAZID workshop within the process part and not the framework and the principle parts of ISO 31 000, a potential risk could easily "slip within the cracks of the safety crystal ball" (with reference to Rea's safety manifesto [6]). The review also discusses the balancing of a holistic risk management implementation in the context of risk management maturity concepts.

Methods

This systematic review followed a meta-analysis, including Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure transparency and rigor [21], [22]. Searches in Scopus, Web of Science (WoS), and Elton B. Stephens Company Academic Search Elite (EBSCO) included all years; no time restrictions were applied because risk management maturity is a niche field wherein early publications remain influential. The time frame covered all years up to the date of record extraction, 3 September 2026. Conference proceedings were included as they often contain emerging concepts that may develop into more established research.

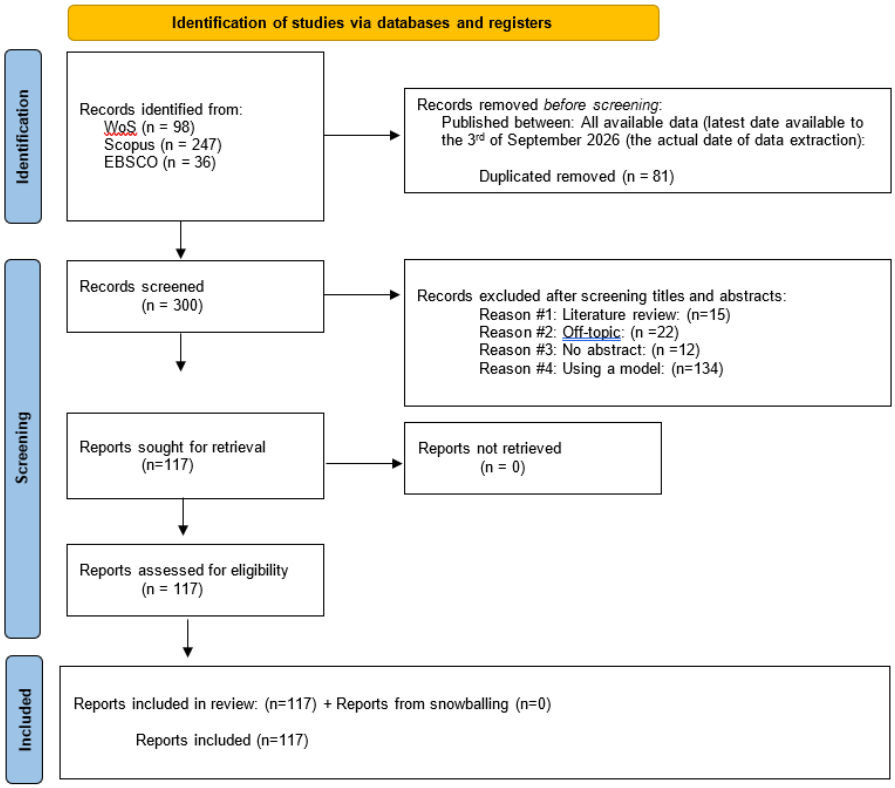
The search strategy was developed through an extensive review across databases and Google Scholar and revealed that reports on maturity concepts often use recognizable terminology in their titles. Risk and safety are closely related concepts, as reflected in their common treatment in risk literature, where terms such as "framework," "model," and "concept" are used interchangeably. The final search string became:

(TITLE(risk OR safety) AND TITLE(maturity OR readiness) AND TITLE(framework OR concept OR model))

This search strategy was designed to capture research on maturity frameworks. Initial testing showed relevant reports consistently contained these terms, especially in titles. Snowballing supported its effectiveness and yielded no additional relevant reports.

The initial search returned a large but manageable dataset of 322 records. After removing duplicates (116), records were screened by title and detailed abstract reading. As shown in Table 1, 56 records were removed during screening: 15 were removed because they were literature reviews; 22 were off topic, such as different definitions of maturity; 12 had no available abstracts; and 134 addressed the use of existing models, safety management, or organizational assessment. The remaining 117 reports underwent full-text review based on predefined criteria.

Table 1: Overview of a simplified table, following the PRISMA guidelines [21]



Data extraction was conducted systematically for each report. Information collected included industry sector, risk domain, and—most importantly—the maturity dimensions, assessment approach, concept characteristics, and conclusions and limitations. This review is grounded in how each concept aligned with the three core dimensions of ISO 31000: principles, framework, and process, as seen in Figure 1. This classification enabled the comparison of maturity models across industries and professional domains.

The analysis employed qualitative synthesis and comparative coding to identify recurring patterns [23], the foundations for the concepts, models, and innovation, and linked them to appropriate industry and risk topology. The review focused on the generalities and qualities that shape performance, rather than on isolated or specific attributes.

The systematic review provided clear, simple rules and tags that make the research simple for others to reconstruct. Maturity frameworks linked to governance typically addressed ownership and asked how the organization is set up to handle approvals, responsibilities, procedure changes, etc. The maturity model typically used questionnaires or, for example, the use of the Delphi method (interviews) as a basis for the arguments and measurements. The results were often linked to safety culture and improvement steps that align with social and psychological parameters. The typical process maturity frameworks focused on how risks are identified, analyzed, and communicated. These maturity models were often linked to matrices and the infamous risk process steps in clause 6 of ISO 31000 (see Figure 1). Maturity concepts linked to principles often focused on how data could be available to a specific decision-maker and what they needed to capture to enable particular outcomes. These models were either cyber-physical with sensors and IoT or shaped by psychological theories.

Results

The review identified 117 risk management maturity measurement concepts across a range of industries. Figure 2 presents the distribution of maturity concepts across the ISO 31000 dimensions. Concepts focused on the framework dimension accounted for 52%, while those focused on the process dimension accounted for 29%. An additional 13% of concepts were classified as dual focus on both the framework and process dimensions. Concepts with an associated focus on principles represented 2% as a standalone category, while concepts with a focus on principles and process and framework and principles accounted for 2% each. Overall, risk management maturity assessment focuses primarily on the ISO 31000 framework and process dimensions.

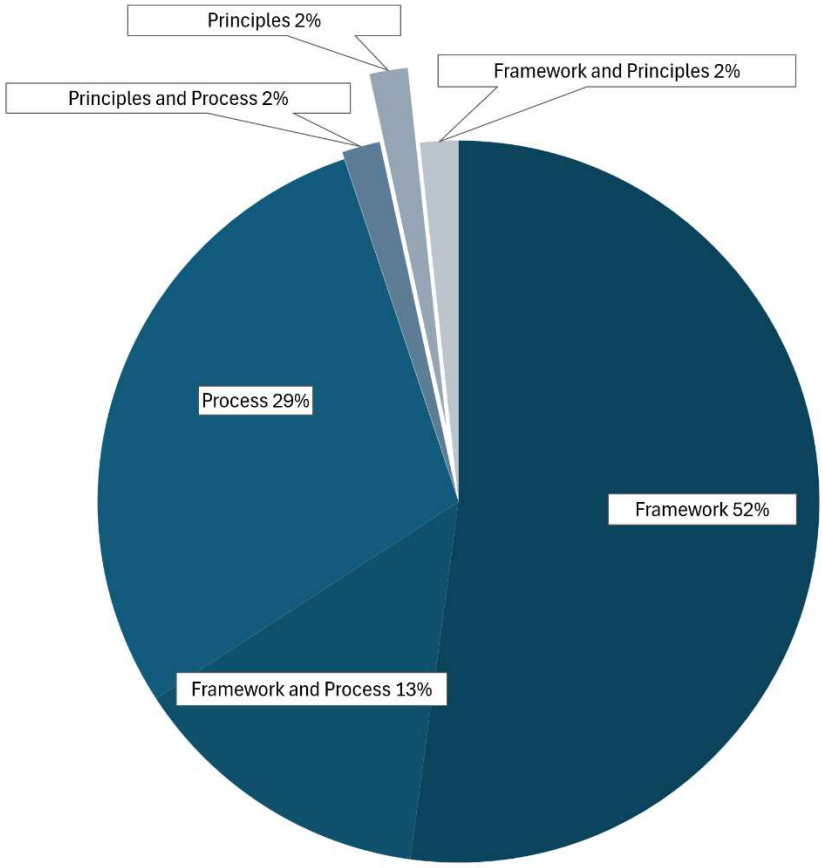


Figure 2: The reports distributed across the three dimensions for risk management based in ISO 31000: process, framework and principles, showing that more than 94% of the reports cover the maturity performance framework, models, and concepts for the framework and process dimensions.

As shown in Table 2, the Information Technology sector category dominated with 31 reports. Eighteen reports focused on the framework dimension of risk management maturity assessment. Eight reports had a process focus. The Construction Industry category had 21 reports, of which 16 were classified under the framework dimension, 3 with a process focus, and 2 with a flavor of both. The Healthcare category had 14 reports and showed a broader distribution across dimensions, including reports addressing frameworks, processes, and combinations involving maturity concepts.

Table 2: The industry topology as viewed through the lens of maturity concepts, emphasizing framework, process, and principles

Industry segments / Maturity focus	Framework	Framework and Process	Process	Principles and Process	Principles	Framework and Principles	Total
Information Technology	18	3	8	1	1		31
Construction	16	2	3				21
Healthcare	3	4	6			1	14
Regulatory, Research and Organizational	10	2	1		1		14
Public Services and Military, Defense, Police	4	1	5			1	11
Energy and Oil and Gas	1	1	5				7
Maritime	2	1	2	1			6
Mining	4		1				5
Aviation	1	1	1				3
Food and Agriculture			2				2
Supply Chain	2						2
Process Industry		1					1
Total	61	16	34	2	2	2	**117**

The category including Regulatory, Research, and Organizational contexts also accounted for 14 reports, largely centered on framework-based approaches. Public Services, Military, Defense, and Police sectors accounted for 11 reports, again with a strong focus on frameworks and processes.

Other industry categories were less represented. Energy, Oil and Gas accounted for 7 reports, while the Maritime sector accounted for only 6 reports. In summary, maturity assessment of risk management concepts is widely adopted across industries.

Discussion

Overall, research on maturity risk management concepts is increasing. A quick search in the Scopus database shows that the number of published articles is growing (from 12 reports in 2025 to 25 in 2026) across multiple sectors, including maritime, aviation, healthcare, construction, oil and gas, cybersecurity, and finance.

This review was motivated by this growing interest in how industries measure risk management maturity, which dimensions receive the most attention, and where key research gaps remain. By synthesizing the literature across industries, the findings show greater emphasis on governance

frameworks and risk management processes, while comparatively little attention is paid to the measurement of risk management principles. Consequently, most maturity concepts assess whether risk management systems exist rather than whether they improve decision quality, organizational resilience, and uncertainty management. As a result, the literature underrepresents the link between risk management systems and operational realities, including how data are collected, interpreted, and used to support decisions. This suggests a "missing leg of a three-legged stool" of risk management maturity that only a few risk management maturity measurement concepts have investigated.

Risk Management Framework Maturity Assessments Are Dominating

The reviewed literature indicates a measurable-object bias within risk management maturity research. Most maturity concepts assess aspects of risk management that can be readily documented, audited, benchmarked, and quantified. This is described by sectors, and in particular in healthcare [24], [25], [26]. Consequently, most concepts focus on the framework and process dimensions described in ISO 31000, including governance structures, risk assessment procedures, reporting mechanisms, organizational roles, performance indicators, and compliance activities.

In contrast, the principles dimension receives substantially less attention. Principles such as decision quality, information availability, adaptability, human and organizational factors, communication effectiveness, and the integration of risk into decision-making are often embedded—or hidden without any effective implementation strategy—within framework or process categories rather than assessed as independent maturity constructs.

One concept illustrates the measurable-object orientation found in many risk management maturity concepts. Designed as a self-questionnaire, assessment focuses on whether performance measures are collected, analyzed, and used to characterize the risk management process. While such questions might provide evidence of governance and process control, they primarily evaluate the existence of organizational mechanisms rather than the quality of decision-making, interpretation of information, or the effectiveness of risk-informed actions [27]. Consequently, the principles dimension of risk management receives less explicit attention than framework and process dimensions. This creates

conceptual overlap between the maturity dimensions and may limit the assessment of the actual effectiveness of risk management. This is described in theoretical risk frameworks and the broken link to safety practice [6], [10].

The distribution of maturity concepts suggests that researchers and practitioners generally favor tangible, observable attributes over more abstract characteristics related to organizational behavior and decision-making. As a result, maturity assessments often describe the existence of risk management systems rather than the extent to which those systems improve organizational resilience and support informed decisions.

The Missing Principles

While the results show that both framework and process maturity measurement are part of our research agenda, they also reveal that risk management principles lack maturity measurement.

Consider a vessel where risk analysis is performed based on operational data generated onboard, for example from a Plan Maintenance System (PMS). The analyst is frequently located onshore and interprets data received from the vessel. However, this information is often available at intervals that do not match the sampling frequency needed to detect the development of specific failure modes, especially weak signals. As a consequence, even when the analysis process is robust and the organization clearly defines governance and ownership of risk management for the identified risks (the framework), a critical challenge remains. The final decision-makers are often on-board personnel who need timely access to decision support (e.g., analytical results) to make operational risk management decisions. When information reaches them too late, the analysis becomes obsolete. In other words, if the right data are not available to the right person at the right time, situational awareness can be degraded.

Updated situational awareness and effective risk management go beyond data and information availability; interpretability and predictability are equally important. Risk management effectiveness requires data and information to be accessible, comprehensible, and capable of supporting future states [12], [28]. Measuring the quality and effectiveness of a risk management implementation is difficult

without a maturity measurement concept for the principles, alongside the usual suspects: framework and process.

Furthermore, from a theoretical risk management perspective, these aspects remain relatively underresearched within the risk management literature, even though there is research that suggests solutions, such as the concept of justified belief [29] as part of addressing decision-making in a high-uncertainty environment.

Another possible explanation for why the focus has tended to be on two of the three parts, is that the risk owners—those more removed from the real risk (and hazard of the potential accident) and those who make the final economic decisions—are much more concerned about their part of the risk management overview, and that is covered more in the risk framework (clause 5). They are the ones who pay the bills and drive the business's profits, which is why they have been overly interested in these maturity-measurement concepts; hence, they are overrepresented in research.

For the process part (clause 6), technical specialists, such as safety scientists, dominate because this is where they can apply their tools and methods. They use risk matrices, build bowties, run a HAZID workshop, and so on. The wider research community also focuses on tools and methods which are perceived as a challenge in terms of a lack of empirically driven research—for example, the reification challenge and the purely frequentist view of risk [6], [29], [30].

Operators at the sharp end would naturally be more interested in the principles of risk management, since this is where results from theories, assumptions, models, and tools meet reality, and decisions must be made to ensure that a catastrophic event does not play out, such as the closure of the Suez Canal or a collision with a large tank vessel. These events can be dismissed as Black Swan events or freak incidents, but another way to understand these accidents is to look at what data and information must be available, interpretable, and predictive to support better decision-making in high-risk scenarios. A laminated picture of a “fire in the engine room” bowtie at head office has little value when a fire is slowly developing onboard a vessel in the middle of the Atlantic Ocean and the crew suffer from alarm and reporting fatigue and are unable to detect the growing flames [31], [32], [33].

The few reports on principle-oriented maturity assessment of risk management systems clearly demonstrate their focus on supporting effective, risk-informed decision-making. As an example, the report on Digital Forensic Readiness in IoT [34] focuses on preparedness, contingency planning, and organizational readiness. The risk assessment model emphasizes predetermining device capabilities, incident procedures, and forensic requirements before adverse events occur. Rather than concentrating solely on governance structures or assessment processes, the model addresses foundational organizational capabilities required to respond effectively to uncertainty.

Similarly, the report on Risk Assessment Framework for Cyber Resilience of Smart Ships [35], integrates IACS UR E26/E27, IEC 62443, and NIST SP 800-160 through a layered maturity architecture. The framework combines risk quantification, asset criticality assessment, threat likelihood evaluation, and real-world testbed validation. While the model includes traditional process elements, it also shows how emerging technologies can support continuous situational awareness and decision-making through dynamic risk monitoring, attack detection, and cyber resilience measurement.

Another example is the report, Advancing Safety Analytics: A Diagnostic Framework for Assessing System Readiness Within Occupational Safety and Health [36], which focuses on organizational preparedness for safety analytics. The report states: “The readiness framework is designed to give organizations an understanding of their current capabilities,” and they propose this to be done through four prerequisites for analytics readiness: data quality; organizational norms regarding data management; supporting technological infrastructure; and measurement culture. These dimensions extend beyond traditional risk processes and highlight the importance of information quality and human–technology interaction in supporting effective decision-making.

In sum, the discussion suggests that while risk management maturity research has extensively developed assessments of framework and process capabilities, the principles that determine whether risk information is available, interpretable, predictive, and effectively integrated into operational decision-making remain comparatively immature and underrepresented in both theory and practice.

Limitations

An SLR has limitations by design, such as the framing of the search string. As explained, much time was spent in reviewing different search results to test which search terms would best fit. The core challenge is that words have different meanings across industries, and abstract search terms such as "framework," "concept," and "model" made this even more difficult. While ISO 31000's broad acceptance across industries provided common ground and may have helped establish a strong search string, reports that used alternative terminology or interpreted the terminology differently may have been missed as a consequence.

On the same theme of interpretation, classifying findings according to the ISO 31000 dimensions of framework, process, and principles requires significant interpretation. ISO 31000 provides a proven analytical structure for maturity assessment analysis [27], but the boundaries between the dimensions are subject to interpretation, as discussed in risk science research [1], [12]. This means that the results carry subjective components from the analysis of the reports and might change depending on the researcher.

A final limitation is that the review focused on conceptual synthesis rather than empirical validation. Consequently, the findings identify patterns and gaps within the literature but do not demonstrate causal relationships between specific maturity dimensions and organizational performance. As a result, the conclusions regarding the underrepresentation of principles within a maturity concept should be viewed as indicative rather than definitive.

Conclusion and Further Research

This SLR shows that the framework dimensions—meaning, design, implementation, evolution, and organizational structures—dominate, with 52% of the reports focused on this part of risk management system maturity measurement. Just under one third (29%) of the reports had a focus on measuring the process dimension of the maturity of the risk management systematics, and 13% had a dual focus on framework and process. This means that 94% of reports do not address the maturity measurement of the principles of risk management systematics.

This suggests that most maturity concepts evaluate organizational structures, governance arrangements, reporting mechanisms, risk assessment activities, and operational procedures because they

are easier to document, audit, benchmark, and quantify through maturity scales, questionnaires, interviews, and performance indicators.

As a result, maturity assessments have largely evolved into tools for evaluating the existence of risk management systems and processes rather than the underlying conditions that determine whether these systems support effective decision-making, the principles in ISO 31000. Consequently, assessments often absorb principles into framework or process evaluations rather than evaluating them independently. This creates a conceptual gap between what ISO 31000 identifies as the foundation of effective risk management and what existing maturity concepts actually measure.

This review does not suggest that the current focus on framework and process dimensions is incorrect. Rather, it highlights an observable pattern in the literature and identifies underexplored areas. It remains unclear whether increased attention to principle-based maturity assessments would improve maturity evolution within an organization or simply add complexity without measurable benefits. Ultimately, the review suggests that future maturity concepts may benefit from a more balanced approach that treats principles, frameworks, and processes as interconnected dimensions of risk management rather than largely independent areas of assessment.

Further empirical research is needed to clarify whether the observed gap reflects a true shortcoming of current maturity concepts or a deliberate focus on measurable organizational traits. Many reports suggest that their maturity concepts are more a contribution to a theoretical foundation rather than something to be used, since they lack empirical testing, as seen in this example from a maturity concept for maritime administrations: “the model has not undergone explicit testing” [9].

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the author used Copilot in order to improve the readability and language of the manuscript. After using this tool/service, the author(s) reviewed and edited the content as required, taking full responsibility for the content of the published review article.

Data availability statement

The materials supporting the findings of this review are available from the corresponding author upon reasonable request. These materials include the completed PRISMA 2020 checklist and flow diagram, full search strategies for all databases consulted, screening and eligibility records (inclusion and exclusion decisions), data extraction forms, and synthesis tables used in the analysis. These materials are provided to enable verification of the review methodology, study selection process, and reported findings.

References

[1] S. H. Björnsdóttir, P. Jensson, R. J. de Boer, and S. E. Thorsteinsson, "The Importance of Risk Management: What is Missing in ISO Standards?," *Risk Anal.*, vol. 42, no. 4, pp. 659–691, 2022, doi: 10.1111/risa.13803.

[2] F. Goerlandt and J. Li, "Forty Years of Risk Analysis: A Scientometric Overview," *Risk Anal.*, vol. 42, no. 10, pp. 2253–2274, 2022, doi: 10.1111/risa.13853.

[3] J. O. Zinn and P. Taylor-Gooby, "The Challenge of (Managing) New Risks," *Risk Soc. Sci.*, p. 54, Nov. 2006.

[4] E. Zio, "The future of risk assessment," *Reliab. Eng. Syst. Saf.*, vol. 177, pp. 176–190, Sep. 2018, doi: 10.1016/j.ress.2018.04.020.

[5] M. Ylönen and T. Aven, "A framework for understanding risk based on the concepts of ontology and epistemology," *J. Risk Res.*, vol. 26, no. 6, pp. 581–593, Jun. 2023, doi: 10.1080/13669877.2023.2194892.

[6] A. Rae, R. Alexander, and J. McDermid, "Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment," *Reliab. Eng. Syst. Saf.*, vol. 125, pp. 67–81, May 2014, doi: 10.1016/j.ress.2013.09.008.

[7] M. Wieczorek-Kosmala, "Risk management practices from risk maturity models perspective," *J. East Eur. Manag. Stud.*, vol. 19, no. 2, pp. 133–159, 2014.

[8] U. Beck and U. Beck, *Risk society: towards a new modernity*, Repr. in Theory, culture and society. London: Sage, 2009.

[9] V. Laine, *Risk management framework for maritime authorities: Concepts, processes and maturity*. Aalto University, 2025. Accessed: Apr. 19, 2026. [Online]. Available: https://aaltodoc.aalto.fi/handle/123456789/138910

[10] T. Aven, "Risk literacy: Foundational issues and its connection to risk science," *Risk Anal.*, vol. 44, no. 5, pp. 1011–1020, 2024, doi: 10.1111/risa.14223.

[11] "SO 31000: Risk Management – Guidelines Final Report of Task Group 5 Assess the market acceptance challenges and next steps for ISO 31000 Technical Committee 262 Task Group 5 August 16, 2023." Technical Committee 262, 2023. [Online]. Available: https://committee.iso.org/files/live/sites/tc262/files/ISO%2031000-2018%20Risk%20Management%20Guidelines%20-%20Technical%20and%20Market%20Analysis%20with%20Proposed%20Next%20Steps%20230816A.pdf

[12] T. Aven, "The flaws of the ISO 31000 conceptualisation of risk," *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, vol. 231, no. 5, pp. 467–468, Oct. 2017, doi: 10.1177/1748006X17690672.

[13] G. Purdy, "ISO 31000:2009—Setting a New Standard for Risk Management," *Risk Anal.*, vol. 30, no. 6, pp. 881–886, Jun. 2010, doi: 10.1111/j.1539-6924.2010.01442.x.

[14] M. Leitch, "ISO 31000:2009—The New International Standard on Risk Management.," *Risk Anal. Int. J.*, vol. 30, no. 6, p. 887, Jun. 2010, doi: 10.1111/j.1539-6924.2010.01397.x.

[15] D. Hillson, “Towards a Risk Maturity Model.” The International Journal of Project and Business Risk Management, 1997. [Online]. Available: https://risk-doctor.com/wp-content/uploads/2020/06/RMM-IJPBRM-Mar97.pdf
[16] A. Hopkins, “Risk-management and rule-compliance: Decision-making in hazardous industries,” *Saf. Sci.*, vol. 49, no. 2, pp. 110–120, Feb. 2011, doi: 10.1016/j.ssci.2010.07.014.
[17] A. Rae, R. Alexander, and J. McDermid, “Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment,” *Reliab. Eng. Syst. Saf.*, vol. 125, pp. 67–81, May 2014, doi: 10.1016/j.ress.2013.09.008.
[18] M. Braglia, R. Gabbrielli, L. Marrazzini, and L. Padellini, “Key Performance Indicators and Industry 4.0 – A structured approach for monitoring the implementation of digital technologies,” *Procedia Comput. Sci.*, vol. 200, pp. 1626–1635, Jan. 2022, doi: 10.1016/j.procs.2022.01.363.
[19] S. Kraus, S. Durst, J. J. Ferreira, P. Veiga, N. Kailer, and A. Weinmann, “Digital transformation in business and management research: An overview of the current status quo,” *Int. J. Inf. Manag.*, vol. 63, p. 102466, Apr. 2022, doi: 10.1016/j.ijinfomgt.2021.102466.
[20] C. Reale *et al.*, “Decision-Making During High-Risk Events: A Systematic Literature Review,” *J. Cogn. Eng. Decis. Mak.*, vol. 17, no. 2, pp. 188–212, Jun. 2023, doi: 10.1177/15553434221147415.
[21] M. J. Page *et al.*, “The PRISMA 2020 statement: an updated guideline for reporting systematic reviews,” Mar. 2021, doi: 10.1136/bmj.n71.
[22] M. Gusenbauer and S. P. Gauster, “How to search for literature in systematic reviews and meta-analyses: A comprehensive step-by-step guide,” *Technol. Forecast. Soc. Change*, vol. 212, p. 123833, Mar. 2025, doi: 10.1016/j.techfore.2024.123833.
[23] J. Saldaña, *The coding manual for qualitative researchers*. Los Angeles, Calif: Sage, 2009. [Online]. Available: https://www.daneshnamehicsa.ir/userfiles/files/1/%D8%B3%D8%A7%D9%84%D8%AF%DB%8C%D9%86%D8%A7.pdf
[24] S. Dekker, “Safety Theater: Where your accidents hide in the green.” 2024.
[25] S. Dekker, *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems*, 0 ed. CRC Press, 2016. doi: 10.1201/9781315257396.
[26] M. Power, “The risk management of nothing,” *Account. Organ. Soc.*, vol. 34, no. 6, pp. 849–855, Aug. 2009, doi: 10.1016/j.aos.2009.06.001.
[27] D. Proença, J. Estevens, R. Vieira, and J. Borbinha, “Risk Management: A Maturity Model Based on ISO 31000,” in *2017 IEEE 19th Conference on Business Informatics (CBI)*, Jul. 2017, pp. 99–108. doi: 10.1109/CBI.2017.40.
[28] A. Olechowski, J. Oehmen, W. Seering, and M. Ben-Daya, “The professionalization of risk management: What role can the ISO 31000 risk management principles play?,” *Int. J. Proj. Manag.*, vol. 34, no. 8, pp. 1568–1578, Nov. 2016, doi: 10.1016/j.ijproman.2016.08.002.
[29] T. Aven, “On the gap between theory and practice in defining and understanding risk,” *Saf. Sci.*, vol. 168, p. 106325, Dec. 2023, doi: 10.1016/j.ssci.2023.106325.
[30] A. John Rae and R. D. Alexander, “Probative blindness and false assurance about safety,” *Saf. Sci.*, vol. 92, pp. 190–204, Feb. 2017, doi: 10.1016/j.ssci.2016.10.005.
[31] M. Hravnak *et al.*, “A call to alarms: Current state and future directions in the battle against alarm fatigue,” *J. Electrocardiol.*, vol. 51, no. 6, Supplement, pp. S44–S48, Nov. 2018, doi: 10.1016/j.jelectrocard.2018.07.024.
[32] F. Crestelo Moreno, V. Soto-López, J. A. García Maza, and M. Sernaglia, “Fatigue as a latent risk factor in maritime safety systems: A systematic review and implications for reliability analysis,” *Reliab. Eng. Syst. Saf.*, vol. 267, p. 111930, Mar. 2026, doi: 10.1016/j.ress.2025.111930.
[33] A. Rajapakse and G. R. Emad, “Fatigue, an unsolved puzzle that continues contributing to accidents at sea,” *Mar. Policy*, vol. 155, p. 105745, Sep. 2023, doi: 10.1016/j.marpol.2023.105745.
[34] A. D. Forfot and G. Østby, “Digital Forensic Readiness in IoT - A Risk Assessment Model,” in *Intelligent Technologies and Applications*, S. Yildirim Yayilgan, I. S. Bajwa, and F. Sanfilippo,

Eds., Cham: Springer International Publishing, 2021, pp. 53–64. doi: 10.1007/978-3-030-71711-7_5.

[35] J. Lim, W. Lee, and Y. Yoo, "Risk assessment framework for cyber resilience of smart ships: A maturity model integrating IACS UR E26/E27 with testbed validation of the baseline and advanced tiers," *Int. J. Crit. Infrastruct. Prot.*, vol. 54, p. 100875, Sep. 2026, doi: 10.1016/j.ijcip.2026.100875.

[36] M. E. Ezerins, T. D. Ludwig, T. O'Neil, A. M. Foreman, and Y. Açıkgöz, "Advancing safety analytics: A diagnostic framework for assessing system readiness within occupational safety and health," *Saf. Sci.*, vol. 146, p. 105569, Feb. 2022, doi: 10.1016/j.ssci.2021.105569.

Ethical Approval

This article does not contain any studies with human participants performed by any of the authors.

Informed Consent

This article does not contain any studies with human participants performed by any of the authors.