Bibliometric analysis and comparison of current risk management methodologies in accordance with project management principles

Jon Arteta Ibinarriaga

Faculty of Engineering Bilbao, University of the Basque Country, Ingeniero Torres Quevedo Plaza, 1, 48013 Bilbao, Biscay

Abstract

The study takes a look into methodologies offering a holistic approach to risk management, assessing their level of alignment with project management principles, and pinpointing gaps in terms of managerial risk.

The scope of the research covers project management, project management principles, risk management methodologies, and comparative processes, providing the study with sufficient background to identify gaps, priorities, focus areas, and research needs.

In consequence, the analysis was able to identify that, in average, risk management methodologies integrate about half (i.e. 58.3%) of the concepts defined by project management principles. However, complex and interconnected risks tend to be left aside, including the ones associated to the human factor and business interrelations.

Furthermore, risks associated to change, adaptability, and the managerial capabilities of the workforce still require further research and development.

In the overall, risk management methodologies tend to consider project management principles throughout their content. However, further alignment is required.

Keywords

Risk management, Risk assessment, Risk mitigation, Project management principles.

1 Introduction

Risk management may be referred to the process of identifying, assessing, and controlling the existing uncertainties, hazards and threats surrounding projects and organisations. It involves planning and measuring the likelihood for events to occur, so project managers can monitor and control their consequences.

Risks may stem from a wide variety of sources, including financial and economic uncertainties, legal liabilities, management errors, accidents, or even natural disasters. The outcomes derived from these risks could be small and isolated, as well as widespread and large, which may result in catastrophic consequences if counter-action and planning is avoided.

Within a project management context, the dynamic and ever-changing environments surrounding project work tend to generate risks both in teams and organisations. Consequently, defining an effective risk management strategy proves essential to enhance the chances of project success, clear out cascading impacts, and protect an organisation's strategic goals. Nevertheless, today´s risk management strategies seem to be oriented towards operations, asset security, and error avoidance, leaving aside the risks associated to the management side on itself.

Understanding the gaps in this particular area would be crucial to underline the work in need to be done for the definition of an effective risk management strategy. Therefore, getting to know the strengths, weaknesses, and orientation of today's most utilised risk assessment, management and planning strategies would seem key to reach that goal.

The results of this study will analyse the main features and characteristics of most utilised risk management methodologies to provide a clear view on the level of integration of project management principles in risk related studies. The focus will be on those methodologies that apply a holistic approach to risk management. Relevant knowledge gaps affecting the risk assessment and mitigation processes will also be addressed.

This paper is structured as follows. The next chapter compiles topic-relevant information on project management principles and risk management methodologies, summarising the reviewed content. The third section, on the other hand, presents the applied methodology, including the scope, the analytical and comparative approach, and data sources. In the fourth section results are presented based on the gathered data, and finally, the fifth section includes the conclusions to the findings and the recommendations for future research directions.

2 Literature Review

This chapter analyses the information of most interest for the development of the study. It will be divided into two sections:

- *Project Management Principles*. A look on the foundations for project management proposed by the PMI´s PMBOK.
- *Risk Management Methodologies*. An assessment of the main risk management procedures with a holistic view.

2.1 Project Management Principles

Previous editions of PMBOK defined process-based approaches for the successful development of project work. These could be arranged into different groups or areas, being Project Management Knowledge Areas one of the most popular categorisations. However, with the development of PM knowledge, these Knowledge Areas have evolved, and latest editions of PMBOK (i.e. 7th edition) introduce principle-based guidelines instead of the previous process-based outlook.

These principles serve as a series of key ideas that establish the bases for project management, guiding users through the most adequate routes of action aimed towards fulfilling project needs. Therefore, principles provide direction on; how to apply knowledge throughout the project, what tools to utilise, or which skills to foster, amongst others.

The PMBOK 7th Edition proposes 12 principles that define the purpose and reason behind project management, laying down the foundations for the successful development and completion of a project, and offering project managers a simplified structure that considers the fast-pacing environment that surrounds project work.

2.1.1 Stewardship. Be a diligent, respectful, and caring steward

Stewardship takes into account corporate responsibilities both inside and outside organisations. These may be presented, in an orderly manner, in Table 1.

Table 1. Corporate responsibilities.

Inside Organisations
- Operating in line with the mission, vision, and values of an organisation. - Maintaining caring, motivating, and respectful relations within the project team. - Efficiently controlling both the economic and material resources used in a project. - Adequately using authority, accountability, and responsibility, especially by the leadership.
Outside Organisations
- Committing towards sustainability and social responsibility. - Ensuring healthy and fluent stakeholder relations. - Evaluating the project's/organisation's impact on its surroundings. - Advancing towards the integration of best practices in the industry.

In order to display confidence in the team, Stewards should delegate responsibility and provide members with enough freedom to act independently. Furthermore, considering their views and opinions proves essential to sustain that trust.

Amongst the duties and skills required by Stewards, the following four are to be highlighted:

- **Integrity**. Stewards should perform to the highest standards and reflect the values, principles, and behaviours pursued by the organisation they

represent. Stewards should also challenge their team, as well as stakeholders to be more assertive, empathetic, and open to feedback.

- **Care**. It refers to, not only creating a transparent and open working environment, but also managing the potential downsides of project outcomes. Stewards should diligently oversee the organisational matters in their charge, both internally and externally.
- **Trustworthiness**. Stewards represent the entirety of a project, and should behave accordingly both inside and outside the organisation they represent. Trustworthiness entails identifying conflicts of interests between the organisation and its clients, and avoiding situations and behaviours that could undermine trust between the two.
- **Compliance**. Stewards should comply with laws, regulations, and requirements both inside and outside their organisation, striving to follow those guidelines that effectively protect all actors involved in the project.

Accounting for the impacts related to projects enables Project Leaders to make responsible decisions, not only focusing on project objectives, but also targeting the needs and expectations of their stakeholders.

2.1.2 Team. Create a collaborative project team environment

In order to create the bases for a collaborative environment, synergies between different professional backgrounds and support for individuals is to be considered. For that purpose, elements enabling organisations to achieve this working climate should be examined:

- **Team agreements**. It refers to a set of behavioural limits and working norms established, and agreed, by the entirety of the team at the beginning of a project. The agreement may change as the project develops.

- **Organizational structures**. These help coordinate the working efforts associated to project work. These structures may be based on roles, functions, or authority.
- **Processes**. These are defined to enable the completion of tasks and work assignments.

Even if project teams are greatly influenced by the environments they operate in, these may create their own working culture, defining the most suitable structure to achieve project goals. It should be noted that inclusive and collaborative environments that foster information exchange enable for better project outcomes.

Within teams, roles and responsibilities should be clearly clarified. This involves;

- **Authority**. The capability of making relevant decisions, define procedures, make use of resources, or approve certain actions.
- **Accountability**. Answering for an outcome. It cannot be shared.
- **Responsibility**. The obligation to do something. It can be shared.

That said, collaborative project teams take collective ownership of project outcomes.

The incorporation of standards, ethical codes, and guidelines to the practices of project teams, may support the efforts aimed towards avoiding possible issues both internally and externally.

2.1.3 Stakeholders. Effectively engage with stakeholders

Stakeholders may arise, disappear, gain relevance, or lose it, during the life cycle of a project, influencing, both directly and indirectly, a large extent of variables that affect the project's development, performance, and outcome. Similarly, stakeholder interest, influence, or impact on the project, may also change over time.

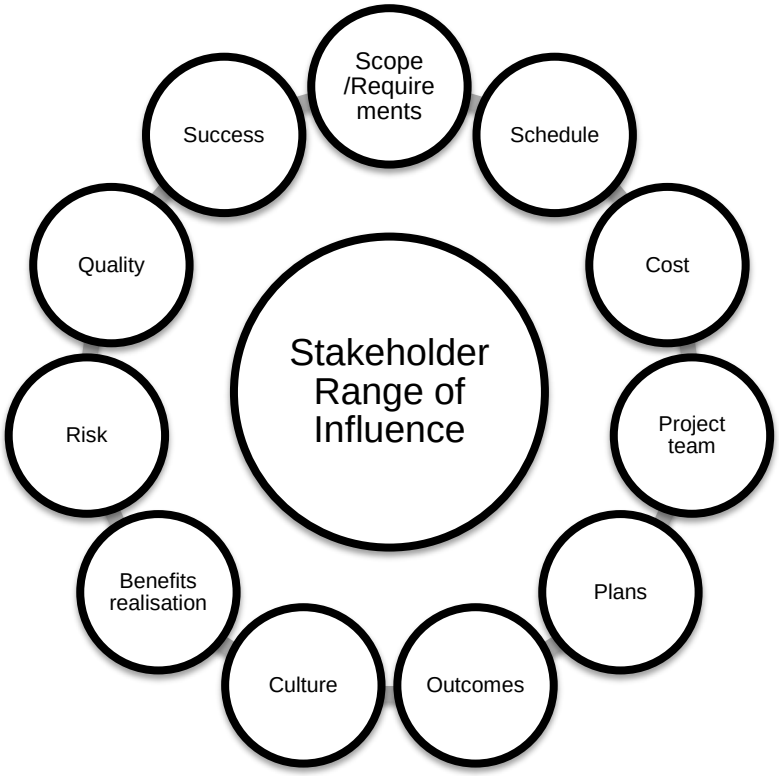


Figure 1. Stakeholder Range of Influence.

Stakeholder engagement is a key feature to understand the interests, concerns, and rights of stakeholders. Knowing how, when, and under what circumstances are stakeholders to be engaged, proves to be elemental for an efficient stakeholder management.

By engaging with stakeholders, project teams have the chance of detecting, collecting, and evaluating information, data, and opinions. This enables teams to align themselves with the project environment, fostering their adaptability and reducing potential negative impacts.

The stakeholder engagement process should also include building and maintaining solid relationships through frequent, two-way communication, assimilating perspectives, and shaping shared solutions. Therefore, working on interpersonal skills may be an option to be considered.

Finally, it should be highlighted that solutions developed through a stakeholder engagement process, are more likely to be acceptable for a broader range of stakeholders.

2.1.4 Value. Focus on value

Value may be classified differently depending of the expected outcomes of a project. This is, it may be defined as the financial contributions of a particular organisation, the perception of the social benefits achieved, or a project's contribution to the wider objectives of an organisation. Nevertheless, it should be clear that value is the ultimate success indicator and driver of projects.

Projects look to provide a valued solution based on the desired outcomes within a project. For that purpose, they usually present a business case.

Business cases state how project outcomes will be translated into the desired value. This may be done by applying a qualitative, or a quantitative approach, as well as a mixture of the two. A business case is composed of the sections defined in Table 2.

Table 2. Elements of a Business Case.

Business need	It presents the reason for the development of a project. It provides understanding on business drivers, as well as the identification of opportunities.
Project justification	It provides a detailed explanation between the deployed investment and the value to be attained, giving grounds for the efforts exercised.
Business strategy	The required strategy to meet with project objectives and achieve the desired value.

Business cases allow project teams to make the informed decisions that aid them on achieving the desired value contributions.

Since value is a subjective concept, varying between people and organizations, placing a priority on the customer's perspective proves essential.

It is also worth highlighting that value contributions may present themselves as a short- or a long-term measure, and that evaluating the whole context and life cycle of the project is essential to achieve the outputs and value intended. Project managers and organizational leaders should work together to ensure that project tasks and deliverables are correctly prioritised to achieve the end goals.

2.1.5 Systems Thinking. Recognize, evaluate, and respond to system interactions

A system is a set of interactive and interconnected elements that work together as a whole. Under this definition, project work may easily be related to the attributes of a system and, therefore, treated as such.

In project environments, the work developed may end up becoming part of a larger structure or system-of-systems. Thus, adopting a holistic approach towards project work may prove beneficial for project teams, allowing synergies between departments, the generation of new ideas, or the adoption of more efficient approaches and working methodologies. Efficient project teams balance inside/out and outside/in perspectives to enhance alignment throughout these project structures.

To ensure that the desired outcomes are reached, systems thinking should consider both the evolution of the project over time and the impacts generated after its end.

Due to the ever changing nature of project work, evaluating the internal and external conditions affecting a project may allow project teams to pinpoint the possible changes that influence development, protecting both the project's and the stakeholders' interests.

Project systems often bring diverse teams together, generating value and increasing the chances of success. Recognizing, evaluating, and responding to these interactions may derive into various positive results. These are highlighted in Table 3.

Table 3. Positive outcomes derived from system interactions.

Positive outcomes derived from system interactions
- Early and effective consideration of uncertainty and risk. - Study of unfavourable scenarios and possible alternatives. - The ability to adjust to changes during project development. - Identification of variables affecting project delivery. - Clear communication amongst the project team and with stakeholders. - Alignment of the project goals and objectives with the customer's vision. - Adaptability to the different needs of project actors. - Synergies between projects and systems. - Increase in performance and the subsequent savings. - Emergence of new opportunities. - Identification of project threats. - Better decisions making procedures.

2.1.6 Leadership. Demonstrate leadership behaviours

The interconnected and ever-changing nature of projects, involve the participation of multiple actors, both internal and external, with an interest in influencing project development. These actors are to be dealt with in regular basis. Therefore, requiring an effective leadership capable of managing the generated confusion and conflict, and guide the process to a successful outcome.

This last point proves particularly relevant considering the presence of too many actors, whom might generate additional conflict and confusion if they try to influence project

focus in multiple, misaligned directions. In consequence, project participants should aim to increase performance by adopting leadership skills and complementing each other.

Successful leaders allow controlled influence, motivating and coaching members throughout the project and including the company's culture and practices throughout the process.

Effective leaders combine elements of multiple leadership styles (i.e. autocratic, democratic, laissez-faire, directive, participative, assertive, supportive, autocratic to consensus), adjusting to different situations. An effective leadership is achieved, mainly, through the combination of a set of different skills and techniques. These are presented in Figure 3.

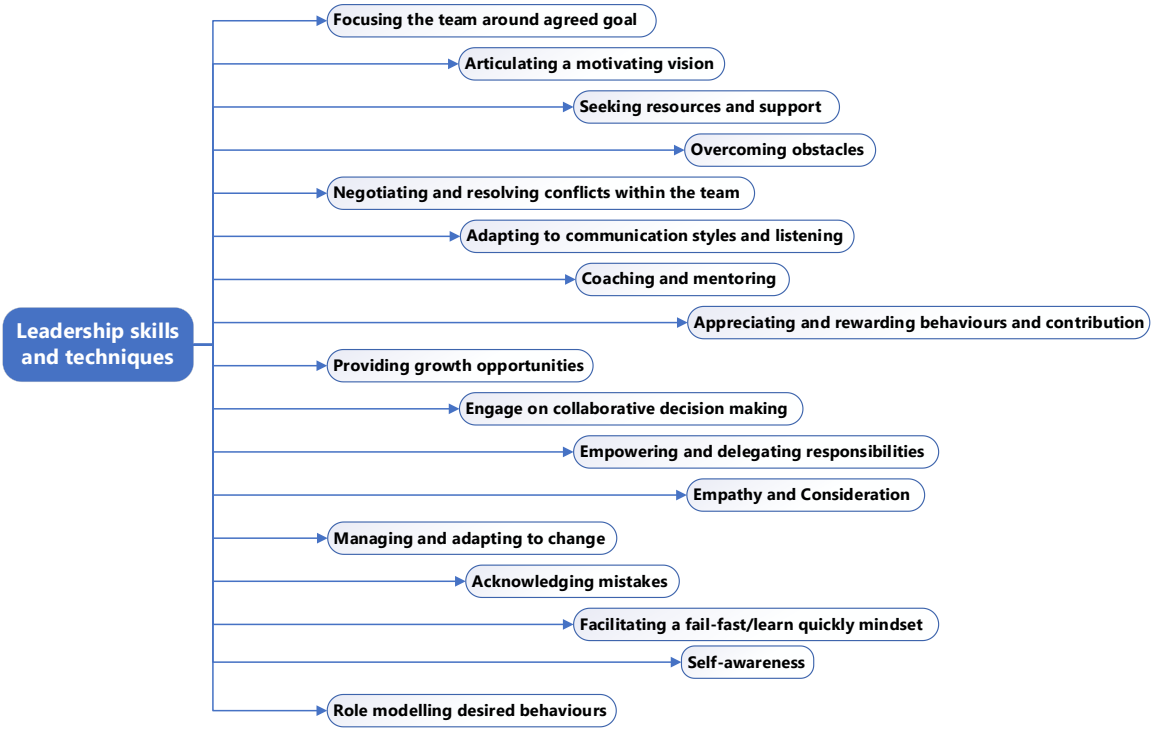


Figure 2. Leadership Skills and Techniques.

Authority, on the other hand, is the position of control/power given to individuals within organizations. This characteristic aims to foster effective and efficient functions.

However, it should not be confused with Leadership. Authority may be used to influence, direct, or demand when project members do not perform as expected.

Leadership may be practiced by more than one person, fostering efficient and trusting environments.

2.1.7 Tailoring. Tailor based on context

Tailoring is referred to the act of adjusting the approach, practices, or methodology of a project to suit its needs and surroundings. Depending on the number of people involved on a project, its complexity and uncertainty levels, or the risk, project teams will need to adopt flexible approaches that enable them to adapt and reach the desired outcomes.

The purpose of project tailoring is the maximization of project performance by managing constraints, risks, and resources, and applying the most efficient working practices and methodologies. Hence, and considering the unique nature of projects, tailoring processes tend to be iterative processes that change in time in order to provide the most adequate working framework. Collecting feedback and evaluating project effectiveness is, therefore, an essential practice to be adopted during a project's life cycle.

Amongst the various benefits of a tailored project, the following ones may be highlighted:

- Higher team commitment
- Reduce the need for additional actions or resources
- Customer-oriented focus
- Reduction of project times and costs.
- Efficient utilization of project resources
- Innovation, efficiency, and productivity;
- Improvement of the existing methodologies, through trial and error.
- Discovery of better/more suitable processes or approaches, for project work.
- Effective integration of new working procedures methods and practices

- Adaptability

2.1.8 Quality. Build quality into processes and deliverables

Quality refers to the level of requirement-accomplishment reached by a particular product or service. These requirements may be presented as objectives, customer stated demands, or even customer implied needs.

Quality levels are measured based on their conformance to the acceptance criteria and their fitness for use. Within this particular spectrum, several areas may be distinguished, with the most relevant ones being presented in Figure 4.

Figure 3. Quality Levels.

These characteristics are measured by project teams through metrics, as well as the acceptance criteria described in the statement of work/ design documents. Both the criteria and the relevance of these quality areas may vary as the project is updated and prioritisation occurs.

Quality measuring and evaluation aims to mitigate waste, reduce the use of resources, and enhance the probability of reaching the desired objectives. Project processes and activities are assessed through reviews and audits.

Amongst the positive results derived from process and deliverable quality, the following may be highlighted:

- Project deliverables that are fit for purpose.
- Project deliverables that meet stakeholder expectations and business objectives.
- Project deliverables with little to no mistakes.
- On time project delivery.
- Improved cost control.
- Fewer rework and waste.
- Fewer customer complaints.
- Enhanced supply chain integration.
- Enhanced productivity.
- Healthier project environments.
- Motivated project teams.
- Robust service delivery.
- Better decision making.
- Continuous process improvement.

2.1.9 Complexity. Navigate complexity

Human behaviours, system interrelations, uncertainties, and ambiguity may lead to an increase in project complexity.

As the number of project interactions rise, the level of complexity within projects rises as well. In consequence, project teams modify their activities and working styles to address

the effects of high complexity situations. The most common sources of complexity are presented in Table 4.

Table 4. Sources of complexity.

Human behaviour. Subjectivity, conflicting personal agendas, or even cultural and language differences contribute to complexity within projects.
System behaviour. It is referred to the issues, risks, and ambiguous reactions derived from the interdependencies between project variables.
Uncertainty and ambiguity. Uncertainty is referred to the lack of understanding, or awareness, on issues, practices, or solutions to engage in, while ambiguity is usually a consequence of the excess of information, which derives into a lack of clarity. In complex environments, uncertainty and ambiguity may lead to vague definitions of probabilities and impacts.
Technological innovation. New technologies can contribute to positive market disruption, as well as complexity. If technology related uncertainties are not identified, or well defined, project complexity will rise.

Increasing complexity levels can arise at any point during the life cycle of a project. Nevertheless, project teams may identify these peaks in complexity by looking at project components. The team's ability to identify complexity will vary depending on; the knowledge of systems thinking, previous experiences, experimentation, system interactions, or even stakeholders.

2.1.10 Risk. Optimize risk responses

An uncertain or ambiguous situation with the power of creating an, either positive or negative, impact on project objectives.

Risks are to be identified and tackled during the entire life cycle of the project, as these may arise, both internally and externally, throughout its development. The role of project teams, in this particular subject area, is to identify, monitor, and manage project risks to maximise positive risks and minimise negative risks.

- **Positive Risks or Opportunities**. These may generate benefits throughout the project, including; time and cost reductions, greater performance, greater market share, or improved reputation.
- **Negative Risks or Threats**. These may generate problems throughout the project, including; Time delays, cost overruns, technical failure, performance reduction, or lesser reputation.

Project teams should also consider the Overall Project Risk. This is, the effect of uncertainty on the entirety of the project.

Overall risk arises from uncertainty, at any stage and from any component of the project, exposing stakeholders to variations in project outcome. Risk management strategies include: mitigating threat drivers; promoting opportunity drivers; enhancing capabilities that contribute towards reaching project objectives; and, engaging with key stakeholders to determine risk appetite and risk thresholds.

- **Risk appetite**. Level of uncertainty that Stakeholders are willing to accept for a particular outcome.
- **Risk threshold**. Measure of acceptable variation around an objective. It reflects the stakeholders' risk appetite. The risk appetite and the risk threshold are indicators on the team's capability to navigate risk.

In order to effectively identify de define risk responses, project teams should consider evaluating:

- Relevance and the effects over the schedule;

- Cost effectiveness;
- The probability of appearance within the project context;
- Acceptance or rejection by key stakeholders; and,
- Responsibility and ownership.

2.1.11 Adaptability and Resiliency. Embrace adaptability and resiliency

Adaptability refers to the capability of adapting to changing environments, while resiliency may be defined as the ability to quickly assimilate the impacts derived from upsets.

Project teams commonly face internal and external challenges that slow down the development of projects. However, counting with a resiliency and adaptability focused approach enables teams to adapt to these setbacks and thrive.

Accordingly, the assumption that projects should keep the same initial scope and planning structure throughout the project, may be an approach limiting its value generating potential. That said, adaptive proposals should consider holistic views and include the following capabilities in project environments:

- Easily adaptive short feedback loops;
- Constant improvement and learning mentality;
- Quickly assimilating the “lessons learned” from previous experiences;
- Broadly skilled project teams, in combination with experts in specific subject areas;
- Monitoring and control to ensure quick adaptation to better performing practices;
- Diverse project teams that enhance synergies amongst team members;
- Open and transparent planning with team members and stakeholders;
- The possibility of testing new ideas/approaches to project work;

- Being open to alternative ways of thinking and working;
- Ensure that decision making is made after all alternatives are considered;
- Management support; and
- Open process design balancing work speed and scope stability.

Project teams should consider and be ready to adapt to alternative working dynamics and plans, if these enable an advantage or opportunity. Nevertheless, this sort of decisions should be taken with the support of the project sponsor, product owner, or customer.

These adaptive processes should consider a holistic view towards potential changes or undesired circumstances, envisioning outcomes rather than deliverables. This outlook may offer project teams better solutions, as well as providing them with the capability of quickly recovering from setbacks.

2.1.12 Change. Enable change to achieve the envisioned future state

Change management is the structured, clear, and cyclic approach towards adjusting teams and organisations to new states or scenarios.

These changes may derive from internal project needs (e.g. new expertise, greater performance levels) or external sources (e.g. socioeconomic changes, technological developments), generating an impact in project teams, as well as stakeholders. Nevertheless, enabling the participation of both these agents throughout the transition, may aid the project in the process of delivering the intended outcome.

Change in organisations may prove challenging, especially when dealing with conservative working environments, where risk tends to be avoided and practices have faced no change for long periods of time.

Effective change management delivers a motivational communication strategy and addresses working concerns to favour an adoption-friendly environment. Furthermore, project teams should consider working together with key stakeholders to pinpoint possible resistive actions and increase the chances of assimilating change. Amongst the different change favourable actions available, the following may be highlighted:

- Communicating the vision and goals regarding change early in the project;
- Communicating the benefits of this transition to all levels of the organisation;
- Adapting the speed of change to the change appetite, cost, and project environment;
- Fostering activities that reinforce change and its implementation; and
- Recognising and addressing the needs of stakeholders to embrace change effectively.

2.2 Risk Management Methodologies

There are several risk management methodologies used throughout the industry, depending on the objectives and sectors being analysed. Amongst these, the following have been identified as the most widely used in the risk management field (Table 5).

Table 5. Risk Management Methodologies.

- ANACT - ANSI/ISA-62443-3-2-2020 - Australian ACSC security manual - Austrian IT Security Handbook - BOEHM - BSI STANDARD 200-2	- EVENT TREE - FAIR - FINE - Guide to conducting cybersecurity risk assessment for critical information infrastructure	- IS risk analysis based on a business model - ISF Methods - ISO 31000 - ISO/IEC 13335-2 - ISO/IEC 17799 - ISO/IEC 27001 - ISO/IEC 27005:2018	- NIST SP 800–30 - NIST SP 800-37 - NIST SP 800–39 - NIST SP 800–82 - OCTAVE ALLEGRO - OCTAVE FORTE - OCTAVE-S - O-RA - PSYCHOSOCIAL

- CORAS	- Guidelines on cyber security on board ships	- ISRAM	- RISKIT
- COSO ERM		- IT-Grundschutz	- RiskSafe Assessment
- CRAMM		- LEST	
- Dutch A&K Analysis	- HITRUST	- MAGERIT V.3	- RNUR
	- IEC 62198	- Marion	- SEI-SRE
- EBIOS	- IMO MSC-FAL.1/CIRC.3	- MEHARI	- SERIM
- ERGONOMIC		- MIGRA	- SERUM
- EU ITSRM	- INSHT	- MONARC	- SHERPA
	- IRAM2	- ETSI TS 102 165-1 (TVRA)	- SP800-30
			- THERP

As it may be observed, there are a considerable amount of risk management methodologies currently available, most of which are centred towards the information security field (60%).

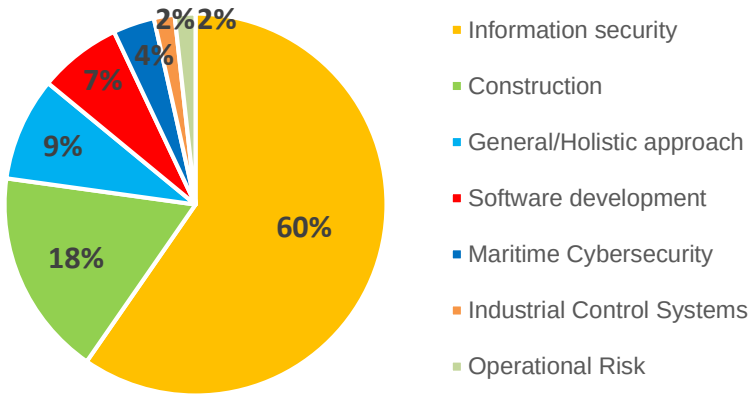


Figure 4. Risk Management Focus Areas.

Regarding holistic risk management methodologies complying with the criteria defined in Section 5. Methodology, the following ones were identified:

- COSO ERM
- EC 62198
- ISO 31000

- OCTAVE FORTE
- RISKIT

This section will analyse the features of these risk management methodologies, highlighting their approach and alignment with project management principles.

2.2.1 COSO ERM

The COSO Enterprise Risk Management (ERM) is an organisation oriented methodology that defines the essential components for enterprise risk management. It aims to help companies and organisations adapt to the changing conditions of business environments through a common language and a holistic view of enterprise risk. Furthermore, it pushes on the idea of integrating. The methodology revolves around the idea of inter-function integration, integrating risk management activities in all business areas to prevent risk management from being perceived as an independent activity.

The process analyses risk through 5 components and a total of 20 different principles.

- **Governance and Culture**. It regulates the management within an organisation, defines responsibilities, and guides on how to attain the desired behaviours and risk understanding.
    1. Exercises Board Risk Oversight
    2. Establishes Operating Structures
    3. Defines Desired Culture
    4. Demonstrates Commitment to Core Values
    5. Attracts, Develops, and Retains Capable Individuals
- **Strategy and Objective Setting**. It provides guidance on strategic and objective setting activities during the planning process. Risk management should be aligned with the organisation's strategy and objectives.
    6. Analyses Business Context

7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

- **Performance**. Deeply related to the organisation's strategies and objectives. Risks are prioritized based on the weight assigned and in terms of risk appetite. The amount of risk and organisation is willing to undertake should be collected.

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

- **Review and Revision**. Reviewing the operating performance and the efficiency of the risk management tools over time is key to achieve business objectives.

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

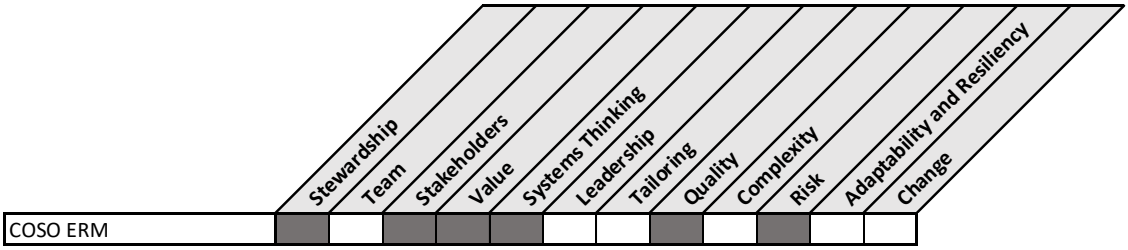
- **Information Communication and Reporting**. Providing the necessary information to both internal and external stakeholders is essential during the risk management process. Communications channels should ensure continuous communication.

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance Executive

The methodology also highlights the need to incorporate technological advancements in the risk management process in pursue of further benefits. These may include; enhanced data analytics (e.g. Big Data, Artificial Intelligence) and visualization tools.

Regarding its alignment with PM principles, COSO ERM may be classified as indicated in Table 6.

Table 6. COSO ERM Compliance with PM principles.



2.2.2 IEC 62198

The IEC 62198 is a project oriented methodology that provides generic guidelines on risk management. The methodology is based on the systematic approach used in the ISO 31000 standard, providing guidance on risk management principles, the framework and organisational needs, and the steps to be followed for an effective risk management process.

The risk management process structure is based on a system of 7 different phases (Rehacek, 2017).

- **Establishing the Context**. The standard only considers the existence of risk in the context of objectives. It highlights the need to understand an organisation's internal and external circumstances, so objectives are reached. This implies identifying gaps and understanding the factors that derive in uncertainties.
- **Risk Identification**. Identifies uncertainties and their consequences over project objectives. This process may lead into updating risk criteria, as well as the purpose and scope of the project. It considers all available information and stakeholder views.
- **Risk analysis**. It provides further understanding of the risk and enables a measure of their magnitude. It provides inputs to the evaluation and the decision-making process, as well as response strategies and methods. It involves the identification, assessment, and forecast of both positive and negative scenarios. It considers tangible or intangible effects.

- **Risk evaluation**. Defines risk thresholds, deciding acceptance in relation to the project/organisation objectives. It compares risk levels with project criteria, while considering the wider context of risk (internal and external). It considers both positive and negative consequences.
- **Risk treatment**. It refers to the selection of the most suitable options for responding to risk. Options for treating risk involve one or more of the following:
    - Avoiding risk by seizing the activity generating risk;
    - Accepting risk in pursue of an opportunity;
    - Removing the risk source;
    - Altering the likelihood;
    - Altering the consequences;
    - Sharing risk;
    - Financing risk; and
    - Retaining risk.

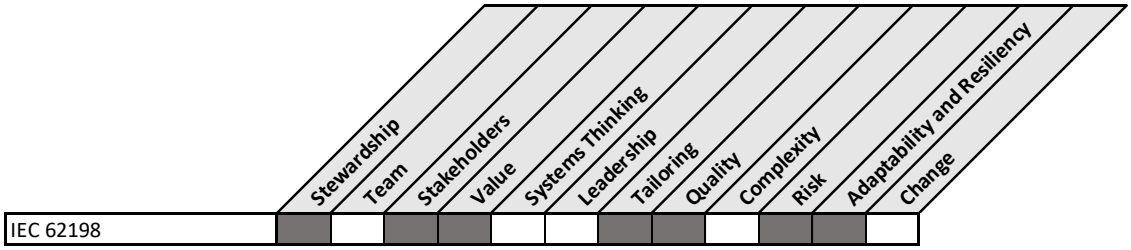
  The selection of the most appropriate risk treatment option involves considering both the costs and the benefits. The justification for risk treatment may not only be economic, considering the organisations internal policy.
- **Monitoring and Review**. It encompasses all aspects of the risk management process and includes the use of indicators and alerts to provide a measure of performance. Results should be used as input and included into the measurement and external and internal reporting activities.
- **Communication and Consultation**. Includes internal and external stakeholder judgement and their perception on risk. These inputs are identified, recorded, and taken into account in the decision-making process. Provides guidance on effective external and internal communication and consultation methods.

The processes and techniques used for risk assessment and analysis include both qualitative and quantitative methods. The techniques highlight the need for

harmonisation, so outputs may be aggregated and compared. Unlike the ISO 31000, the IEC also includes exploitation, sharing, enhancing and retaining methods while responding to risk.

Regarding its alignment with PM principles, the IEC 62198 may be classified as indicated in Table 7.

Table 7. IEC 62198 Compliance with PM principles.



2.2.3 ISO 31000

The ISO 31000 standard is a project and organisation oriented methodology that provides a generic and rational approach to risk management. It defines a systematic and structured framework that enables the adaptation to multiple risks through the lens of a probabilistic logic.

The standard is based on procedural logic and the classical principles of *Plan, Organize, Direct, and Control*, so risks may be clearly defined, measured, and managed. Regarding the process, it is worth highlighting that the standard analyses risk through 8 guiding principles.

1. **Integrated**. It should be oriented to the entirety of the organisation/project and ensure the integration of risk management at every level and stage. This includes working practices and processes.
2. **Structured and comprehensive**. In order to effectively compare the results derived from the risk management process, a structured and comprehensive approach is required.

3. **Customized**. It involves developing tailored and fast responses for internal and external objectives. Over-reactions to risk should be mitigated to avoid inefficient resource management and enable focus on necessary actions.
4. **Inclusive**. Communication between the project team and the stakeholders should be fostered, accepting advice and direction on the most successful approaches on how to tackle issues. Organisations should look towards a strategic alignment with their stakeholders throughout their risk management process.
5. **Dynamic**. Risks can emerge, change or disappear. Therefore, risk management should adapt to project needs and align itself with the organization's external and internal context and risk profile.
6. **Best available information**. Having the best possible resources during the risk management process and accounting for limitations and uncertainties associated to the available information and expectations, improves the chances of identifying and effectively responding to risk.
7. **Human and cultural factors**. Human behaviour and culture significantly influence all aspects of risk management at each level and stage.
8. **Continuous improvement**. Improving should be a constant when it comes to risk management. This step may include training employees on risk management, as well as monitoring, reviewing and communicating risk throughout the organisation. This may also allow managers to learn from past experiences.

The processes and techniques used for risk assessment and analysis include: determining the anticipated efficacy of the risk measures; identification and definition of accountability mechanisms; assessment based on the legal or regulatory requirements the organisation; stakeholder preferences; cost-benefit analyses; and, comparative

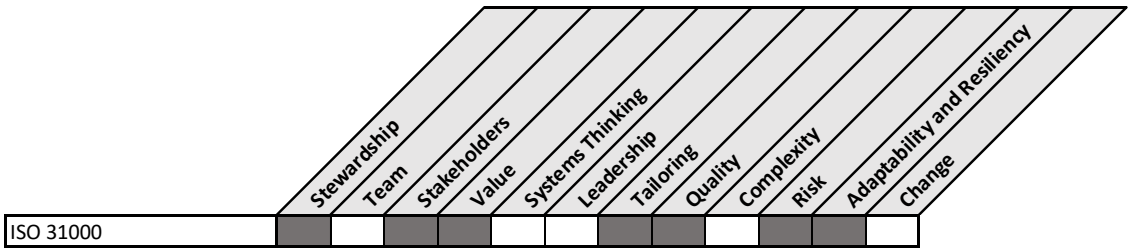
reviews. That said, the standard fosters the use of alternative approaches if these aid the risk management process.

The methodology offers a comprehensible and clear approach to risk management, highlighting the need to establish a policy on risk management, communicating the benefits to stakeholders, and ensuring that enough resources are available. Furthermore, the methodology allows an easy integration with existing practices and pushes on adaptation.

However, due to its generic approach, the methodology fails to include typical recurrent problems previously documented in retrospective analyses, not providing aid, or guidelines, on how to face most commonly repeated crises. Additionally, the ISO 31000 falls short in the process of integrating basic risk management principles into the strategic practices of organizations.

Regarding its alignment with PM principles, the ISO 31000 may be classified as indicated in Table 8.

Table 8. ISO 31000 Compliance with PM principles.



2.2.4 OCTAVE FORTE

The OCTAVE FORTE model is a project and organisation oriented risk management methodology aimed towards helping the understanding and prioritisation of complex risk. The methodology addresses risk through a holistic approach, making use of risk portfolios for the risk management process. It is meant to offer an effective, adaptable,

and agile framework for risk evaluation by applying Enterprise Risk Management (ERM) principles to bridge the gap between executives and practitioners.

The methodology analyses and manages risk through the application of a 10 step process.

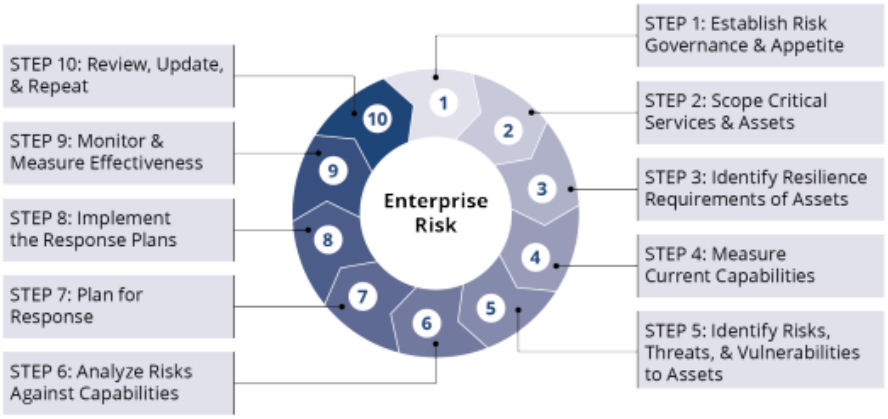


Figure 5. OCTAVE FORTE Process [13].

- **Step 1. Establish Risk Governance & Appetite**. The organisation establishes a governance structure, its risk appetite and tolerate, and sets risk management policies.
- **Step 2. Scope Critical Services & Assets**. Assets are identified and documented, and asset management plans are established.
- **Step 3. Identify Resilience Requirements of Assets**. For every asset in the asset catalogue, resilience requirements are identified and documented
- **Step 4. Measure Current Capabilities**. The organisation's existing controls are reviewed to determine their effectiveness and create a priority list.
- **Step 5. Identify Risks, Threats, & Vulnerabilities to Assets**. The effects of change over the organisation are identified (e.g. technological advancements, evolving environments, fluctuating market condition, new practices). Critical assets are identified and their associated risks, threats, and vulnerabilities documented.

- **Step 6. Analyse Risks Against Capabilities**. Stakeholders are consulted to evaluate risk and create a risk register.
- **Step 7. Plan for Response**. Development of risk response plans. Stakeholders are educated response plan development, interdependent risk identification and response plan maintenance. Governance support is also gathered.
- **Step 8. Implement the Response Plans**. Governance structures allocate resources to implement response plans. Project Managers measure and report response plan performance.
- **Step 9. Monitor and Measure for Effectiveness**. The ERM program is evaluated through the use of metrics. This is done under the bigger purpose of attaining meaningful data that supports change and improvements. Metrics must measure and monitor, not only most relevant variables, but the program's effectiveness and the exposure and impact to risk.
- **Step 10. Review, Update, & Repeat**. The ERM program's effectiveness is reviewed, improvement plans developed and implemented, and the FORTE process repeated. Depending on the organisation's risk appetite and risk management maturity levels, reviewing processes may occur more or less frequently. During this step, the inputs of Tier 1 leaders are included.

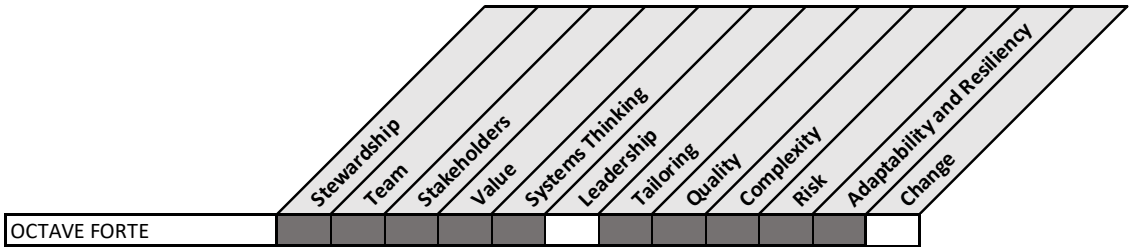
The processes and techniques used for risk assessment and analysis include: Bow Tie Analyses; Business Impact Analyses; Challenges Mapped to ERM Solutions; Decision Matrixes; Decision Trees; Factor Analysis; Failure Mode and Effects Analysis; GAP Technique; GQIM Method; Heat Maps; SMART Goals Method 7; and, Value Stream Mapping.

The methodology offers benefits throughout the organisation, aiding governance structure development, prioritising risk, allocating resources, or during the decision-making processes. Furthermore, by providing a feedback loop linked with the

managerial team, it establishes a robust framework that enables Project Managers to communicate concerns securely and effectively.

Regarding its alignment with PM principles, OCTAVE FORTE may be classified as indicated in Table 9.

Table 9. OCTAVE FORTE Compliance with PM principles.



2.2.5 RISKIT

The RISKIT Method is a project-oriented risk management methodology used in large organisations. The methodology has found use large variety of projects, including; IT, business planning, marketing, and technology related projects. The methodology revolves around probability theory.

The process analyses risk under a framework based on 7 different principles (Stern and Arias, 2011).

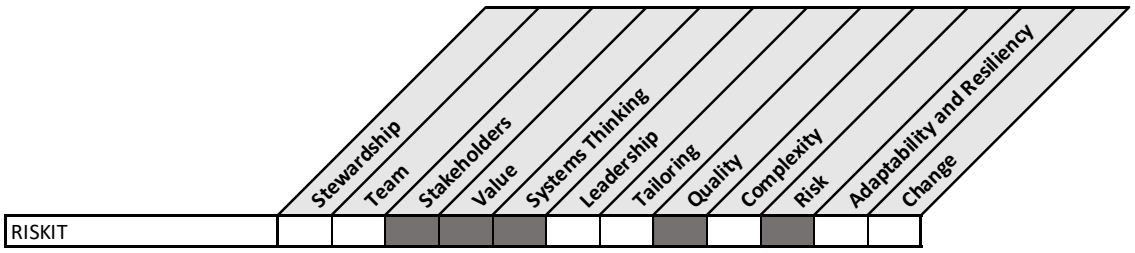
1. Provide precise and unambiguous definitions for risks.
2. Offer a clear definition of the objectives, constraints and drivers influencing the project.
3. Qualitative modelling and documentation of risks.
4. Utilise ratio and ordinal scale risk ranking information to prioritise risks.
5. Apply utility loss to rank the loss associated to a risk.
6. Consider and model stakeholder perspectives.
7. Include an operational definition and training support.

The processes and techniques used for risk assessment and analysis include: graphical methods (i.e. Risk Analysis Graph) to chart risk scenario development; Brain storming techniques; Templates and questionnaires: Utility loss for impact assessment; Pareto ranking; and, risk controlling options (i.e. No action, Contingency plans, Loss reduction, Risk avoidance, Event probability reduction).

The methodology offers a flexible approach, being capable of adapting to projects outside the IT field. However, it does not harmonise stakeholder perspectives within risk results and fails to provide fully reliable data on potential risk estimates.

Regarding its alignment with PM principles, RISKIT may be classified as indicated in Table 10.

Table 10. RISKIT Compliance with PM principles.



3 Methodology

The scope of the research will cover: project management; project management principles; risk assessment and management methodologies; and, comparative processes. These subject-areas will enable a better understanding on risk management, providing enough background to identify gaps, priorities, focus areas, and research needs.

In order to determine the level of alignment with PM principles, the analysis will look for indicators that showcase principle-related features within the evaluated risk management methodologies. This is, the inclusion of elements such as:

- Integrated conceptions of the rules defined by the PMBOK (7th Edition);
- Tools and techniques aimed towards assuring, monitoring, and controlling compliance with PM related concepts (e.g. audits, questionnaires, surveys); and
- Engagement procedures focused on fostering collaborative development and communication (e.g. Brainstorming sessions, Stakeholder workshops, feedback processes, agile methodologies).

Due to the large volume of risk management methodologies in existence, the analysis will establish a selection criteria. Therefore, the methodologies being considered will need to comply with the following:

- To be developed by official bodies.
- To be oriented towards projects and organisations as a whole.
- To have a holistic approach to risk management, regardless of the original type of project it was designed for.

The comparative process will be carried out through a Performance Matrix, a tool utilised in multicriteria analyses to process large amounts of complex information in an efficient manner.

The matrix will compare the designated methodologies, against the twelve principles of project management, with the purpose of evaluating their performance. The individual performance assessment will be presented as bullet point scores, indicating their compliance.

The matrix will only focus on scoring the compliance of each methodology with PM principles, assuming an equal weight for all scores assigned. There is no interdependence between the methodologies being compared, meaning that the judged strength of preference for an option on one criterion will be independent of its judged strength of preference on another.

In order to avoid unjustified assumptions, the analysis will assess the extent to which the methodologies comply with the principles. Compliance will be represented through a darker tone filling.

Table 11. Example of a Performance Matrix.

	Criteria 1	Criteria 2	.	.	.	Criteria n
Alternative 1						
Alternative 2						
.						
.						
.						
Alternative n						

The information gathered for the development of this study will come from publicly available sources (i.e. desk-based research), as well as the academic resources available to the University of the Basque Country (UPV/EHU).

4 Results

Project management principles are meant to act as guidelines on the best practices and approaches to be taken in the way to project success. These principles are based on both theory and managerial experiences, defining the grounds for most safe and efficient management styles. Therefore, avoiding the use of the inherent concepts defining these principles may result to be a risk on itself.

Out of the five methodologies analysed, OCTAVE FORTE was the one most compliant with the principles of project management (10), followed by IEC 62198 (7), ISO 31000 (7), COSO ERM (6) and RISKIT (5).

Table 12. Methodology compliance with Project Management Principles.

	Stewardship	Team	Stakeholders	Value	Systems Thinking	Leadership	Tailoring	Quality	Complexity	Risk	Adaptability and Resiliency	Change
COSO ERM	■		■	■	■			■		■		
IEC 62198	■		■	■			■	■		■	■	
ISO 31000	■		■	■			■	■		■	■	
OCTAVE FORTE	■	■	■	■	■		■	■	■	■	■	
RISKIT			■	■	■			■		■		

As it may be observed, some common gaps were identified amongst risk management methodologies, especially on areas such as change management and interpersonal relations. While all methodologies complied with the principles of *Quality, Risk, Stakeholders,* and *Value*, demonstrating care and interest for internal and external Stakeholder contributions and ensuring that quality requirements and perceived needs were met, other areas were left aside.

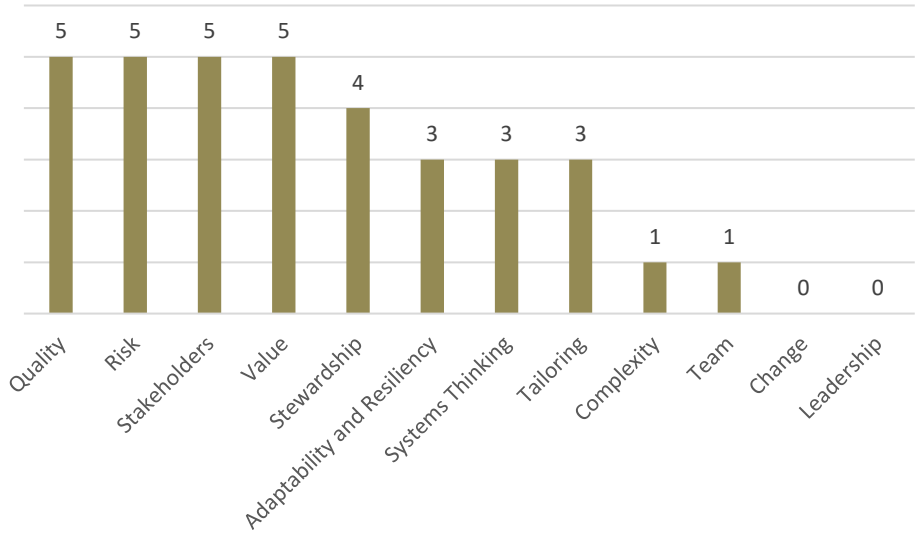


Figure 6. Level of Compliance with PM Principles.

OCTAVE FORTE complied with most of PM principles, considering needs both inside and outside organisations, the contributions of stakeholders, organisational structures and responsibilities, or even interdependent risks, amongst others. However, the methodology did not consider leadership capabilities while managing confusion and the conflict of interest amongst stakeholders. Furthermore, OCTAVE FORTE does not delve into the risks derived from the lack of an effective change management strategy, which would include defining a structured, clear, and cyclic approach towards adjusting teams and organisations to new states or scenarios.

The IEC 62198 and the ISO 31000, on the other hand, share their compliance with PM principles, accounting for the organisation's internal and external responsibilities while focusing on stakeholders, value, and the quality of the process. That said, the standards do not consider interrelated risks and lack information on ways to foster efficiency, synergies and collaboration on working environments. They also lack guidance on effective leadership, change management, or ways to navigate complexity, as they fall short on detailing procedures that engage in system behaviour, ambiguity, and technological innovation.

The COSO ERM methodology is not fully compliant with the tailoring and adaptability needs that the previously referenced standards detailed. However, it did consider systems thinking throughout its risk management process, highlighting the influence of interrelated risks over the overall performance of a project/organisation and providing information on effective integration.

Finally, RISKIT proved to be the least compliant risk management methodology regarding PM principles, not incorporating concepts like the organisation's strategic objectives, or its internal and external responsibilities throughout its risk management process. The methodology provides a structured risk management process, but does not consider the organisation's qualities or circumstances, and it lacks the guidance on how to handle the risks derived from possible changes in working environments, to quickly assimilate the impacts derived from upsets.

5 Conclusions

The study analysed and compared the most commonly used holistic risk management methodologies in order to determine their level of alignment with PM principles. Based on the attained results, the following conclusions may be obtained.

- In average, risk management methodologies integrate about half (i.e. 58.3%) of the concepts defined by PM principles, mainly focusing on performance, risk assessment and control, stakeholder influence, and business/project related needs. However, complex and interconnected risks tend to be left aside, including the ones associated to the human factor.
- The risks associated to change and the managerial capabilities of the workforce require further research and development within the risk management field. Adjustment efforts towards new and evolving scenarios tend to be ignored during the risk management process, avoiding both internal and external evaluations of their impact.
- Most methodologies do not offer ways to mitigate the risks associated to complexity, which may impact technical business environments due to the nature of their practices. Considering that most risk management methodologies are oriented towards the IT and the cyber security field, the lack of progress performed in this field should evoke further research.
- Risk management methodologies lack sufficient adaptability measures to ensure versatility throughout the project. The inclusion and definition of effective tailoring processes is scarce and objective dependent, leaving aside the human factor. Therefore, designing effective tools and guidelines that consider these concepts is still required.
- Personal interrelations tend to be left aside by most risk management methodologies, avoiding the possibility of synergies between departments and lacking to explore the

risks associated to the lack of motivation, working environments, burnouts, or project closings.

- In the overall, risk management methodologies tend to consider PM principles throughout their content. However, further alignment between risk management strategies and project management principles is still required.

Alternatively to the points presented above, the following points should also be highlighted.

- M&E tools and techniques should be extended to include technological advancements and continuous improvement structures. Current methodologies fall short on the inclusion of audits, or automated information flow channels, requiring further details on monitoring and control procedures.
- Current risk management methodologies do not include examples on typical risks, or the most effective responses, which may prove useful for users facing similar scenarios. Considering, the recording and inclusion of this kind of information could increase success rates within projects and business environments, as well as foster alternative evaluation approaches.

Funding

No funding was allocated for the development of this study.

Declaration of Competing Interest

There is no conflict of interest.

References

[1] Project Management Institute. (2017). “A guide to the Project Management Body of Knowledge (PMBOK guide) (6th ed.)”. Project Management Institute. Available at: https://www.pmi.org/

[2] Project Management Institute. (2021). “A guide to the Project Management Body of Knowledge (PMBOK guide) (7th ed.)”. Project Management Institute. Available at: https://www.pmi.org/

[3] European Environment Agency. (2020). “Introduction to Risk Assessment Concepts”. Copenhagen. EEA. Available at: https://www.eea.europa.eu/publications/GH-07-97-595-EN-C2/chapter1h.html

[4] Polyzos, S. Kungolos, A. (2007). “Comparative analysis of decision-making methodologies used in environmental planning. Sustainable Development and Planning III”. Available at: https://www.academia.edu/15141482/Comparative_analysis_of_decision-making_methodologies_used_in_environmental_planning

[5] Department for Communities and Local Government. (2009) “Multi-criteria analysis: a manual”. Communities and Local Government Publications. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/7612/1132618.pdf

[6] Carpio de los Pinos, A. J. González García M. (2017) “Critical analysis of risk assessment methods applied to construction works”. Revista de la Construcción. Available at: https://www.redalyc.org/pdf/1276/127651042009.pdf

[7] Lambrinoudakis, C. Gritzalis, S. Xenakis, et al. (2022). “Compendium of risk management frameworks with potential interoperability”. ENISA. Available at:

https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks

[8] ENISA. (2022). "RM/RA Methods". ENISA. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods (Last checked: 25 May 2022)

[9] Stern, R. Arias, J. C. (2011) "Review of risk management methods". Business Intelligence Journal. Available at: https://condor.depaul.edu/~dmumaugh/readings/handouts/SE477/SERIM_Article_3.pdf

[10] International Organization for Standardization. (2018). "ISO 31000: 2018, Risk Management". International Organization for Standardization. Available at: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

[11] Lalonde, C. Boiral, O. (2012). "Managing risks through ISO 31000: A critical analysis". Risk Management 14, 272–300. Available at: https://doi.org/10.1057/rm.2012.9

[12] Rehacek, P. (2017). "Risk management standards for project management". International Journal of Advanced and Applied Sciences. Available at: http://science-gate.com/IJAAS/Articles/2017-4-6/01%202017-4-6-pp.1-13.pdf

[13] Tucker, B. A. (2020). "Advancing Risk Management Capability Using the OCTAVE FORTE Process". Carnegie Mellon University. Available at: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2020_004_001_644641.pdf

[14] Onay, A. (2021). "The Role of Internal Audit from New Enterprise Risk Management Frameworks Perspective: Research in Turkey". Istanbul University Press. Available at: https://www.researchgate.net/publication/348605664_The_Role_of_Internal_Audit_from_New_Enterprise_Risk_Management_Frameworks_Perspective_Research_in_Turkey