Enhancing Risk Assessment Accuracy: Addressing Organizational Complexity through Graph-Based Models and Correction Factors [1]

Marco Pinzaglia[a] and Dr. Michele Vincenti[b]

[a] FEMBA, Rome, Italy
[b] University Canada West, Vancouver, Canada

Abstract

This work aims to stimulate a reflection on the fact that organizations that have or adopt very complex organizational structures may encounter results in risk assessment that are not entirely reliable or compromised by their complexity.

The work examines the main approaches to risk analysis organizations adopt, particularly the models and techniques used to assess processes and information management risks.

Risk analysis is an essential process to ensure adequate governance for the organization. For it to be effective, it is also necessary to define a *Risk Analysis Model* (a methodology) capable of preserving specific properties such as *completeness* and *repeatability*. These are some of the indispensable elements to ensure a (recurrent) risk assessment that can consider the evolution of the corporate asset protection system over time and thus determine whether the system as a whole increases or decreases its performance.

In this context, some factors can jeopardize the quality and reliability of the results obtained, and one of these factors is the *complexity of the organization*. Organisations are becoming increasingly complex due to their structure, processes, and rapidly changing external environment, and we know that some limitations exist in using the graph theory applied to RACI. The study of corporate complexity measurement is a vast subject, but this simplified tool is intended to support risk analysis processes in complex organisations specifically.

Measuring *organizational complexity* is a subject that can be addressed with multiple approaches. This work proposes a strategy based on graph and flow network tools applied to RACI matrices. This tool can reproduce an organization starting from its representation produced through RACI matrices and, with the necessary assumptions,

[1] How to cite this paper: Pinzaglia, M. and Vincenti, M. (2024). Enhancing Risk Assessment Accuracy: Addressing Organizational Complexity through Graph-Based Models and Correction Factors; *PM World Journal*, Vol. XIII, Issue IX, September.

express an *index of the complexity* of the organization itself using the algebraic properties of graphs. The reflection that emerges is that risk assessment could be subject to errors caused by the detection of input data used to calculate the level of risk. The generation of these errors is linked to the size and complexity of an organization. To manage this phenomenon, the work introduces a correction parameter of the results produced by risk analysis (an "adjustment" factor) that can mitigate any measurement errors produced precisely by the complexity dimension.

Complexity can significantly compromise the reliability of risk assessment results, and organizations must implement correction parameters to mitigate such measurement errors, ensuring better governance and performance over time.

The Importance of Risk Analysis for Organizations

Risk analysis is a fundamental process that allows organizations to identify, evaluate, and mitigate risks that can negatively affect their operations, reputation, financial stability, and overall resilience. Risk analysis has a strategic function within an organization; the identification and measurement of risks enable the company to protect its assets and strengthen its ability to counter threats while also helping it understand better the organizational structure and the costs incurred to deliver its services adequately.

Studying risks can, in some cases, especially in conjunction with significant market changes (e.g., regulatory changes, production technologies, macro-trends such as climate changes, etc.), be one of the elements from which an organization can acquire strategic information related to the convenience or otherwise of staying within a particular business rather than changing its strategy. Some large companies have had to review their market choices, for example, following regulatory updates that have necessitated significant changes to the product/service, up to opting to discontinue the product once the necessary activities to be compliant are evaluated. Today, organizations are becoming more complex because of their structure, processes and the fast-paced changes in the external environment. Randal (2011) defines complex organizations as complex systems due to their typical attributes, such as non-linearity, adaptation to external changes, internal feedback loops, and emergence [1]. Complex systems are usually riskier than simple systems and require strict risk management control. Risk assessment is a process that involves the entire organization and often uses standards and methodologies that guide and provide instructions for managing the various phases of the activity.

Recently, because of the arrival of Artificial Intelligence, a new regulatory landscape for financial services with a particular focus on Environmental, Social, and Governance (ESG) has been created. The new regulations ask the financial service industry to engage proactively with regulators on new prudential developments, focus on resolutions and recovery strategies, establish rigid governance frameworks and continue to manage ESG

risks through an institution-wide approach, only to mention a few requests [2]. The push for effective risk management in financial services comes from economic uncertainty, geopolitical tensions, sustainability and technological advancements. In one of their recent studies, Deloitte recommends that organizations focus on credit risk, operational resilience, supervisory expectations and climate and environmental risks [3].

Regardless of the methodology employed, it remains essential that it can ensure its "reproducibility," that is, by keeping the system in the same organizational and productive conditions and without varying the analysis methodology, it must produce similar results. For example, we can consider the definition provided by the National Institute of Standards and Technology (NIST) in Guide for Conducting Risk Assessments Special Publication 800-30 [4]: "*Reproducibility refers to the ability of different experts to produce the same results from the same data. Repeatability refers to the ability to repeat the assessment in the future, in a manner that is consistent with and comparable to prior assessments—enabling the organization to identify trends".*

Conducting risk analyses through a constant reference model allows for obtaining more easily comparable results with previous studies and understanding whether an organization is improving. The first phase of a risk analysis is represented by defining the perimeter on which it will be carried out; then, information and data useful to understand the context, the assets involved, and what is necessary to assess the level of maturity of the organization in implementing organizational and technical controls to counter threats are collected. The criteria for investigation, analysis, and evaluation are often very well codified in the methodology. However, the process of gathering information can undergo frequent changes to adapt to the organizational and procedural changes of the organization, and in general, can occur through various modes, also integrated, that contribute to defining a reliable picture of the perimeter considered. Typically, information can come from tools, databases, automatic processes, recordings, reports, and, in general, through interviews with members of the organization (process owners and key users, etc.). The results of the interviews, despite employing a methodology that guides both the questions and the possible answers, remain strongly influenced by the perception and knowledge of the "subject" who responds.

Thus, minimizing or eliminating elements of "subjectivity" concerning those who conduct the analysis and evaluate the results is significantly different from being able to *eliminate or mitigate aspects of "subjectivity" that affect the subjects who have to provide the information differently*.

One of the most widely used standards for conducting risk analysis is ISO 31000:2018 (Risk Management - Guidelines), an international standard that provides the necessary guidelines to adopt a risk analysis methodology, implement a structured and integrated

risk assessment methodology in business processes, and promote a culture of continuous improvement.

Considering ISO 31000:2018 as a reference methodology for risk analysis, we faithfully take from the standard the principles on which it is based [5]:

- *Systematic*: The methodology must be structured and consistent, ensuring the risk analysis is conducted methodically and *repeatably*.
- *Evidence-based*: The analysis should be based on accurate and reliable data and information, combining historical data, observations, *experiences, and expert insigh*ts.
- *Transparent and inclusive*: The process should involve relevant stakeholders and make decisions transparently. Involving stakeholders helps ensure that different perspectives and knowledge are considered during the analysis.
- *Adaptable*: The methodology must be flexible enough to adapt to any context or change in circumstances, allowing the analysis to be modified based on new information or an evolving context.
- *Integrable*: Integrating the risk analysis methodology into the organization's existing decision-making processes must be possible, ensuring that risk management is part of the overall decision-making process.
- *Dynamic*: The methodology should allow for continuous monitoring and review of risks, as the context and external conditions can change rapidly.
- *Results-oriented*: Risk analysis should provide results that help improve risk management by guiding decisions that reduce risks in proportion to their potential impact.
- *Prudent in managing uncertainties*: The methodology must recognize that every risk analysis involves a certain degree of uncertainty and must attempt to quantify and manage that uncertainty.

Figure 1 illustrates the phases that comprise the risk analysis according to ISO 31000. Specifically, we find:

- *Definition of the context*: This is the start phase of the process and includes defining the perimeter on which to apply the analysis;
- *Risk identification*: Determine the events causes that could cause a security incident and understand how;

- *Risk analysis*: Estimate the risk associated with the previously identified incident scenarios;
- *Risk evaluation*: Analyze risks against the criteria and thresholds established in the context definition phase;
- *Risk treatment*: In this phase, residual risk is calculated, in other words, the level of risk after implementing security measures;
- *Recording & reporting*: The entire process and its results must be documented and reported through appropriate mechanisms;
- *Continuous monitoring*: This phase considers that the elements that allow risk calculation are not static over time: threats, vulnerabilities, probabilities of occurrence, and impacts can change quickly;
- *Risk communication*: Exchange of information related to risks among stakeholders

Figure 1 – ISO 31000:2018 Risk Analysis Framework

Once the risk analysis tool has been defined, its application in terms of complexity (time, effort, etc.) is strongly linked to the characteristics of the organization and its size. Understanding the organizational structure, processes, procedures, and responsibilities and identifying internal skills is essential. A practical tool to understand how responsibilities and processes are organized in a company is represented by the RACI matrix. RACI matrices were developed around the 50s and 60s and were mainly created as a tool for managing project activities to define roles and responsibilities clearly.

The acronym *RACI* stands for:

- *Responsible*: The person or team that performs the work required to achieve the goal. Accountable: The person or team with (final) decision-making authority over the task and decisions. It must approve the work that the Responsible has completed.
- *Consulted*: The person or team that needs to be consulted before making a final decision or completing a task. These individuals often have relevant skills or information, and their input is necessary for a successful task outcome.
- *Informed*: The person or team who needs to be notified after a decision has been made or a task has been completed.

Figure 2 is an example of a RACI matrix of a process (Process A) that consists of 4 tasks.

RACI MATRIX - PROCESS A

	Business Unit A	Business Unit B	Business Unit B1	Business Unit B2	Business Unit C	Business Unit D	Business Unit E	Business Unit E1	Business Unit E2	# Business Unit	TYPE OF OUTPUT
task 1	A	R	C	I		I	C	I	C	8	document
task 2	C				A	R	I	I		5	data
task 3	I		C		I		A	R	C	6	document
task 4	R				A		I		C	4	document
…	…	…	…	…	…	…	…	…	…	…	…
task n	…	…	…	…	…	…	…	…	…	…	…

Figure 2 – RACI Matrix Example

The following is the transposition of a RACI matrix into a (non-oriented) graph, where the nodes represent the Business Units and the edges represent the functional/operational links between the different organizational units participating in the process. In Figure 3, we have a representation of the graph for task 1, the graph for the entire process consisting of tasks 1,2,3,4, and the relative representation of the Task 1 graph concerning the business functions involved. The Swiss mathematician Leonard Euler has been called the father of the graph theory. The theory is a branch of mathematics that studies the properties and applications of graphs. The graph represents connections and

relationships through nodes and links, and it is widely used in computer science, biology, social science, and organizational management to describe systems [6].

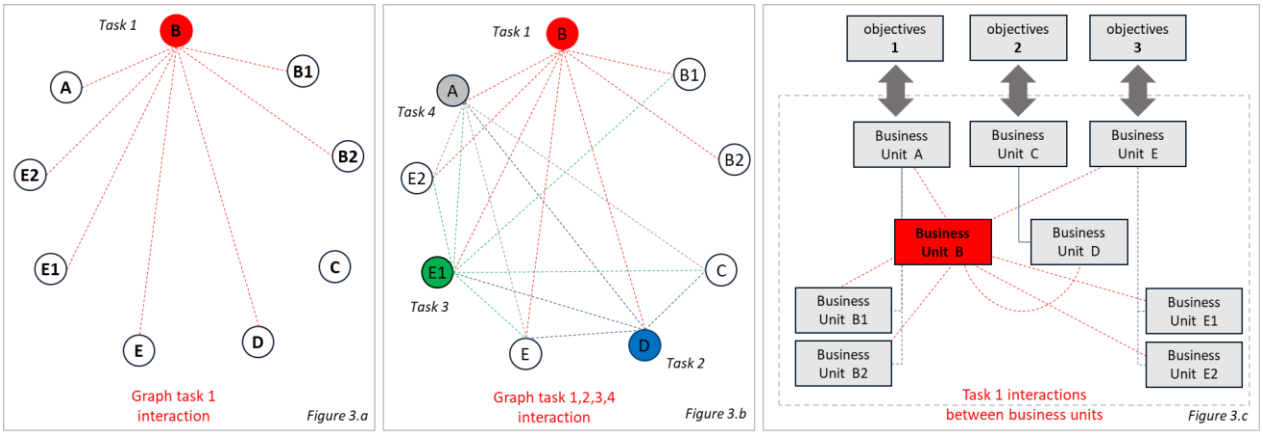

Figure 3 – transposition of the RACI Matrix in Figure 1 into a graph

An excellent example of a successful implementation of risk comes from Principal Financial Group, a cybersecurity company in Seattle, USA. They were successful in their implementation, focusing on proactive risk management and employee engagement. They emphasized the importance of monitoring and detecting potential cyberattacks involving their employees [7].

Ballast Risk Management is another company that recently succeeded in risk management using RACI. They are based in Brentwood, Tennessee, USA. Using RACI with well-defined roles and responsibilities improved stakeholders' engagement and effective communication and execution of the risk management tasks [8].

Introduction to a Model Representing Organizational Complexity

Let's revisit some definitions of complexity that can help us better contextualize the adoption of this term and transpose it into the analysis context:

- *1948 - Warren Weaver*: Complexity can be classified into disorganized and organized. Disorganized complexity concerns systems with many independent variables, while organized complexity concerns systems with many interdependent variables.
- *1962 - Herbert A. Simon*: A complex system consists of a large number of parts that interact in a non-linear way.
- *1992 - Murray Gell-Mann*: Complex systems are characterized by emergent properties that cannot be understood or predicted by analyzing only the system's components.

Referring to *Murray Gell-Mann's complexity theory*, emergent properties result from interactions between the system's components and can, in turn, influence the system's overall behaviour.

The extent of the corporate organization, the number of processes and structures involved, and the necessary interactions between the various structures to achieve the expected result of a single task or process all determine an organization's complexity.

Using the graph theory previously presented, we can represent the interactions between the various organizational structures. The advantage of this approach lies in the ability to use the fundamental calculation relationships intrinsic to graphs. Figure 5 shows a sample model with a graph of 4 nodes and various hypotheses of connections between the nodes. The *Density of the graph* is an indicator of the number of relationships; a density D=1 indicates that all nodes have reciprocal relationships, while D=0 suggests that there are no edges connecting the graph nodes.

In this analysis, characteristics of graphs, such as the "directions" of the relationships, are not considered.

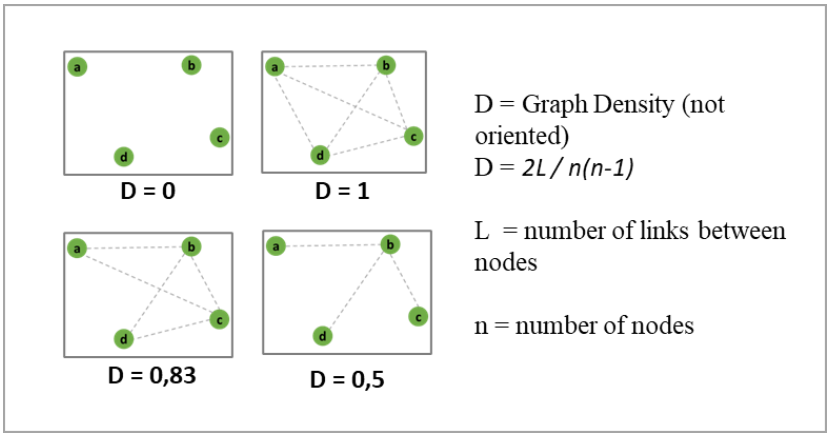

Figure 5 – Graph Density Calculation – Graph Theory

If we revisit the graph in Figure 3, applying the graph density calculation, we find two very different values, as shown in Figure 6, considering that the density D⊂{0;1}. We find:

$$D=2Ln(n-1)D = \frac{2L}{n(n-1)}D=n(n-1)2L$$

$$D1=(2x7)(9x8)=0.19D1= \frac{(2x7)}{(9x8)} = 0.19D1=(9x8)(2x7)=0.19$$

$$D2=(2x19)(9x8)=0.53D2= \frac{(2x19)}{(9x8)} = 0.53D2=(9x8)(2x19)=0.53$$

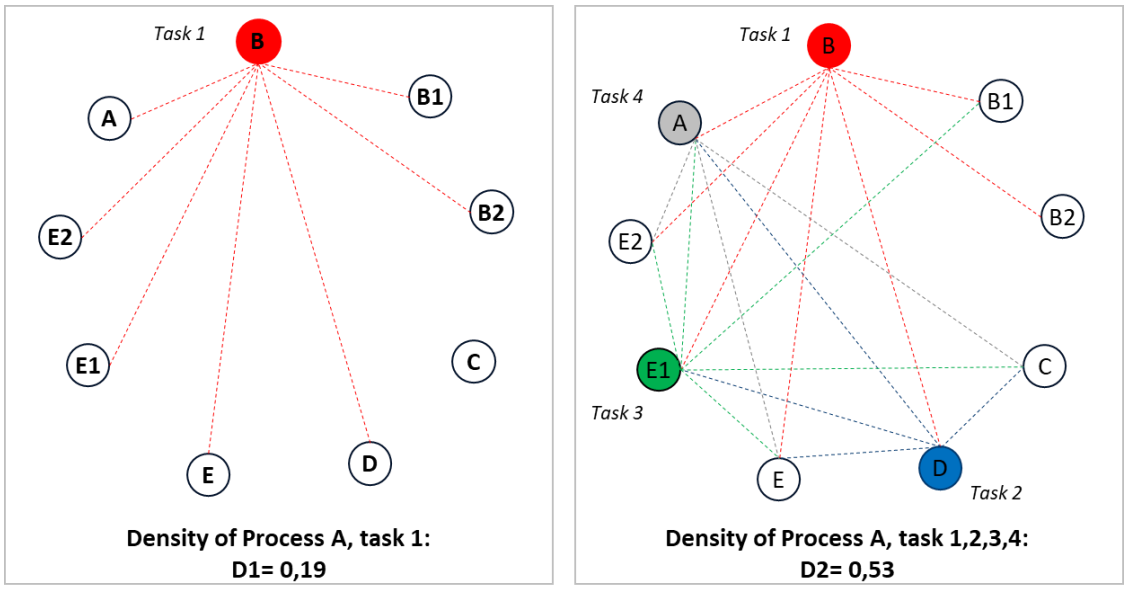

Figure 6 – Graph Density Calculation – Graph Theory

The density dimension becomes, in this representation, an indicator that can approximate the complexity of the organization because it can represent the dimensions of extension and relationship between the various organizational structures. A higher graph density suggests greater complexity due to the more significant number of interactions between the units. The higher complexity can impact the reliability of risk assessment.

The greater the complexity of an organization, the greater its exposure to risks because:

- The "cost" of managing processes increases (proceduralization, document updates, etc.);
- The analysis surface increases and, proportionally, the ability to control decreases (thus the frequency of controls) and the ability to intervene in mitigation processes (i.e., promptly applying the necessary improvement actions);
- It produces knowledge misalignment phenomena that impair the information acquisition phase in risk analysis processes.

The advantage that can be obtained by applying the concept of *"density" of a graph as an expression of an index, albeit partial, of "company structure complexity*" is the ability to apply a representation and calculation model capable of simplifying the analysis context and opening opportunities for increasingly complete reasoning in the search for "optimal conditions." The corporate complexity index, for the considerations produced, provides valuable indications to understand the risk that applying a risk analysis methodology can yield results compromised by the same organizational complexity, i.e.,

organizational complexity can interfere with the quality of the risk analysis activity. What follows aims to exploit the density index as a corrective factor to mitigate the adverse effects of organizational complexity on the results of a risk analysis.

In a risk analysis, the process requires first calculating the inherent risk and then the residual risk.

Definitions:

- *Inherent risk (Ri):* risk that does not consider what the organization can do to counter the threats that generate it.
- *Residual risk (Rr):* risk that considers what the organization can do to counter the threats that generate it (thus, it is always true that Ri≥Rr).

The calculation of the risk level generally involves assigning a value to two variables characterizing the risk itself:

- The *probability* of occurrence of the risk event;
- The *impact* generated by it.

Figure 7 provides a generic qualitative representation of the different levels (high, medium, and low). This representation can take various forms depending on the purposes and needs of the Organization.

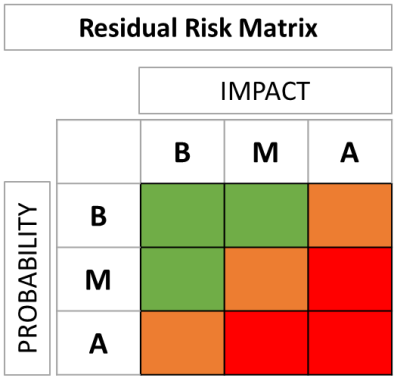

Figure 7 – Qualitative Representation of Residual Risk

The *residual risk* represents the risk on which the organization must make managerial choices regarding treatment hypotheses. At this point, we apply a reclassification to the residual risk considering the organizational complexity, aware that any analysis procedure at this stage does not aim to lower the identified risk value but only to act on elements that may not have allowed a correct identification of the actual risk. The corrective factor acts, therefore, only as an element that increases the identified residual risk. The principle

now applied to the analysis context represented in the form of a matrix identifies the dynamic by which the definition of a risk in a non-complex organization is unlikely to be subject to (unintentional) process errors, and therefore, the identified risk is as such. In a complex organization, the identified risk may not fully represent the state of the organization in its definition and classification level. Hence, applying a corrective factor that considers this condition can bring the final risk assessment result closer to the actual condition of the organization, helping it focus better on the risks to be managed. Figure 8 illustrates how the Density of the graph, typically represented in numerical form and with a scale from [0-1], can also be represented by a qualitative scale (Low, Medium, High). From what has been said above, a low level of Density of a graph, with the assumptions we have represented, corresponds to a low level of Complexity in the organization. This is because there are little or no relationships between the nodes, and the complexity of the underlying processes is also considered low.

Graph Density Value	Density level
0 - 0,33	**LOW (B)**
0,33 - 0,66	**Medium (M)**
0,66 - 1	**High (A)**

Figure 8 – Relationship between Density and Complexity Level

Using the same matrices, we calculate the absolute risk considering the complexity level, i.e., the recalculated residual risk.

Figures 9. a and 9. b highlight the density level parameter, which affects recalculating the residual risk as an upward correction element of risk values.

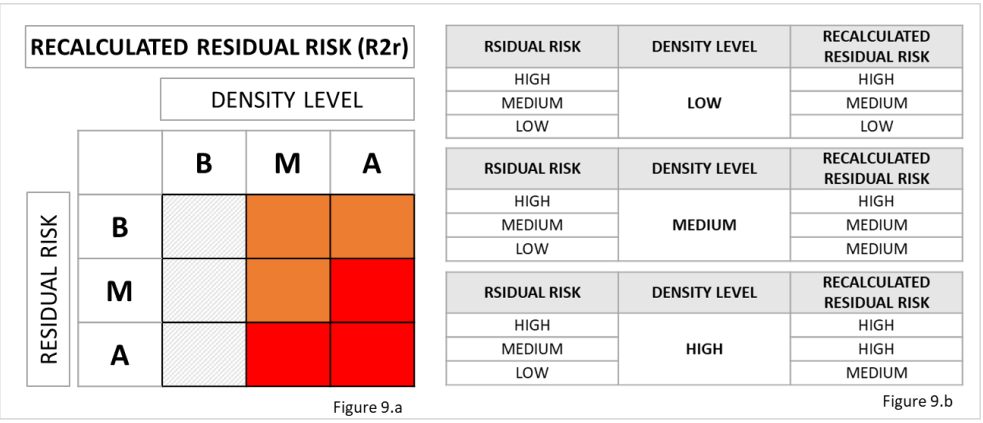

Figure 9 – Matrix for Recalculated Residual Risk Considering Organizational Complexity

The graph-based model, of course, is not the only model that can manage organizational complexity. The Complex Adaptive Systems (CAS), as per its name, sees organizations composed of interacting agents that adapt over time, and the model helps organizations by emphasizing self-organization, learning and adaptation in organizations with high uncertainty and rapid changes [9]. This model may lack clear role definitions and structured accountability, making it less suitable for environments where explicit responsibilities are crucial. The Multiple Perspectives Model (MPM) combines the different stakeholders' perspectives, including their needs and expectations, to address the organization's complexity. The model is holistic and facilitates decision-making and organizational learning [10]. This model may not provide the same role-specific clarity and structured communication level as the RACI model. The Network Theory-Based Models analyze organizational structures and relationships. They map the complex interactions inside the organization, identify key nodes and connections and optimize communication and collaboration [11]. This model focuses on structural relationships rather than assigning individual responsibilities and accountability, which can lead to ambiguities in task ownership.

The RACI model offers advantages in defining roles and responsibilities, simplifying implementation, improving communication, and ensuring accountability, which is better than the other models.

Limitations

When we look at the limitations of the RACI model, the oversimplification of the roles, its static nature, the potential for ambiguity, the time-consuming setup and the lack of depth in role definitions are usually the items identified by the practitioners [12].

This article understands that some limitations exist in using the graph theory applied to RACI. The issue is magnified in unique organizations or non-traditional structures. The accuracy of the RACI model depends entirely on the quality and completeness of the data used in its matrix. Using graph density as a proxy for complexity is a simplification, and the complexity of the organization might not be fully captured. The practitioner of the RACI model must also be familiar with the tool; otherwise, errors are possible. Focusing on internal complexity is another limitation when regulatory changes, market dynamics and geopolitical risks can influence the organization. Lastly, data and graphs can be subjective based on perceptions and not facts [13].

Conclusions

In this work, organizational complexity has been considered as an element capable of creating inefficiencies and, specifically, as an element that can make the results of risk

analyses conducted by organizations on their perimeter less reliable. The correct focus on risks for a company is synonymous with resilience, and the main risk is to reiterate cycles of analysis based on consolidated models over time where work is often done "by differences" to be faster.

Introducing an external reclassification factor to the risk analysis process can help organisations introduce elements of change and counteract stationary dynamics that can make the process less effective, helping the organisation understand which methods are more complex and thus devote more attention to them when performing a risk analysis.

Furthermore, working on graphical representations of the organisation, starting from the transposition of a RACI matrix into a graph, provides the organisation with an easier-to-understand view (map) of the relationships between the various functions, a helpful element in assessing its complexity and supporting any necessary 'simplification' interventions, considering the complexity in processes a force capable of negatively impacting the structure of governance controls (and in general the efficiency of operations).

References

[1] Randall, A. Risk and Precaution; Cambridge University Press: Cambridge, UK, 2011

[2] Bellens, J., Woolard, C., Saidenberg, M., Goyne, E., & Grennan, D. (2023, December 4). *How financial firms can prepare for the 2024 regulatory landscape*. EY. https://www.ey.com/en_gl/insights/banking-capital-markets/how-firms-can-respond-to-the-2024-regulatory-landscape

[3] Deloitte. (2023). *Regulatory Outlook 2024: Global regulatory landscape*. Deloitte. https://www.deloitte.com/uk/en/Industries/financial-services/perspectives/regulatory-outlook-global-landscape.html

[4] National Institute of Standards and Technology NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, SP 800-30 Rev. 1, Guide for Conducting Risk Assessments | CSRC (nist.gov)

[5] Institute of Risk Management, Standard Deviations A Risk Practitioners Guide to ISO 31000, 2018, https://www.theirm.org/media/6907/irm-report-iso-31000-2018-v2.pdf; ISO 31000:2018 Risk management — Guidelines ISO 31000:2018 - Risk management — Guidelines;

[6] West, D. B. (2000). *Introduction to graph theory* (2nd ed.). Prentice Hall.

[7] Cyber Magazine. (2023). *Navigating the threat landscape in 2024*. Cyber Magazine. https://cybermagazine.com/articles/navigating-the-threat-landscape-in-2024

[8] Fulford, M. (2018). *How a RACI matrix can enhance your risk management program*. Ballast Risk Management. Retrieved from https://ballastrisk.com/

[9] Riaz, S., Morgan, D., & Kimberley, N. (2023). Managing organizational transformation (OT) using complex adaptive system (CAS) framework: future lines of inquiry. *Journal of Organizational Change Management*, *36*(3), 493–513. https://doi.org/10.1108/JOCM-08-2022-0241

[10] Zhu, Y., Xu, S., Li, Q., & Wang, L. (2023). Risk management in complex projects: An application of the RACI matrix. *Expert Systems with Applications*. Advanced online publication. https://doi.org/10.1016/j.eswa.2023.119934 Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0957417423009934?via%3Dihub

[11] Gregorius Airlangga, Denny Jean Cross Sihombing, Julius Bata, & Anggun Fitrian Isnawati. (2024). Optimizing Femtocell Networks: A Novel Game Theory Based Power Management Model for Enhanced SINR and Energy Efficiency. *IEEE Access*, *12*, 74444–74455. https://doi.org/10.1109/ACCESS.2024.3405534

[12] Fulford, M. (2018). How a RACI matrix can enhance your risk management program. Ballast Risk Management. Retrieved from https://ballastrisk.com/

[13] Vallejo Díaz, A., Herrera Moya, I., Garabitos Lara, E., & Casilla Victorino, C. K. (2024). Assessment of Urban Wind Potential and the Stakeholders Involved in Energy Decision-Making. Sustainability (2071-1050), 16(4), 1362. https://doi.org/10.3390/su16041362

About the Authors

Marco Pinzaglia

Rome, Italy

Marco Pinzaglia, Engineer at the University of Rome, UniRoma2, and FEMBA Master at Luiss Business School in 2024. I am an expert in cybersecurity, digital transformation, and IT business processes. I have written numerous articles related to cybersecurity, models' impact on governance and compliance, and sustainability. I am an expert and certified ISO27001, expert in management systems (e.g. ISO9001, 20000, 22301), IT cybersecurity

architectures and solutions, and Risk Analysis. I am an expert in process and IT solutions for Supply Chain and Third-Party Security (certified Cybersecurity Insurance Strategy and Third Party Risk Management). I have attended in-depth courses specifically on digital services and innovation (Bocconi, A Scientific Approach to Innovation Management, and Copenhagen Business School - Digital Competition in Digital Services). Since 2024, I have also been Director and Secretary of FembaClub, an international association of managers, and a former MBA. Marco can be contacted at marco.pinzaglia@gmail.com

Dr. Michele Vincenti

Vancouver, BC, Canada

Dr. Michele Vincenti's distinguished academic and professional journey showcases his profound organizational development, leadership, and management consulting expertise. He is a full professor and the MBA Leadership and People Management department Chair at the University of Canada West (UCW). His experience spans various international institutions, marked by significant teaching, research, and professional practice achievements. His contributions to academia and industry and his commitment to mentorship and community involvement underscore his exceptional credentials, making him a notable figure in his field. He can be contacted at michele.vincenti@ucanwest.ca

University Canada West
1461 Granville Street, Vancouver, BC, V6Z 0E5, Canada
www.ucanwest.ca