• • • WHITE PAPER

protiviti®
Global Business Consulting

Optimizing Business Resilience: effective strategies for consolidating Non-Financial Risks in organizations

Introduction

Imagine a global manufacturer reliant on a vast network of suppliers spread worldwide. A sudden geopolitical crisis disrupts the supply of essential raw materials, halting production lines and threatening profitability. In today's volatile business environment, such non-financial risks are far from theoretical; they're real and significant threats.

Over recent years, the importance of Non-Financial Risk (NFR)- including operational, artificial intelligence, ESG and third-party risks - has sharply increased. Companies and executives are increasingly aware that these risks originate from multiple sources, and that one risk event can trigger or intensify others. For example, integrating new technology in a business process creates cybersecurity vulnerabilities that may lead to data breaches and cause operational disruptions, all of which can affect a company’s reputation and regulatory compliance.

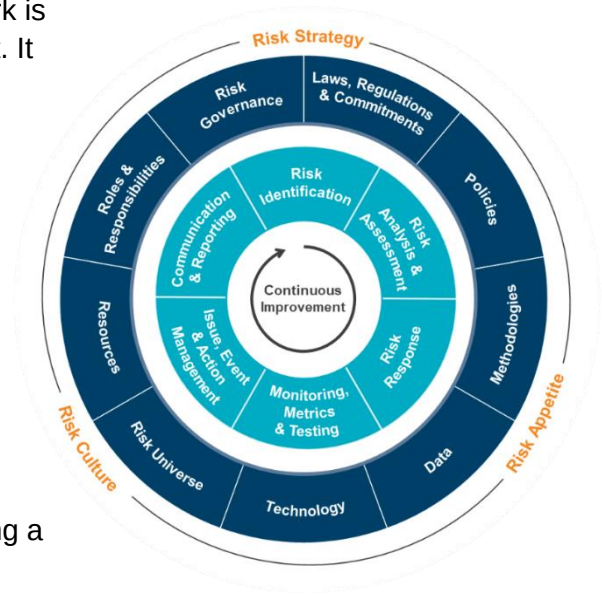
It is a fact that organizations face considerable challenges in managing NFRs due to several factors, such as the complex interplay among various risks, inconsistent risk reporting practices, and a rapidly evolving regulatory and business landscape. To effectively address these issues, it is crucial to adopt a comprehensive NFRs management approach. This approach involves developing a robust framework equipped with tools for identifying, assessing, and mitigating NFRs, all while aligning with the organization’s mid-to-long term risk strategy. The goal is to achieve a cohesive and clear view of the overall risk landscape, thereby enabling informed and strategic decision-making.

Achieving a clear and cohesive view of NFRs within an organization is not an easy endeavor. It requires, at a minimum, establishing a well-defined governance structure with robust oversight mechanisms; gaining a thorough understanding of individual risks while recognizing their interconnections and cumulative impact; implementing a robust data collection method alongside reporting tools; and ensuring continuous monitoring. In this article, we will provide guidance on how organizations can effectively aggregate NFRs, moving from a fragmented view and interpretation of risk to a single cohesive overview that facilitates informed and strategic decision-making in the face of an increasingly volatile business environment.

protiviti®
Global Business Consulting

NFRM Framework supports organizations in having an aggregated overview of NFRs

A robust Non-Financial Risk Management (NFRM) framework is essential for navigating the complexities of risk management. It should address challenges such as the intricate interactions among diverse risk factors, inconsistent risk reporting practices, and a rapidly evolving regulatory and business landscape. To address these issues, Protiviti has developed a holistic NFRM framework (see figure 1) that translates core principles from renowned standards such as COSO ERM, COSO Internal Control, and ISO 31000 into actionable components. These components (or building blocks) support organizations of all maturity levels in refining their operating models and strategically planning their enhancement roadmap.



For example, the NFRM framework offers tools for developing a cohesive and unified overview of NFRs, which offers several significant benefits, such as:

- Holistic NFRs perspective: Offers a unified view of NFRs, enabling a better understanding of how different risks interact and impact the organization.
- Enhanced decision-making: Provides actionable insights that improve the quality of decisions by integrating comprehensive risk data and analysis.
- Improved resource allocation: Helps in prioritizing recourses and investments based on the identified landscape and its potential impact.
- Strengthened risk monitoring and management: Enhances the ability to monitor, manage, and respond to non-financial risks more effectively.

In the following sections, we will dive into how Protiviti's NFRM framework can be leveraged using a structured five-step approach. This approach is designed to create a clear and aggregated overview of non-financial risks, thereby enhancing strategic decision-making and reinforcing risk management practices within the organization. This comprehensive methodology not only addresses current risk management needs but also adapts to evolving challenges, ensuring that organizations are well-equipped to maintain resilience and achieve long-term success.

Step 1: Establishing a well-defined governance structure

The first step in implementing effective NFRM is to establish a clear and robust governance model, the most common being the 'three lines model'. This model delineates specific roles and responsibilities for managing risk within the organization, including those related to non-financial risks.

In the three lines model:

1. The first line consists of business units responsible for day-to-day business activities, including delivering of products and services, management of systems, and IT functions. These units are critical in driving the organization towards its objectives and hold ownership of the risks within their areas. They identify, assess and manage risks directly, ensuring that they are addressed at the source.

   The first line maintains continuous communication with the governing body, providing detailed reports on outcomes and associated risks. Additionally, the first line maintains structures and processes for effective operational risk management. To succeed, the first line must be equipped with appropriate tools, training, and support to proactively manage and mitigate risks.

2. The second line, comprising risk management and compliance functions, provides complementary expertise, support, monitoring and challenge related to risk management. It plays a key role in the development, implementation and continuous improvement of risk management practices, including internal controls, across processes, systems and the organization as a whole. The second line also escalates risk matters when the first line does not address them and provide oversight and analysis to evaluate the adequacy and effectiveness of risk management efforts, guiding and supporting the first line as needed.

3. The third line, represented by the internal audit function, operates independently from management and maintains primary accountability to the governing body. It provided objective assurance and advice to both management and the governing body on the adequacy and effectiveness of governance, risk management, and internal controls, ensuring they align with organizational objectives. The internal audit is crucial for evaluation the overall effectiveness of risk management practices and promoting continuous improvement. Any impairments to its independence or objectivity are reported to the governing body, with safeguards implements as necessary.

To effectively establish this governance model, it is important to clearly define and document the roles, responsibilities, and accountability mechanisms for each of these lines. This includes specifying who is accountable for managing risks, implementing controls, and managing actions. Proper documentation and integration of these elements into daily business practices are essential for maintaining transparency and alignment throughout the organization.

Nevertheless, while the three lines model is theoretically robust, practical implementation can pose challenges. Roles and responsibilities may not always be clearly delineated, which can impede effective risk management and collaboration across the lines. For instance, issues such as insufficient education

for the first line or overlapping responsibilities between the first and second lines can compromise the effectiveness of the model. Addressing these challenges requires ongoing training, clear communication, and periodic reviews to ensure that each line functions effectively and collaboratively.

Step 2: Establishing a risk taxonomy

The second step is to establish a comprehensive and institution-wide risk taxonomy. This involves developing a structured classification system for the various types of (non-financial) risks that an organization has identified. This taxonomy creates a common language and understanding across the organization which is crucial for risk management. The key aspects of risk taxonomy development are:

- **Structured classification**: Develop a detailed and organized classification system that categorizes different types of non-financial risks to ensure clarity and, as much as possible, prevent overlaps which do often happen between various stakeholders. This system should reflect the diverse nature of risks, from operational to reputational and strategic risks.
- **Common language**: Create a unified language for risk management that ensures consistency in how risks are described and communicated across the organization; as well as common understanding amongst stakeholders to facilitate common interpretation of the terms to avoid any misunderstanding.
- **Top-Down and Bottom-Up Structure**: Design the taxonomy to support both top-down and bottom-up risk management approaches. This means identifying overarching risk themes and breaking them down into specific, localized risks within different parts of the organization. This is crucial for aggregation, consolidation and reporting to management, regulatory authorities or business partners.
- **Integration into Risk Management Framework**: Incorporate the taxonomy into the organization's overall risk strategy, appetite, infrastructure and management cycle. This ensures that all relevant risks are considered in the organization's risk management practices and decision-making processes.

Step 3: Implementing risk taxonomy across the organization

The third step in effectively managing NFRs is to implement the risk taxonomy across the organization. This involves mapping the taxonomy to various aspects of the organization, including its structure, processes, controls, and IT systems. The key aspects of implementing risk taxonomy are:

- **Mapping the taxonomy**: Align the risk taxonomy with the organizational structure, i.e., business units, legal entities, and operational processes. This alignment ensures that risks are managed at the appropriate level and within the relevant contexts. The mapping should also include integrating the taxonomy into existing controls and IT systems, facilitating seamless oversight and management.

- **Tailoring oversight**: By mapping risks to specific areas of the organization, you enable more targeted and effective oversight. This helps in identifying which parts of the organization are most exposed to certain non-financial risks and tailoring risk management strategies accordingly.
- **Structured review process**: Given the rapidly evolving regulatory and business environment, it is crucial to establish a structured process for regularly reviewing and updating the risk taxonomy. This review process should be planned and communicated based on factors such as the organization's size, complexity, and geographical scope. Typically, it is advised to conduct reviews annually unless there is a need to perform an off-cycle review prompted by internal or external factors, such as market conditions, geopolitical situations, and organizational changes.

  This ongoing review process ensures that the classification of the different non-financial risks remains updated, incorporating new and emerging risks into the risk management framework. It enables more accurate risk assessment, keeps the organization's risk profile up to date, improves the accuracy of risk reporting and provides decision-makers with the necessary information to support effective decision-making. Moreover, it fosters a common understanding of risks among employees, promoting a risk awareness culture within the company.

Step 4: Establishing a risk data management framework

The fourth step entails setting up a comprehensive data management framework. This framework is vital for ensuring that data related to non-financial risks is accurately collected, managed, and utilized. The key components of the data management framework are:

- **Roles and responsibilities**: Clearly define and assign roles and responsibilities for data creation, usage, and change management.
- **Data collection mechanism**: Implement a clear and robust data collection system to capture information on non-financial risks.
- **Standardized data formats and classifications**: Adopt standardized formats and classifications for data to ensure uniformity across various risk categories.
- **Data quality measurement**: Introduce a methodology for measuring, assessing, and comparing data against established quality target, ensuring that the data remains accurate, relevant and actionable.
- **Data integration and accessibility**: Ensure that data from various sources and systems is available to relevant (internal) stakeholders in a centralized single location.

By establishing this framework, organizations can effectively capture, manage and utilize non-financial risk data, facilitating a more informed and strategic approach to risk management.

Step 5: Integration of risk management technology into business processes

In the fifth step technology tools and systems are integrated into business processes to effectively manage and analyze information on each type of non-financial risk outlined in the risk taxonomy. Technology plays a crucial role in automating, streamlining, and enhancing the efficiency of risk management activities. The key aspects of technology integration are:

- **Automation of risk management processes**: Implement technology solutions that automate repetitive and time-consuming activities.
- **Streamlining processes**: Utilize technology to streamline risk management processes, making them more efficient and less prone to errors.
- **Enhanced analysis and reporting**: Leverage technology for advanced risk analysis and reporting.

Integrating technology tools into business processes ensures that NFRM is not only more efficient but also more effective. By consolidating data sources and automating processes, organizations can achieve a complete and timely view of their risk landscape, ultimately improving their ability to respond to and manage potential threats.

The journey towards effective NFRM

Effective NFRM is a strategic necessity for organizations operating in today's complex and dynamic business landscape. As we conclude this whitepaper, it’s crucial to underscore the key activities suggested to aggregate NFRs by using Protiviti’s NFRM framework.

At its core, the NFRM framework offers a systematic approach for organizations to comprehensively identify, assess, and mitigate non-financial risks. By leveraging established principles from standards such as COSO ERM, COSO Internal Control, and ISO 31000, this framework translates theoretical principles into practical components (or building blocks) that can be tailored to organizations of varying sizes and complexities.

Key takeaways:

1. **Governance model**: Establishing a governance model is fundamental. This model provides a solid foundation for managing non-financial risks by ensuring clear assignment of responsibilities, maintaining accountability, and integrating risk management processes into daily operations. Clear delineation of roles and responsibilities is paramount for effective NFRM. Adopting the three lines model and clearly documenting roles and responsibilities fosters collaboration and accountability. However, it is essential to address challenges such as overlapping responsibilities and expertise gaps to ensure practical effectiveness.
2. **Risk taxonomy**: Developing a comprehensive risk taxonomy is essential for organizing and understanding non-financial risks. This taxonomy acts as the cornerstone for all risk management activities, offering a unified language and understanding across the

organization. This taxonomy acts as the cornerstone for all risk management activities, creating a unified language and framework across the organization. By implementing a structured review process, organizations can keep their risk taxonomy relevant and updated, incorporating emerging risks into their management strategies.

3. **Data management**: A robust data management framework is critical for NFRM. Integrating technology tools into business processes allows organizations to gather timely and accurate data on non-financial risks. Standardizing data formats and classifications ensures consistency across risk categories, which supports informed decision-making and enhances risk reporting.
4. **Technology Integration**: Integrating technology solutions is pivotal in streamlining NFRM processes and improving efficiency in responding to potential threats. Ensuring that these tools are part of a unified IT platform provides a comprehensive view of the organization's risk exposure.

Overall, while the journey towards effective NFRM presents challenges, the rewards in enhanced risk awareness and management are significant. By implementing the foundational the building blocks outlined in this whitepaper – whether starting from scratch or enhancing an existing process - organizations can greatly improve their resilience to non-financial risks, enhance decision-making processes, and secure their long-term success. Moving forward, organizations must remain agile and adaptable, continually reassessing and refining their NFRM strategies to meet the evolving demands of the business environment.

AUTHORS:

Laura Benavides

Manager, Risk Management and Compliance

Giovanni Zennaro

Manager, Risk Management and Compliance

CONTACTS:

Luca Medizza

Managing Director

luca.medizza@protiviti.it

Ellen Holder

Managing Director

ellen.holder@protiviti.de

Peter Berger

Associate Director

peter.berger@protiviti.nl