Capgemini invent

NON-FINANCIAL RISK MANAGEMENT

> WHILE IT MAY NOT BE POSSIBLE TO FULLY AVOID CERTAIN NON-FINANCIAL RISKS, IT IS POSSIBLE TO IMPROVE THE RESILIENCE TO SUCH EVENTS

-Basel Commitee on Banking Supervision, 2020

CONTENTS

Inventive Finance, Risk & Compliance

Inventive Finance, Risk and Compliance (Inventive FRC) supports the respective functions within banks to move fast to stay compliant at minimum cost as well as to help their organizations compete through digital innovation. The key is for the FRC functions to add value by leveraging data solutions embedding regulatory competences.

€ 500 bn

Total amount of damage resulted from inadequate or failed internal processes

5-15%

Cost reduction by using the FRC framework

To transform their business functions, banks need to be inventive. We identified five areas in which financial institutions can level-up their business and bring to life what's next:

- FRC Data Platform
- Credit risk
- Non-Financial Risk
- Compliance
- Finance

Our inventive approach empowers banks to tackle the challenges of transformation. We welcome you to read on and find out more.

Inventive Non-Financial Risk Management

Operational risk functions need to improve the way they use operational risk data to detect, understand and predict operational risk events. Across the globe, operational risk related losses are increasing at alarming rates. Between 2011 and 2017 alone, the total amount of damage caused by inadequate operational risk management was more than € 500 bn, and much of that damage resulted from inadequate or failed internal processes or from people, systems, or external events.

Data breaches, cyberattacks, and system failures, as well as external and internal fraud, represent the top challenges organizations and especially financial institutions are currently facing. Businesses are becoming victims of ransomware attacks at the alarming rate of one every 14 seconds.

By far the most critical success factors for transformation towards an effective operational risk management approach are the right organizational culture and an adequate governance structure with "tone from the top". In addition, a holistic and comprehensive view of all risks is important. The first step is usually to take a critical review of the existing business model, then determine risk capacity and appetite.

Finally, the fact that the Basel Committee on Banking Supervision published 2 new consultative papers "Principles for the sound management of operational risk" and "Principles for operational resilience" emphasizes the importance of sound management of operational risk, especially after the lessons learned and challenges organizations are facing in times of global pandemic COVID-19.

While it may not be possible to avoid certain operational risks, such as a pandemic, it is possible to improve the resilience of a bank's operations to such events.

Our Publications

Non-Financial Risk Blog Series

In the recent years, we have helped many financial institutions to manage their challenges related to the Non-Financial Risk Management. While some of our projects were products of internal or external inspections, some organizations acted proactively to further improve their Non-Financial Risk Management.

In our blogs, we provide an overview about the Non-Financial Risk challenges and evolution in the last decade as well as an outlook about the main trends. In addition, we focus on some specific areas that represent sources of increased Non-Financial risks and provide best practices from European financial institutions.

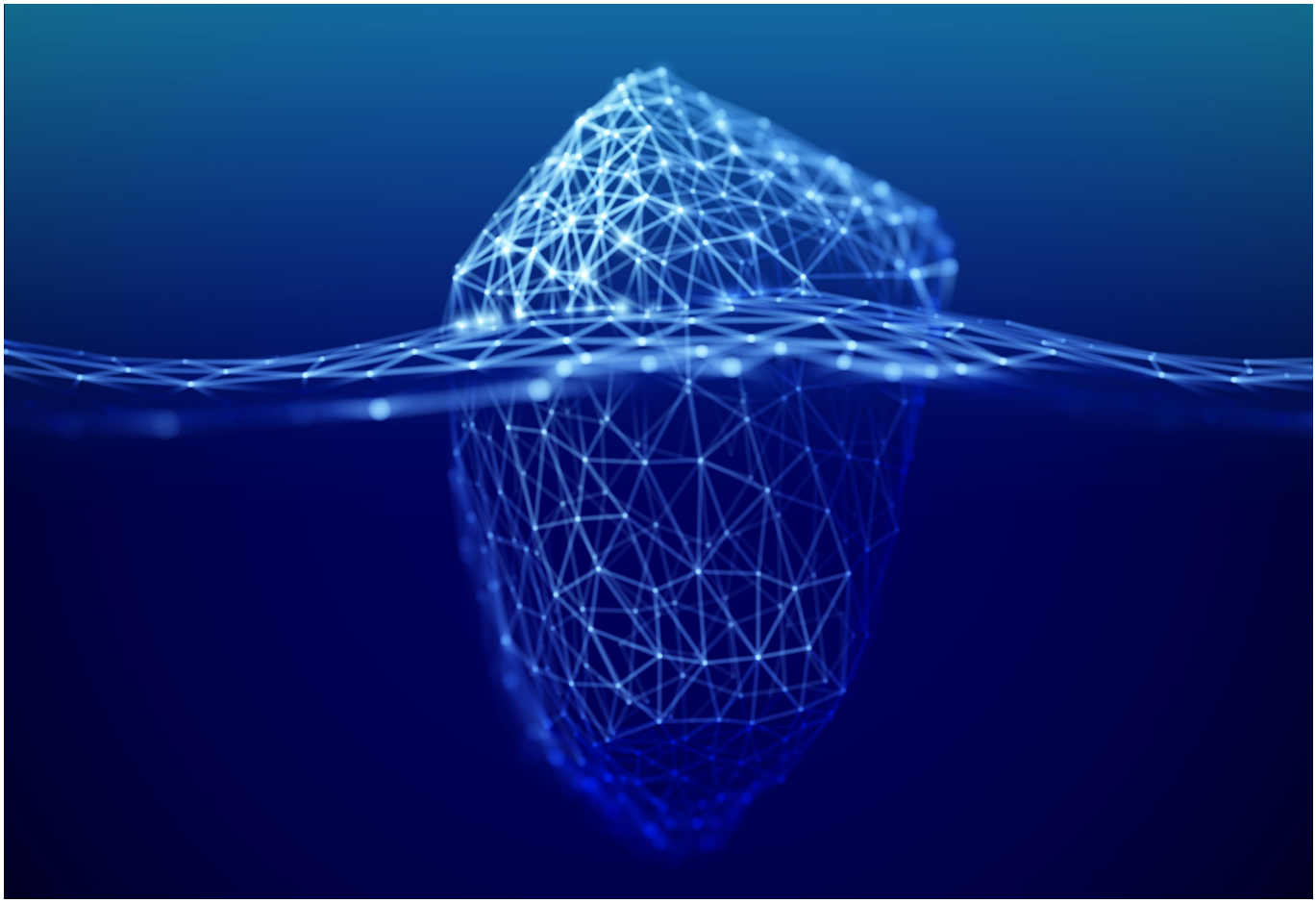
1. **"Non-Financial Risk: Be a pioneer in key areas before you lead the list of fines" –** Impact of Non-Financial Risk Management on financial institutions and main trends on the market
   -Erekle Tolordava and Hans Lohrmann

2. **"Non-Financial Risk – Incident Management" –** Incident Management is a homework for any institution, but most of them struggle to establish a sound incident management process. In our article we provide some key elements for a sound incident management process.
   -Erekle Tolordava, Crispijn Groeneveld and Marco Meyer

3. **"Risk culture: from reactive to preemptive" –** one of the key trends on the market is the increased focus on improved risk culture, to pro-actively prevent Non-Financial risk incidents.
   -Erekle Tolordava, John Giurgius, Christopher Beck and Dr. Rita Motzigkeit

4. **"The changing face of Operational Risk" –** The risks facing financial services players are multiplying and evolving. Creating a dynamic and proactive risk culture is essential to prevent serious losses.
   -Erekle Tolordava, Dr. Rita Motzigkeit and Kerem Cigerli

1. Non-Financial Risk: be a pioneer in key areas before you lead the list of fines



In 2018 the sum of fines for the three largest infringements of non-financial risk regulations among European banks amounted to €5,420,000,000. Losses caused by Non-Financial Risks are increasing at an alarming rate worldwide.

Non-Financial Risk (NFR) is one of the essential drivers of risk within a bank. In recent times these risks have increasingly become the root cause of significant losses. Between 2011 and 2017 alone, the total amount of NFR-related losses amounted to more than EUR 500 billion. In particular, the main reasons for this can be traced to inadequate or failed management approaches of internal processes, systems, human error and external events. Non-Financial Risk can quickly take on large proportions and spread deep within the business. When this occurs NFR can also indirectly affect business areas not directly involved with the NFR incident. New risks, such as cyber risk and contract risk, can negatively affect a company's image.

The increasing rate of NFR incidence is a call to action, with companies now attacked every 14 seconds by cyber-attacks. In fact, the average cost of lost and stolen data due to data breaches amounts to €125,000 per person.

Only the following holistic approach will provide sustainable security and minimize Non-Financial Risk.

The foundation for mitigating non-financial risk will be anchored with the organization in the form of specialized governance and cultural change.

Changes to internal and external conditions and the consequent impact on an organization's risk situation require an adjustment to the organizational structure used for risk management.

More than ever, the organization must react to new and increased Non-Financial Risk events. For this purpose, dedicated teams of specialists for Non-Financial Risks must be established. Their role is foremost to manage risk of new dangers from cyber-attacks across the entire risk management process.

To support the establishment of specialist teams, it is necessary to closely integrate them with operational employees. A high level of awareness and expanded awareness must be created. Change in organization and governance can only be ensured in the long term through cultural change. Talented risk managers must be brought to the organization who are familiar with the new data-driven approaches and the technologies available on the market.

Non-Financial Risk are constantly evolving in terms of scale and complexity and should be examined across four fundamental areas.

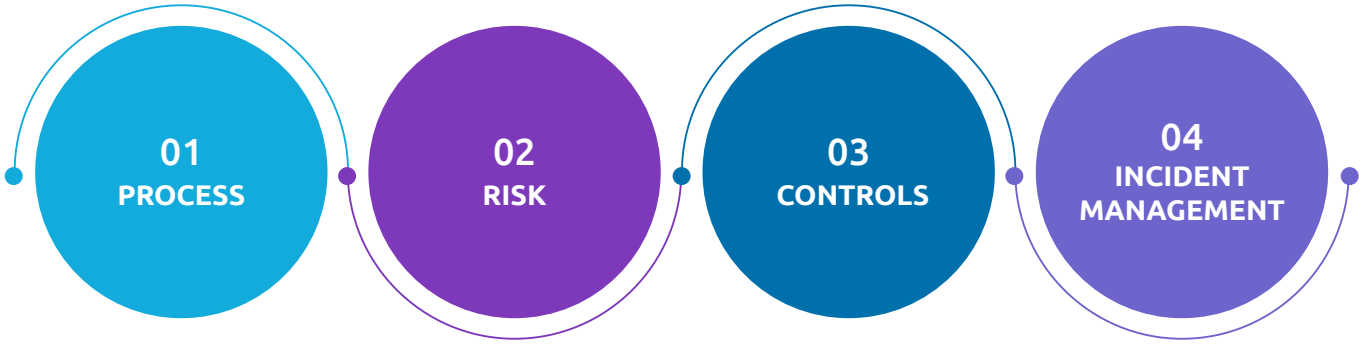
Non-Financial Risk never stands still. Due to internal and external influences, it is subject to constant change which can lead to assessments of low risk today but assume dangerous proportions tomorrow.

A continuous evaluation of NFR is required. Evaluation and risk mitigation can be significantly improved by standardizing, harmonizing and automating the underlying processes.

In addition, a clear definition and allocation of NFRs to specific business areas as well as an evaluation of their potential business impact is of great relevance. This is the only way to assign specific controls to individual NFRs and establish an optimal control environment for risk mitigation.

In order to not only evaluate existing risks and take precautions before an incident occurs, but also to react quickly to the incidents and make deductions for the future, it is important to establish modern technology.

Strategic orientation of organization & governance



Supported by modern technology based on artificial intelligence

Appropriate tools must be carefully selected and implemented in the daily business process.

Modern tools for risk forecasting and operational risk efficiency, supported by artificial intelligence, must be established to establish an efficient Non-Financial Risk management process. Only new types of technology can respond adequately to new needs. A first step, for example, is the establishment of a comprehensive database that identifies individual risks in detail, derives a reasonable clustering and assigns appropriate controls. Only through the holistic recording of potential risks and events is it possible to include artificial intelligence.

The authors strongly believe that Non-Financial Risk management provides the basis not only for selective optimization, but also for holistic alignment of risk management with current requirements. This holistic approach can raise a bank's performance to a new level.

Banks can overcome the challenges involved in the transformation of risk management to include Non-Financial Risk by a reasonable effort. Capgemini Invent, with experience in NFR management in more than 15 European countries, can support this process with a variety of projects and expertise.

2. Non-Financial Risk: Incident Management

Data availability is fundamental for effective incident management.

Incident management in Non-Financial Risk Management (NFRM) encompasses the identification, capture, and analysis of risks and the elaboration of respective actions. The establishment of an effective incident management solution promotes faster response to risks, and makes it possible to proactively address potential vulnerabilities and prevent further incidents. It identifies potential sources of risks (e.g., implementation of a new product, outsourcing of services, external incidents, etc.), provides the necessary data, and triggers subsequent risk assessments in every impacted unit. In one word, sound incident management simplifies Non-Financial Risk Management. In addition, process efficiency and effectiveness can be increased through the use of new technologies.

Data availability is fundamental for effective incident management. At Capgemini Invent, we are pleased to provide you with structural recommendations based on the cross-sector best practices discovered during our various projects across Europe:

Common taxonomy:

Development of a mutually exclusive and comprehensively exhaustive risk taxonomy of actual risk events and an effective risk identification process; alignment of the taxonomy with external sources to facilitate the integration of external data into the internal (incident) database.

Governance and organization:

This involves establishing a clear structure with explicit ownership and responsibilities along the three lines of defense. In particular, the responsibilities between the first and second lines of defense should be clearly articulated within the organization and a permanent control team should be created to review the activities and controls performed by the first line and to report to both the first and second lines in order to permanently monitor operational risks and promote a sound risk culture.

People and culture:

This involves living a culture that recognizes the importance of managing Non-Financial Risks to the extent that everybody in the organization is aware of the risks triggered by their activities regardless of whether they are directly or indirectly affected by them. One of the best practices to support risk culture is the establishment of a respective risk culture entity in the organization. The entity should be sponsored by different departments, such as Risk, Legal, Compliance, and HR. Beyond that, the community should foster knowledge sharing, leverage best practices, and encourage actively challenging existing methods.

Technology and tools:

This involves implementing tools supported by new technologies to examine historical data on losses and to identify (potential) correlations and patterns. New technology will also help to maintain a more complete risk inventory and better integrate external data (e.g., such as the data from ORX).

In addition to the above-listed prerequisites, incident management furthers improves when best practices are implemented:

Risk identification and documentation

When identifying an incident, a comprehensive picture of the incident must be captured. Appropriate governance and organization, combined with the right people and culture, leverage the identification process. Lastly, a well-developed risk taxonomy facilitates clear and appropriate categorization.

Assessment and documentation of root causes

Every identified incident must be analyzed to its root cause. Storing this information in a central database promotes an accelerated initial analysis and makes it possible to proactively reduce incident frequency and solve the root cause of every NFR problem.

Documentation of (potential) impacts of each incident

The impact of each incident to the enterprise is documented, resulting in measurable outcomes, making results comparable and improving audit tracking.

Creation of an action plan

The fundamental remediation of historical incidents is a solid basis to prevent potential incidents in the future. Every remediation action should be defined by considering the link between the root cause and the (potential) impact of each incident and it should target failing controls and processes. Remediation actions can vary, from automating failing processes to questioning management bonuses, by repeatedly incurring incidents.

Incident management using modern applications

A solid incident management tool supports the above best practices and provides a dashboard with customizable outputs to track and report incidents. Automated mail triggers include escalation and security processes. To further improve the identification, documentation, and assessment of incidents, the possibility to couple big data with advanced analytics. This can be further enhanced by using natural language processing and optical character recognition. Machine learning, APIs, knowledge base, and SLAs support should also be facilitated.

3. Risk Culture: from Reactive to Preemptive

Organizations with a preemptive risk culture are better equipped to mitigate, minimize, and avoid risks due to the proactivity and risk awareness of their associates.

The recent evolution of risk culture

Most companies have extensive experience with risk management, and financial institutions firmly belong in this group. However, the 2008 financial crisis demonstrated that financial institutions had behavioral shortcomings with respect to how risk and internal controls were measured and applied – often in contrast to formal process protocols. This behavior led to unimaginable consequences and contributed to the deepening of the financial crisis. Regulators devised a number of post-financial crisis measures to close this gap, including a formal guidance on how financial institutions must maintain a risk culture.

Many chief level executives regard this evolution as a genuine opportunity to make their organizations more sustainable and resilient in the face of future crises. They engaged in serious self-assessment of their risk cultures, determined where deficiencies existed, and then began the long-term programs necessary to transform their organization's behaviors related to risk. By doing so, COOs, CROs, CEOs and boards became proactive in discussing the internal tradeoffs for risk and control. By setting up the top management tone communicated to internal stakeholders giving direction to the overall organizational risk culture, they managed to make the cultural aspects of risk issues more visible, better understood, and more widely accepted across the entire organization. The top management tone also allowed them the opportunity to reestablish credibility with regulators and the public while they continued to fulfill their essential mandate within the economy. Financial institutions thus formalized company preemptive cultures centered around self-awareness of risk. This risk awareness is the core instrument designed to ensure their overall stability and sustainability into the future. Risk culture is the combination of the awareness, behavior, competencies, and expertise exercised within the context of the technologies and data quality used to perform daily tasks.

Preemptive risk culture stresses the proactivity of internal stakeholders by enabling them through well-communicated risk governance mechanism. The aforementioned proactivity is further empowered by clearly defined risk management processes.

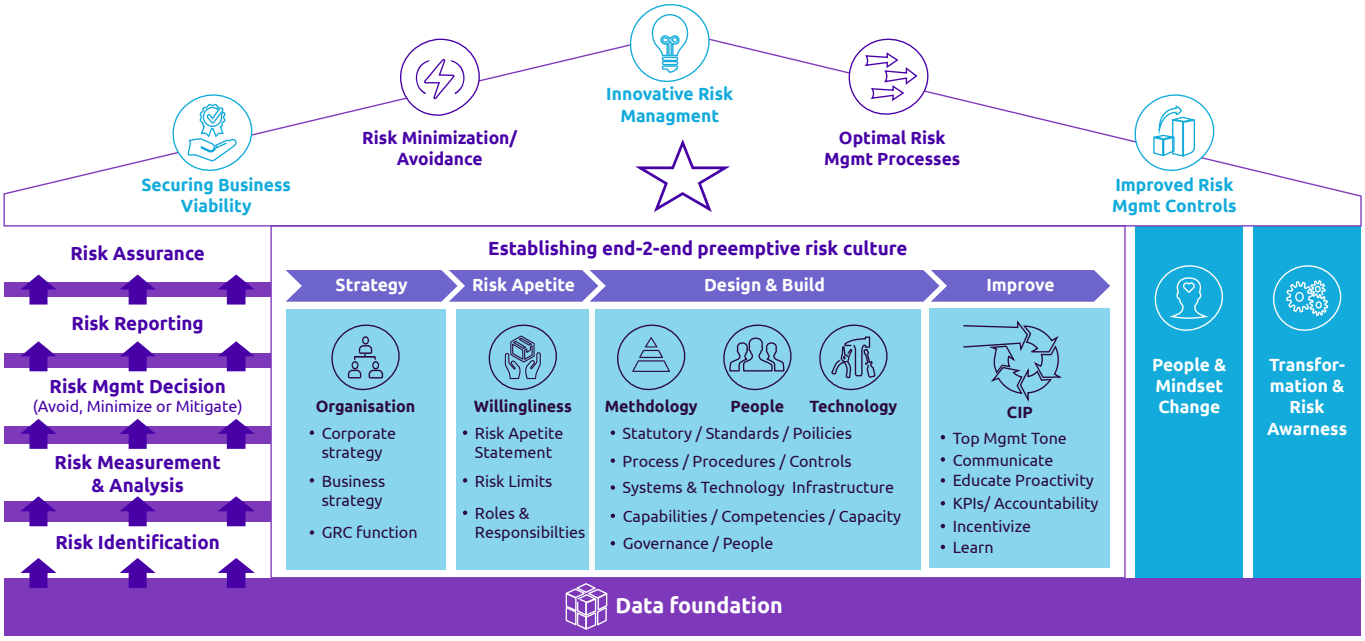
The pandemic and risk culture

The pandemic is resulting in a global economic recession that could lead to permanent shifts in competition across the global business landscape. Although it is too soon to know how a recovery will play out, we do know that firms with mature risk cultures are better equipped to navigate the economic downturn to ensure their survival. We expect risk culture maturity to receive increased attention from regulators in the upcoming months. Consequently, organizations should focus their attention to enhance their risk culture, thus ensuring competitiveness and regulatory compliance.

Risk culture in dynamically changing world

The development of preemptive risk culture in all types of companies – not only limited to financial institutions – will be immensely valuable in helping companies adapt to the dynamically and continuously changing operational ecosystem. Our experience in improving risk culture has led us to conclude the following key findings that indicate a mature risk culture setup:

1. Review and update risk appetite statement in alignment with corporate strategy.
2. Set up a risk governance mechanism that promotes self-awareness, track risk metrics, and hold employees accountable in conjunction to incentivizing them to proactively operate with enhanced risk awareness.
3. Design risk management processes and seek accreditation such as IEC 31010:2019 & ISO 31000:2018 (relevant for FS and non-FS).
4. Improve risk processes continuously, communicate and educate employees about risk awareness.
5. Enhance operational efficiency to ensure high data quality leading to better risk identification, measurement, and assurance.
6. Proactively invest in risk management IT systems to increase resilience to unidentified risks and visibility in tracking identified risks.



Next steps – and validation for a solid preemptive risk culture

The concept of the risk culture should be a core part of a company's strategy. Companies can benefit from acting on the lessons learned by financial institutions in the 2008 financial crisis and be proactive given the reactions taken by regulators to curb the behavioral shortcomings of financial institutions. Many financial institutions are already at the beginning of the risk culture journey and we are expecting an increase in efforts to enhance risk culture maturity to cope with market changes.

- **First**, a functioning preemptive risk culture enables the entire corporation to solve risk problems and take actions at an individual level. In an economic environment where the full scope of risks is not known, this capability will become a vital asset to bolster the firm's ability to react to disruption.
- **Second,** organizations that establish a mature preemptive risk culture can better manage their risks and reduce risk of failure, even when they must deal with extreme unexpected events.
- **Third,** building a mature preemptive risk culture is a dynamic and continuous process that requires time, patience, and effort, but it offers long-lasting resilience during times of financial stress.
- **Fourth,** to build an organization that is stable and sustainable over a long period of time, risk culture is essential. Even outside the scope of the current pandemic, recent years have seen an increase in natural disasters, incidences of cyberattacks and data breaches that are becoming more and more prevalent.
- **Fifth,** in a business system that is set up to anticipate as much as possible and be flexible with procedures when the worst happens, coping mechanisms within risk cultures become second nature for employees and managers alike.

Preemptive risk culture would not only enable organizations to resiliently thrive within uncertain and constantly changing environment, but it would rather create a competitive advantage providing an edge of swiftly and efficiently swaying through unfavorable market movements whether exogenous or endogenous.

4. The changing face of Operatinal Risk

The risks facing financial services players are multiply-ing and evolving. Creating a dynamic and proactive risk culture is essential to prevent serious losses.

From the ever-present threat of cyber-attack, to the unexpected and sudden impact of a global pandemic, operational risk is a fact of life in the financial industry. And while oper-ational risk management is critical, the practice is still in its infancy.

Despite this immaturity, its relevance is highlighted by the continuous revisions and re -views published by the Basel Committee on Banking Supervision (the Committee). Their more recent being the publication of a consultative paper with proposed updates to the Principles for the Sound Management of Operational Risk (PSMOR), as well as the newly minted Principles for Operational Resilience (POR), both in 2020.

Both documents are at the forefront of current affairs in this industry and offer a glimpse of the regulatory challenges financial institutions will face in the future. In this article, we offer an overview of the updates and new principles, and consider the impact on Finance, Risk and Compliance (FRC) functions.

In short

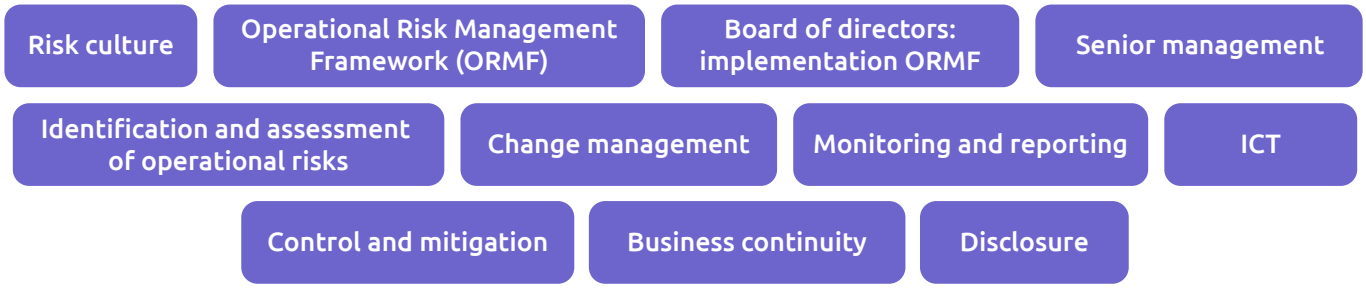
- Additions and changes to the Principles for the Sound Management of Operational Risk include:
- More details to each specification in each principle
- Fleshed out roles and responsibilities of the board of
- directors and senior management
- A fully new principle on Information and Communication Technology (ICT)

The Principles for Operational Resilience aim to:

- Improve banks' ability to deliver critical operations through disruptions
- Strengthen banks' ability to absorb operational risk-related events

The PSMOR: and then there were twelve

Since the adoption of the PSMOR in 2011, the operational risks faced by financial institutions have increased and evolved. The current consultative paper addresses this changed landscape in the following twelve principles:



The following additions are impending:

- Expanded requirements on risk culture, code of conduct, and ethical be-havior
- Explicit delineations of the roles and responsibilities of the board, senior management and the three lines of defense
- A comprehensive non-exhaustive list of tools to identify and assess opera-tional risks, such as operational risk event data, self-assessments, event data and scenario analyses
- A new principle (principle 10) addressing the implementation of sound ICT: its aims, its maintenance, and the roles and responsibilities related to them

The BCBS has published a paper on cyber security.

The following changes were proposed:

- A request for the inclusion of a standardized and fully developed Operational Risk Management Framework (ORMF).
- A call for clear-cut definitions of processes and controls regarding the re-view and approval for new products, processes, and systems and that these should be monitored by a dedicated change manager
- Demands for the analysis of severe but plausible disruption scenarios and the corresponding business continuity planning (e.g.: thresholds, business impact analysis, discovery and recovery procedures)

The POR: brace for impact

The Principles for Operational Resilience were developed and proposed by the Committee to mitigate operational risks and to strengthen operational resilience in this industry. The latest updates aim to enable banks to deliver critical operations through disruption. Their objectives are as follows:

Promote a principles-based approach to improving operational resilience – the ability of a bank to deliver critical operations through disruption.

Reflect any initial lessons learned from the impact of the Covid-19 pandemic.

Ensure that existing risk management frameworks, business continuity plans, and third-party dependency-management are implemented consistently within the organization.

The seven newly designed POR address many critical incidents faced by financial institu-tions, amongst them the Covid-19 pandemic and a rise in cyber-attacks. The scope lies primarily within:

1. Governance
2. Operational risk management
3. Business continuity planning and testing
4. Mapping interconnections and interdependencies
5. Third-party dependency management
6. Incident management
7. ICT including cyber security

With respect to ICT, the Committee sets requirements on how the physical and logical design of information technology and communication systems need to be met by banks. This includes the individual hardware and software components, relevant data and the operating environment. Additionally, a documented ICT policy incorporating the increas-ing issue of cyber security is expected from banks.

When suggesting these principles, the Committee considered third-party activities where failure would lead to the disruption of vital services. This was especially the case with regard to major institutions with a high market share and globally interconnected opera-tions where consequences might represent a serious potential for danger in terms of the non -functioning of the real economy and for financial instability.

Moreover, the POR require that banks reflect on any initial lessons learned from the im-pact of Covid-19 in order to improve the pain points in their operations. Simultaneously, banks should ensure that their existing risk management frameworks, business continuity plans, and third-party dependency-management are implemented consistently within the organization.

How will these changes affect the FRC function?

There are three distinct challenges: risk culture, roles and responsibilities and risk assessment.

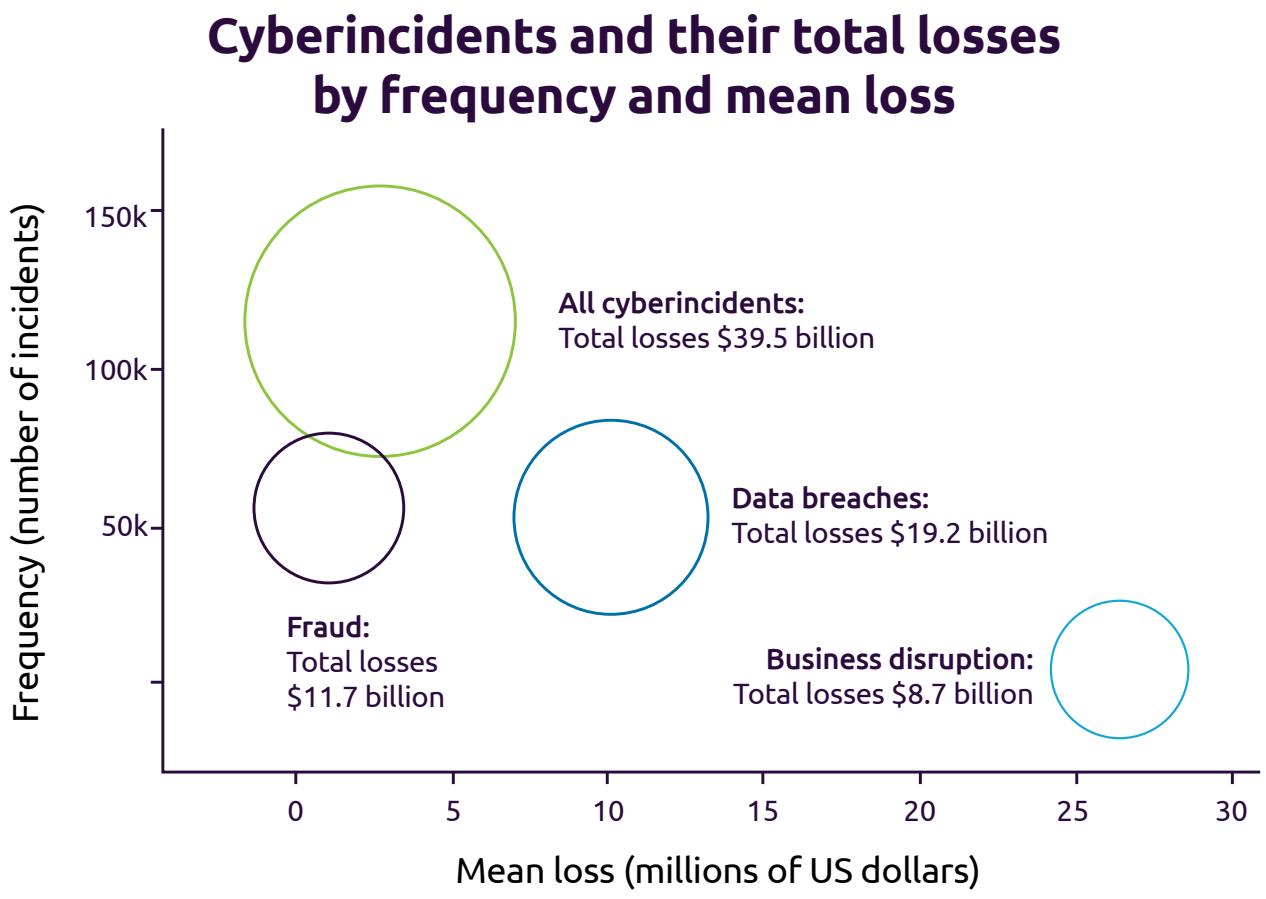
Risk culture includes setting standards and incentives for professional behavior. Roles and responsibilities refer to explicitly delineating the roles and responsibilities of the board and senior management, as well as the three lines of defense, by which we refer to a widely used model for managing risk. Risk assessment comprises choosing and set-ting up the tools to identify and assess operational risks (e.g. event data, self-assessments, and scenario analyses). Responding to these challenges can require fun-damental changes both operationally and institutionally.

At Capgemini Invent, we have many years of expertise in helping financial intuitions en-sure regulatory compliance throughout all corporate functions on a global level. We have drawn on this experience to develop enhanced risk management solutions to tackling the three key challenges:

Risk Culture: The concept of a risk culture should be a core part of a company's strategy. Firms need to establish a mature preemptive risk culture to better manage their risks and reduce risks of failure, even when they are dealing with extreme unexpected events. The building of a risk culture is a dynamic and ongoing process, which enables organizations to resiliently thrive within an uncertain and constantly changing environment. Getting this right can create a competitive advantage by providing the agility to quickly and efficiently navigate through unfavorable market conditions, whether external or internal to the financial industry. Find more details about our preemptive risk culture concept in our Risk Culture Blog.

Roles and responsibilities: Understanding both current and future roles and responsibilities in an organization is the first step in a business optimization process. Organizations need to be clear on their degree of compliance with the recently introduced Basel Committee on Banking Supervision (BCBS) requirements. To support our clients with this, we have developed an extensive governmental and organizational assessment providing guidance on ensuring a compli-ant corporate structure. The Capgemini Invent governmental and organizational assessment uses customized questions to examine any compliance gap and helps to prioritize remedial actions with the key stakeholders.

Risk assessment: The BCBS formulated specific risk management measures as part of its ICT policy, including access controls, critical information asset protection and identity management, to ensure that appropriate risk mitigation strategies are in place. ICT, and cyber security in particular, is embedded in an evolving threat land-scape. A recent study highlights the extent of the average losses for different types of incidents across different economic sectors, as visualized in the diagram below:



Source: Aldasoro et al. (2020) The drivers of cyber risk. BIS working papers, No. 865, May 2020. Graphic by Capgemini (2020)

An intelligent response

At Capgemini Invent, we have created and use various empirical and analytical tools with enhanced visualization, such as our Incident Management Tool. This intelligent tool sup -ports the identification, capture, and analysis of risks, as well as the elaboration of next actions. It enables our clients to proactively address potential vulnerabilities, promote a faster response to risks, and prevent further incidents. Furthermore, this solid Incident Management Tool provides a dashboard with customizable outputs to track and report incidents. It is compatible with the latest technologies, such as natural language pro-cessing, optical character recognition, machine learning, etc. You can find more details about our Incident Management Tool and best practices in our Incident Management Blog.

Inventive Finance, Risk & Compliance from Capgemini Invent helps Finance, Risk and Compliance teams in the financial sector address critical challenges. This article focuses on operational risk.

Stay tuned for further updates on the PSMOR and POR by Capgemini Invent.

This blog is authored by Erekle Tolordava, Dr. Rita Motzigkeit and Kerem Cigerli.

CONTACTS

Ulrich Windheuser
Head of Inventive Finance, Risk & Compliance DACH
ulrich.windheuser@capgemini.com

Joachim von Puttkamer
Head of Financial Services Central Europe
joachim.von.puttkamer@capgemini.com

Peter Stähler
Head of Risk & Regulatory Innovation DACH
peter.staehler@capgemini.com

Erekle Tolordava
Senior Manager – Risk & Regulatory Innovation
erekle.tolordava@capgemini.com

About Capgemini Invent

As the digital innovation, consulting and transformation brand of the Capgemini Group, Capgemini Invent helps CxOs envision and build what's next for their organizations. Located in more than 30 offices and 25 creative studios around the world, its 7,000+ strong team combines strategy, technology, data science and creative design with deep industry expertise and insights, to develop new digital solutions and business models of the future.

Capgemini Invent is an integral part of Capgemini, a global leader in consulting, digital transformation, technology, and engineering services. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year+ heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. A responsible and multicultural company of 265,000 people in nearly 50 countries, Capgemini's purpose is to unleash human energy through technology for an inclusive and sustainable future. With Altran, the Group reported 2019 combined global revenues of €17 billion

Visit us at

www.capgemini.com/invent