CAPCO

NON-FINANCIAL RISK:

THE KEY INGREDIENTS TO DERIVE ORGANIZATIONAL VALUE

CONTENTS

INTRODUCTION

How do we prepare for the future with so many risks to consider? It is no wonder that risk continues to factor into the top list of priorities for CEOs in 2020[1]. Understanding risk, and taking proactive steps towards change, are the key ingredients to derive value for the future.

Wherever financial institutions operate today, they all share a collective need to balance limited resources, assess evolving risk factors, comply with regulations, and better manage their data. While risk comes in various shapes and sizes, non-financial risk (NFR) is a growing area of focus across organizations. The NFR scope is vast, covering a range of risks from cyber, financial crime and fraud to regulatory compliance, legal and resilience risk. These risks may be caused by people, inadequate or failed processes, data or systems, or even external events which can have an adverse impact on an organization and its daily business activities. To prevent calamity, firms which take actions to protect their reputations and revenue can mitigate the challenges from NFRs.

In this article, we examine NFR challenges and propose recommendations in the following areas:

- Anticipating regulatory focus
- Managing data using analytics
- Embedding operational resilience
- Executing a NFR operating model.

ANTICIPATING REGULATORY FOCUS

1. Increasing capital requirements for NFRs

Traditionally, risk metrics and associated reporting have focused on more easily quantifiable financial risks such as credit or market risk. However, in recent years, with an increased awareness and frequency of IT failures, cyber-attacks and other non-financial breaches, the importance of NFR has begun to be more understood.

Banks are increasingly identifying and understanding NFRs that were previously bypassed, such as people risk, model risk and climate risk. Even for NFRs that are better understood, such as operational risk, the overall impact on organizations has typically been underestimated whereas now, a gradual change to a more conservative approach is being adopted.

Given these trends, and via both the Internal Capital Adequacy Assessment Process (ICAAP) and Supervisory Review and Evaluation Process (SREP)[2], financial institutions can expect **Pillar 2 capital requirements to continue increasing**. Pillar 2 requirements apply in addition to the minimum Pillar 1 capital requirements and cover risks not covered by Pillar 1, namely credit, market, and operational risk.

The diagram below demonstrates the interaction between ICAAP and SREP:

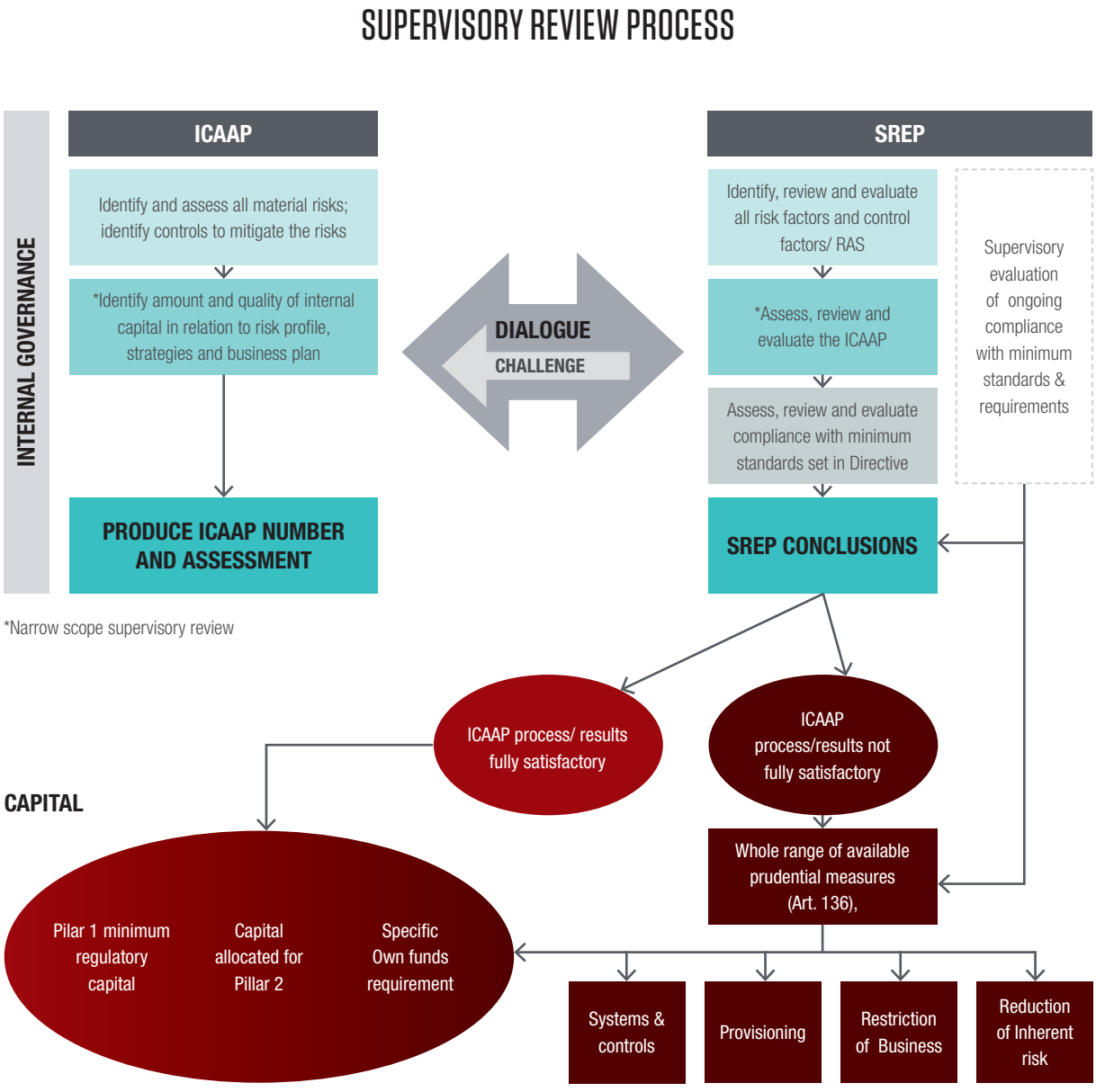


Figure 1: Committee of European Banking Supervisors, 'Guidelines on the Application of the Supervisory Review Process under Pillar 2'

Initially, risks are identified and assessed via ICAAP and then evaluated in SREP. Given that banks have a clearer and better understanding of their NFRs now than in the past, ICAAP is identifying ever more material NFRs. The knock-on effect is that firms are being forced to set aside additional capital because of past NFR events.

The importance of NFR has not escaped the eyes of regulators, who are re-focusing their efforts.

There are numerous examples of regulators imposing large fines on firms that are not managing their NFRs well. For instance, in recent years:

- A French investment bank received a $9 billion fine for sanctions violations in May 2015[3]
- When a UK retail bank's IT systems failed in April 2018, this not only caused £330 million in direct fixes, but also led to the bank losing 80,000 customers and is still under regulatory review[4]
- A US investment bank received a $3 billion fine for conduct breaches in October 2020.[5]

The French investment bank responded by ring-fencing its compliance function, ensuring its independence and embarking on a group-wide ethical culture shift[6]. The UK retail bank responded by firing their CEO and rolling out widespread organizational changes within its IT department as well as improvements to their incident handling[7].

In the case of the US investment bank, the Federal Reserve issued a cease-and-desist order[8] requiring: 1) Improvements to Corporate Governance and Management Oversight, 2) Upgrades to the Anti-bribery and Corruption Program and 3) Transaction Due Diligence on top of the fine. The firm has also already started the process of recouping $174 million from senior executives with oversight of the case.

More generally, banks are doubling down on stress-testing their risk frameworks, identifying and remediating gaps as well as embedding cultural improvements towards NFR. These changes are being made to minimize the chances and impact of future NFR events. Firms need to ensure they have strong controls in place now, across all three lines of defense, otherwise they will be open to significant financial risk.

2. New modelling requirements for NFR

An ever-increasing possibility is a wholesale adoption of industry standardized and mandated (Standardized Measurement Approach or SMA) measurement of non-financial risks rather than internal modelling of non-financial risk events (Advanced Measurement Approach or AMA), which is the current norm. This idea was first proposed by the Basel Committee in 2016[9].

The rationale behind the proposal is that banks currently do not objectively assess their non-financial risks. Standardizing this across the industry will allow for risk-measurement comparisons across organizations and simplifies the assessment process for regulators.

Thus far, the uptake for the SMA process has been limited to regulators in Europe (EBA), Australia (APRA) and Canada (OSFI) with decisions pending from regulators in countries such as the US and UK[10]. The table below provides an overview of the uptake in key markets of the standardized approach:

Jurisdiction (regulator)	Confirmation Date	Loss History Included	Loss data for smaller institutions	Higher Threshold	Capital Impact compared to current approaches	Implementation timeline	Comment
Australia (APRA)	12.06.19	✗	NA	NA	Neutral	2021	AUD versions of the calculation thresholds provided
Europe (EBA)	02.07.19 & 05.08.19	✓	✓	Supervisors discretion	+40% on average	Later than 2022*	Wide ranging recommendations, including qualitative guidance, and more consistency in Pillar 2
Canada (OSFI)	18.07.19	Unconfirmed	Unconfirmed	Unconfirmed	Unconfirmed	2021	Basel II standardized transition year in 2020
US	Not Live						
UK	Not Live						

Figure 2: ORX, 'SMA implementation tracker'

For financial institutions in Europe, a move to a standardized versus individual approach to risk modelling will materially increase capital requirements. The move is also likely to increase the need to set aside provisions to cover for increasingly frequent and severe NFR events for many financial institutions.

3. Embedment of NFR taxonomies

NFR as an area has only recently begun to be fully understood and measured. NFR taxonomies are still often incomplete in many financial institutions or in rarer cases non-existent. The difference is stark when compared to financial risk taxonomies which for many years have been well-defined, understood and owned throughout banks.

There has been increasing regulatory pressure for firms to complete their non-financial risk taxonomies. Regulators are determined to see the benefits of taxonomies realized throughout organizations. The main benefits of taxonomies are:

1. Creating a global golden source of risk titles and descriptions across all material NFRs that the firm has exposure to

2. Enabling consistent categorization of NFRs into a hierarchical list allowing for cross-functional comparisons

3. Driving consistency in the categorization of risk events, causes and impacts as well as verbiage used for NFR. An additional benefit of this is that NFR reporting and governance management information also improve.

Having said this, defining a taxonomy only really covers a small part of the end-to-end risk management process. Banks must be able to use the NFR taxonomy as a basis for identifying, assessing, managing and reporting their NFRs. Thus, the key to ensuring the successful embedment of the taxonomy is a strong wider organizational focus on the NFR framework. Solely defining a taxonomy and leaving it stale will not lead to the realization of any benefits.

4. Embracement of regtech

The pace of regulatory changes has increased by 500 percent since the financial crisis, which has resulted in the creation of multiple cottage industries as firms tried to meet multiple competing deadlines. As a result, between 10 to 15 percent of staff at banks are now estimated to work within their compliance functions[11]. From a cost perspective, it is estimated that $181 billion a year[12] is spent maintaining compliance, which translates to an average yearly cost of $10,000 per employee for large firms[13].

For banks to meet their regulatory requirements, and also to manage spiraling compliance costs, using regtech providers is becoming an ever more attractive option. Our view is that **regtech provides institutions with the ability to automate processes that have typically been highly manual, thereby cutting costs and freeing up time and resource**.

Listed below are functional overviews of regtech providers Capco have partnered with (contact us to find out more):

- Machine learning software to speed-up reconciliations and improve data integrity
- Automated mapping of regulations to internal policies and controls platform
- Artificial intelligence (AI) enabled transformation and formatting of unstructured data.

Firms embracing regtech can significantly reduce the cost of regulatory compliance. Moreover, they can also significantly reduce the cost of non-compliance.

DATA & ANALYTICS FOR NFR

1. Using data to untangle the complexity of risk

Before a bank can develop a sound, data driven risk management framework, they need to first understand the underlying relationship between different risk factors. The approach often taken by institutions is to develop key risk indicators based on certain events which have previously occurred rather than understanding the behavior which led to the event.

Whilst using previous events as the focal point for developing the risk framework may help to prevent similar events from occurring in the future, they will not be as helpful in predicting systemic risks. An important technique that financial institutions can use to better understand the underlying relationship is through utilizing knowledge graphs.

Knowledge graphs allow users to take data from various sources (often siloed) and map them based on commonalities. With the help of machine learning, knowledge graphs can help institutions to identify the relationship between indicators which may not even be considered when relying on human judgement. They can also have a significant impact on a risk manager's understanding of how different risk factors are related and offer a more complete view of all the different activities which

are contributing towards a given NFR category. Knowing this will help institutions to develop a more comprehensive risk framework with better equipped policies and mitigation controls.

2. Ensuring high quality of data inputs

Infrastructure and data maintenance

While implementing a data-driven approach offers multiple benefits to institutions, it does not come without challenges. A key challenge for banks is to evolve their data architecture to support the demands of employing such an approach. As institutions' demand for granular data increases, so will their need to develop a robust infrastructure that can support their need to store and maintain it.

Ensuring that the data available is accurate, and up to date, is fundamental for developing any meaningful insights (garbage in, garbage out principle) which may require investment in both systems and personnel. Data quality is an ongoing concern that most organizations have given the quality of data generated across departments is not up to the required standards[14].

Even if up-front investment is required in the short term, it is important to note the benefits that big data, artificial intelligence, and machine learning can have in driving down cost through automation in the long run which will help to offset the initial cost of investment and save money over the long term.

Data collection

Historically, the focus for NFR has been towards collecting data from self-assessments and incident reports, ignoring other valuable metrics which should be considered. To get a more inclusive view of their NFR, it is imperative for institutions to include metrics from other sources such as employee activity, incentives, and customer complaints in their risk models. Measuring such metrics can prove to be difficult which requires firms to combine data from a variety of sources into a cohesive model.

Data quality is a key consideration that will determine the value banks can gain from the final output. This is often a challenging factor for institutions who have amalgamated vast numbers of legacy systems as they have grown[15], resulting in multiple duplicative systems and making it difficult to identify the 'Golden Source' given the volume of data sets being generated. This runs the risk of providing incomplete or out of date views. This may require remediation activities such as data lineage mapping to identify the correct source of data and a clear governance structure to ensure that the target standards are being achieved.

3. Applying analytics to pinpoint pain areas

With the increase in data that is now available to financial institutions through more sophisticated technology, there is a great opportunity for them to take advantage of advanced analytics and build on their current NFR management practices. Improvements in both the quality and quantity of data should encourage institutions to move from a rear-view mirror approach defined by qualitative controls to a forward-looking predictive approach which can provide a real-time assessment of their risks.

As advanced analytics capabilities continue to develop, this – along with data collation – will have a significant impact on the risk management process. Listed below are three examples in which data analytics can be applied within organizations to derive efficiency and cost savings:

1. **Money laundering:** Using machine learning (ML) based models can help to identify emerging threats more quickly than the existing rules-based triggers and reduce false-positives

2. **Employee behavior:** Natural language processing, along with analytics, help to identify patterns of employee misconduct/ breach of best practice. Analyzing employee interactions and communications with clients along with sales patterns, incentives and customer complaints

can help to flag conduct concerns before it becomes a significant issue

3. **Fraud:** Combining ML techniques such as supervised and non-supervised learning will allow institutions to move away from principle-based techniques based on set patterns, as done historically.

A key benefit firms can realize from utilizing data is identifying potential threats which may not be recognized by the organization's traditional risk management practices. This is especially true for high severity tail-end events such as identifying misconduct by a small group of frontline employees (see Example 2 above).

These kinds of events are uncommon and often do not share the same characteristics, making them difficult to predict but can lead to considerable financial losses and reputational damage. Using analytics to identify and track wider patterns and correlations can help institutions to detect such upcoming risk events which may otherwise prove difficult to identify when relying solely on human judgement.

4. Other considerations: false positives

Historically, banks have relied upon conventional operational-risk detection tools centered on qualitative self-assessment and control reviews which have been shown to be ineffective in detecting critical operational risk categories. Not only can the conventional methodologies be ineffective in identifying certain risks, their reliance on manual work to complete and review self-assessments require enormous effort and time.

A key benefit that institutions can achieve from applying a data centric approach is to reduce the high volumes of false positive rates often found with non-financial risks. A false-positive is a test result which wrongly indicates that a particular condition or attribute is present. Rule-based detection techniques for conduct and other risk types often have a false positive rate of over 90 percent.

For example, a large financial institution based in the United Kingdom had a historically high false-positive rate of 99 percent. Through combining data from multiple sources and using data analytics the bank was able to reduce their false positive rates by 70 percent[16]. Having such a high rate highlights the inefficiencies inherent with existing techniques and stresses the need to move to a data-centric approach. Using data to drive the decision making will help banks to eliminate the constraints of manual dependency, saving time and improving their response rate.

OPERATIONAL RESILIENCE

1. Responding to change

Although the recent pandemic has had an incredible impact on our everyday lives, the resilience impact on financial institutions has been somewhat less[17].

COVID-19 was unusual as a disruptive event in that:

- **Banks were prepared:** Firms in most countries had a number of weeks' forewarning that trouble was on the horizon. Normally, the first time that a firm's leadership team will be aware of an event is after it has happened

- **Business operated (nearly) as usual:** While staff were impacted by the virus, infrastructure was less dramatically affected. Where remote working was possible for a critical mass of staff (noted this was hard for some), then firms were able to cope with the first order effects

- **There was no idiosyncratic impact:** Firms were all impacted more or less at the same time once COVID-19 arrived in a country, so the pressure to respond was shared across sectors rather than being concentrated on one firm.

However, the pandemic still provided useful operational resilience lessons and highlighted required changes to risk frameworks:

1. **The importance of NFR in identifying and highlighting emerging threats:** Some of the earliest conversations in firms around the pandemic started to happen in December 2019 and perhaps led to a lesser impact than might otherwise have been expected

2. **Adaptation to the new normal:** Current rating and scoring methods have not yet been adapted to the 'new normal', and so do not capture current risk levels correctly. Critics have raised doubts about risk management systems' ability to fully reflect the unprecedented new risks and banks must address these concerns now to manage this situation

3. **Revision of medium to long-term outlooks:** Banks will need to revise their inherent risk management approaches and procedures in response to COVID-19. They need to be able to understand the pandemic's impact on their risk profile from a medium and long-term perspective, for instance, the impact of staff working fully remotely. This is necessary for banks' own risk management and risk mitigation procedures, and for all key stakeholders – shareholders, investors, clients, rating agencies and regulators

4. **The continuing need to instill responsive and flexible frameworks**: Risk management will continue to need to be highly adaptable, as banks deal with uncertainty due to the recent pandemic and also contingency plan for subsequent events and respective countermeasures. The classical model-based approaches to risk management need to be supplemented by a more highly flexible ad hoc risk management. This will in turn require adaptations to business and IT architectures as well as to data management for risk.

2. Building operational resilience

In the past, NFR events were assumed to be 'one-offs' and so firms typically responded haphazardly to events on a best-efforts basis with no prior planning. For example, in 2014, hackers stole customer login details from a US investment bank and gained access to systems that went undetected for several months. This breach was only discovered once the hackers triggered a subsequent internal event and customers' data could theoretically have been left indefinitely exposed[18].

However, the underlying assumption behind operational resilience has changed over recent years such that now it is assumed events will occur and that the response needs to be built for when the inevitable happens.

Regulators are also reinforcing this need for firms to build operational resilience. In December 2019, the Bank of England and Financial Conduct Authority released an updated discussion paper[19] on building operational resilience within the financial services sector.

The approach proposed will rely on firms to quantify the maximum level of acceptable disruption for severe but plausible scenarios and firms will then base their risk tolerances on this modelling. Regulators will then measure and test firms' ability to remain within these tolerances and, in cases where limits are breached, ensure firms are identifying the root cause and remediating the identified issues.

The diagram below was initially produced in Capco's 'Managing the inevitable: a primer on operational resilience' paper[20]. It illustrates our methodology for banks to build and embed operational resilience:

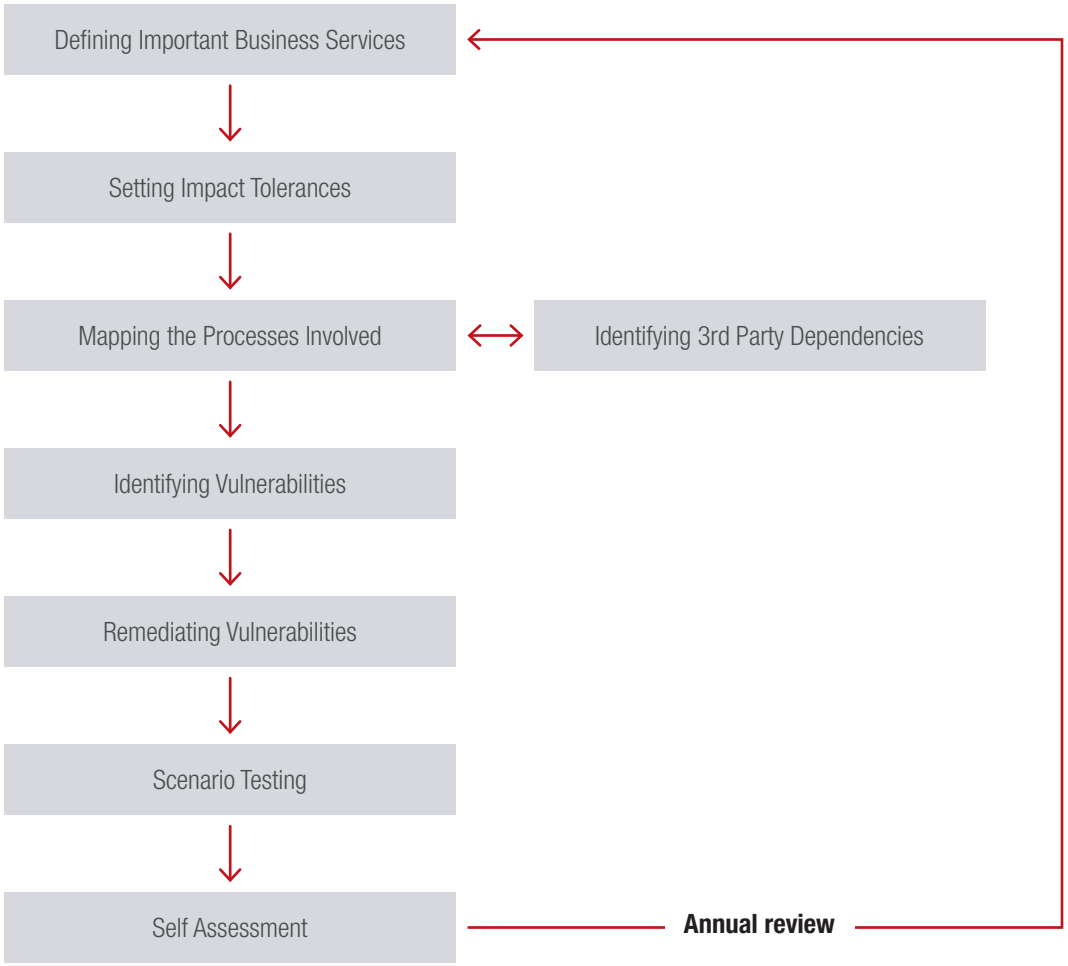


Figure 3: Capco, ' Managing the inevitable: a primer on operational resilience'

The key takeaway from the diagram is that building operational **resilience is a self-reinforcing process**. The better that firms adhere to the steps in the process, and most importantly honestly assess their current state annually, the better their preparation will be for future NFR events.

NFR OPERATING MODEL: UNDERPINNING SUCCESSFUL EXECUTION

While regulation, data and operational resilience are all important in and of themselves, what enables the factors to be brought together, leading to a combined effect greater than the sum of the parts, is a strong NFR operating model[21]. From Capco's perspective, this is built on three fundamental pillars: 1) organization 2) processes and, 3) architecture.

1. Organizational Design

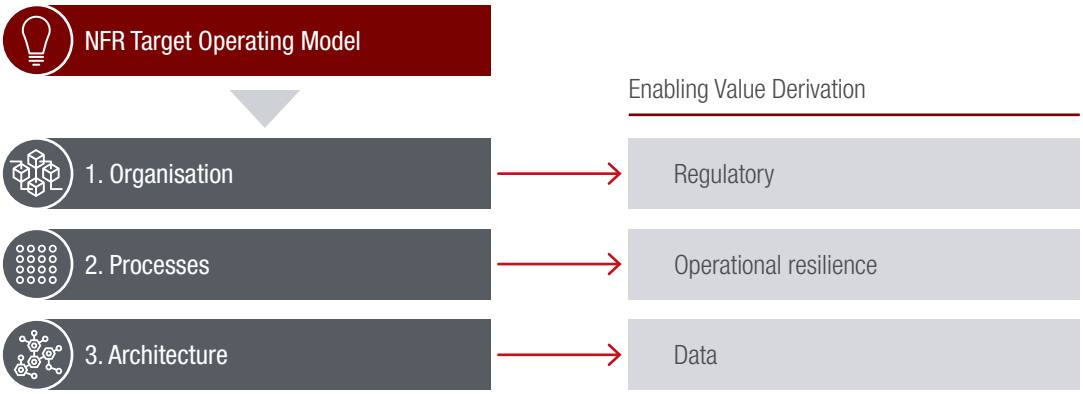
- With expected increases to regulatory capital requirements due to newly identified NFRs via the ICAAP & SREP, a well-run organization will be able to strategically forecast and plan for increasing requirements and therefore be able to optimize its capital position and minimize the knock-on effects on return on equity

2. Processes

- An increased focus on business resilience is only possible through clearly defined pure risk management processes and processes in which risk management is collaborative. Understanding and strengthening linkages between risk management and business units will help firms detect, remediate and close potential new threats and avoid costly regulatory fines

3. Architecture

- Implementing advanced data analytics capabilities is only possible when the underlying quality of the data is sufficiently high. For this, firms need a data management framework with a clear governance and a focus on identifying and remediating data quality issues. They also require a holistically assessed and integrated risk architecture with clearly defined golden sources of data.

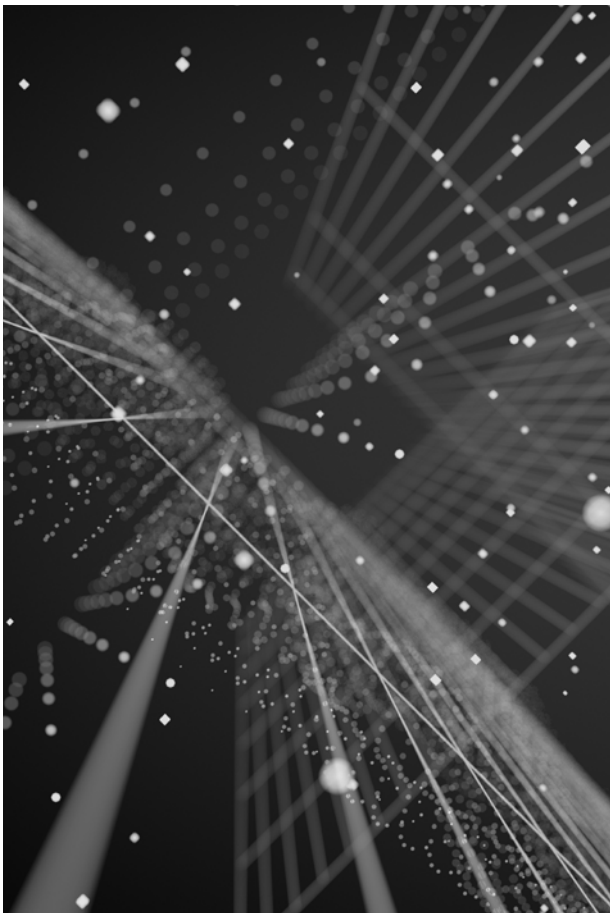


FINAL THOUGHTS

To understand the full scope of NFR, organizations will be required to have a comprehensive and adaptable view across their business. In recent months, many firms have been pushed into a heightened state of readiness and have taken proactive steps to manage their risk and ensure their people, processes and systems can evolve with the ever-changing markets.

Our goal is to support clients through the regulatory minefield which is becoming more complex as the regulators apply new directives to create market sustainability. This challenge coupled with other market factors brings data to the forefront, which raises questions surrounding the power which can be derived from analytics and regtech. Historical responses to change, leaves room for our clients to learn from past operational mistakes and we offer the necessary support to plan for resilience for the future.

There is still much to be done and 'a stitch in time saves nine' for firms who want to make their future now. Capco can help firms transform their vision for risk management into an executable blueprint that clearly articulates how their business will deliver its desired business model in relation to its value proposition.



REFERENCES

1. Gartner, 'Gartner Survey Reveals That CEO Priorities Are Slowly Shifting to Meet Rising Growth Challenges', May 2019, https://www.gartner.com/en/newsroom/press-releases/2019-05-08-gartner-survey-reveals-that-ceo-priorities-are-slowly
2. Committee of European Banking Supervisors, 'Guidelines on the Application of the Supervisory Review Process under Pillar 2', January 2006, pp. 8, https://eba.europa.eu/sites/default/documents/files/documents/10180/585173/9705f895-fbfa-4e39-bac9-3def3127f545/GL03.pdf
3. Reuters, 'BNP Paribas sentenced in $8.9 billion accord over sanctions violations', May 2015, https://www.reuters.com/article/us-bnp-paribas-settlement-sentencing-idUSKBN0NM41K20150501
4. Independent, 'TSB IT meltdown cost bank £330m and 80,000 customers', February 2019, https://www.independent.co.uk/news/business/news/tsb-it-failure-cost-compensation-customers-switch-current-account-a8757821.html
5. BBC, 'Goldman Sachs to pay $3bn over 1MDB corruption scandal', October 2020, https://www.bbc.co.uk/news/business-54597256
6. Financial News, 'BNP Paribas revamps compliance after record sanctions fine', November 2019, https://www.fnlondon.com/articles/bnp-paribas-revamps-compliance-after-record-sanctions-fine-20191120
7. TSB, 'TSB Board publishes independent review of 2018 IT Migration', November 2019, https://www.tsb.co.uk/news-releases/slaughter-and-may/
8. Federal Reserve, 'Order to Cease and Desist', October 2020, https://www.federalreserve.gov/newsevents/pressreleases/files/enf20201022a1.pdf
9. Basel Committee on Banking Supervision, 'Consultative Document on Standardised Measurement Approach for operational risk', June 2016, pp3-8, https://www.bis.org/bcbs/publ/d355.pdf
10. ORX, 'SMA implementation tracker', October 2019, https://managingrisktogether.orx.org/news-and-blogs/sma-implementation-tracker
11. Medici, 'How European Banks Are Using RegTech Solutions', June 2018, https://gomedici.com/how-european-banks-are-using-regtech-solutions/
12. LexisNexis, 'True Cost Of Financial Crime Compliance Study', March 2020, https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report
13. Ascent, 'The Not So Hidden Costs of Compliance', June 2020, https://www.ascentregtech.com/blog/the-not-so-hidden-costs-of-compliance/

REFERENCES CONTINUED

14. SAS, 'How to Succeed With Fraud Analytics: What you need to know about data management, discovery analytics and deployment', October 2018, pp5 https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/sas-whitepapers/en/succeed-with-fraud-analytics-110356.pdf

15. Capco, 'CFO of the Future, 2019, pp45, https://www.capco.com/Capco-Institute/Journal-50-Data-Analytics/The-CFO-Of-The-Future

16. IBM, 'Fighting financial crime with AI', December 2019, pp 5-7 https://www.ibm.com/downloads/cas/WKLQKD3W

17. Capco, 'Regulatory Horizon: Edition 2', 2020, pp9, https://www.capco.com/Intelligence/Regulatory-Horizon

18. SANS Institute, 'Minimizing Damage From J.P. Morgan's Data Breach', March 2015, pp3, https://www.sans.org/reading-room/whitepapers/casestudies/minimizing-damage-jp-morgan-039-s-data-breach-35822

19. Bank of England, 'Building operational resilience: Impact tolerances for important business services', December 2019, pp2-6, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/building-operational-resilience-impact-tolerances-for-important-business-services.pdf

20. Capco, 'Managing The Inevitable: A Primer On Operational Resilience', February 2020, pp3, https://www.capco.com/Intelligence/Capco-Intelligence/Managing-The-Inevitable-A-Primer-On-Operational-Resilience

21. Capco, 'Non-Financial Risk: Agility In Times Of Uncertainty', July 2020, pp4, https://www.capco.com/Intelligence/Capco-Intelligence/Non-Financial-Risk-Agility-In-Times-Of-Uncertainty

AUTHORS

Dr Alfie Lindsey, Principal Consultant
Russel Miah, Senior Consultant
Thomas Parkinson, Senior Consultant
Aized Chaudhry, Consultant

CONTACTS

Dr Alfie Lindsey
Principal Consultant
Risk, Capco UK
alfie.lindsey@capco.com

Tom Leach
Executive Director
Finance & Risk, Capco UK
tom.leach@capco.com

Steve Watts
Partner
Capco UK
stephen.watts@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO