N. Gittfried G. Lienke F. Seiferlein
J. Leiendecker B. Gehra (eds.)

Non-financial Risk Management in the Financial Industry

A Target Operating Model for Compliance and ESG Risks

Frankfurt School Verlag

N. Gittfried G. Lienke F. Seiferlein
J. Leiendecker B. Gehra (eds.)

Non-financial Risk Management in the Financial Industry

A Target Operating Model for Compliance and ESG Risks

Frankfurt School Verlag

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Besuchen Sie uns im Internet: http://www.frankfurt-school-verlag.de.

ISBN (print): 978-3-95647-188-9
ISBN (epub): 978-3-95647-189-6
ISBN (pdf): 978-3-95647-190-2
ISBN (mobi): 978-3-95647-191-9

Table of contents

Editors

Norbert Gittfried is a Partner and Director at Boston Consulting Group. As topic coordinator for Compliance & Regulation, he advises large financial institutions worldwide on complex compliance transformations and the development of overarching non-financial risk steering approaches. His focus lies both in establishing effective Compliance and NFR Management systems, in digitising those functions and making them more efficient. Prior to joining BCG 11 years ago, he was Senior Manager at a Big 4 Company. He is a lecturer at Goethe Business School and a permanent representative in various industry bodies for FI.

Georg Lienke is a lawyer and Associate Director at Boston Consulting Group focusing on non-financial risk management and Compliance. In his work for financial institutions and corporate clients over the last 15 years, his focus was on the design and implementation of target operating models for non-financial risk management. Georg regularly publishes on non-financial risk topic. He holds a Ph.D. in law from the Technical University Dresden and a Master of Laws in Corporate and Financial Law from the University of Hong Kong. Prior to joining BCG, Georg worked at a Big 4 Company and a global bank.

Florian Seiferlein is an Associate Director at Boston Consulting Group. For over a decade, he advised leading companies on Compliance & Non-Financial Risks (NFR). He managed large-scale Compliance & NFR transformations, investigations and regulatory assessments in Europe, North America and Africa, and he was also a part of US Monitor teams. Prior to joining BCG, he worked for Big 4 and management consulting firms. Florian holds a Master of Science in business engineering (Karlsruhe Institute of Technology).

Jannik Leiendecker is a Partner and an Associate Director at Boston Consulting Group. Over the last 11 years, his focus has been on Non-Financial Risk (incl. Compliance) and ESG. He has advised numerous clients especially within the Financial Services industry on the set-up and optimisation of their respective operating model. He has also co-authored various corresponding publications. Jannik holds a Master of Science in Economic History from the London School of Economics and a Bachelor of Science in Business from the Ludwig-Maximilians-University in Munich.

Bernhard Gehra is a Senior Partner and Managing Director at Boston Consulting Group. His focus has been on Risk, Compliance and Technology for more than 20 years. During the last of those, he has led large worldwide projects focused on Risk and Non-Financial Risk. Furthermore, Bernhard recently managed ESG Compliance issues for large companies. Prior to joining BCG, he worked for a global securities service provider. Bernhard holds a Ph.D. in information science.

Contributors

Prof. Dr. Douglas Arner, Kerry Holdings Professor in Law, RGC Senior Fellow in Digital Finance and Sustainable Development, Faculty of Law, University of Hong Kong, Hong Kong

Dr. John Ashley, General Manager, Financial Services and Technology, NVIDIA Inc., San Francisco Bay Area

Ulrike Brouzi, Member of the Board of Managing Directors, DZ BANK AG, Frankfurt

Rene Bystron, Project Leader, Boston Consulting Group, Seattle

Dr. Oliver Engels, Chief Risk Officer, Deutsche Börse AG, Frankfurt

Dr. Erasmus Faber, Managing Director, Head of Compliance & Risk Management Germany, Twelve Capital (DE) GmbH, Munich

Lorenzo Fantini, Managing Director & Partner, Boston Consulting Group, Milan

Barbara Fojcik, Project Leader, Boston Consulting Group, Munich

Dr. Jan-Oliver Fröhlich, Project Leader, Boston Consulting Group, Hamburg

Kai Gammelin, Risk prevention and compliance expert in a leading position in the financial industry, Bludenz

Dr. Julia Gebhardt, Partner, Boston Consulting Group, Munich

Dr. Ulrich Göres, Frankfurt

Peter Gürtlschmidt, Mag. MA, Vice President, Head AFC GMIC Corporate & Investment Bank Germany / EMEA, Deutsche Bank AG, Frankfurt

Dr. Katharina Hefter, Managing Director & Partner, Boston Consulting Group, Berlin

Hurdogan Irmak, Head of Risk Management, Isbank, Istanbul

Marc Peter Klein, Ass. jur., Managing Director, Head AFC Corporate & Investment Bank Germany / EMEA, Deutsche Bank AG, Frankfurt

Dr. Michael Lange, Managing Director, Divisional Head Compliance, DZ BANK AG, Frankfurt

Annika Melchert, Manager, BCG Platinion, Dubai

P. Robert Mieszkowski, DZ BANK AG, Frankfurt

Martina Mietzner, Managing Director, Chief Compliance Officer, Bayerische Landesbank, Munich

Burcu Nasuhoglu, Head of Operational Risk Management, Isbank, Istanbul

Dr. Jochen Papenbrock, Financial Services and Technology Developer Relationship Lead EMEA, Gaia-x FAIC Lead, NVIDIA GmbH, Frankfurt

Aytech Pseunokov, Project Leader, Boston Consulting Group, Dubai

Jennifer Rabener, Project Leader, Boston Consulting Group, Munich

Luca Rancan, Project Leader, Boston Consulting Group, Milan

Michele Rigoni, Principal, Boston Consulting Group, Milan

Dr. Barbara Roth, Managing Director, Head Group Internal Audit, Deutsche Börse AG, Frankfurt

Dr. Christian N. Schmid., Managing Director & Partner, Boston Consulting Group, Munich

Prof. Dr. Martin Schulz, Attorney at law, Counsel, CMS Hasche Sigle, Frankfurt

Björn Stauber, M.Sc., First Vice President Compliance, KfW Bankengruppe, Frankfurt

Rei Tanaka, Managing Director & Partner, Boston Consulting Group, Tokyo

Benedetta Testino, Project Leader, Boston Consulting Group, Milan

Federico Truffelli, Deputy Head of Group Anti-Financial Crime, Group Head of AML/FS Risk Assessment, Controls and Liaison Office Support, UniCredit Group, Milan

Anita Varshney, Global Vice President, Strategy SAP S/4HANA Sustainability, SAP, Hong Kong

Valérie Villafranca, Managing Director, Group Head of ESG Transformation, Société Générale, Paris

Lora von Ploetz, LL.M. Law, LL.M. Finance, Director, Head of Global Financial Crime Unit, Commerzbank AG, Frankfurt

Daniel Wagner, Manager, BCG Platinion, Frankfurt

Dr. Carsten Wiegand, Knowledge Expert, Team Manager, Boston Consulting Group, Frankfurt

Foreword

These are turbulent times for the financial industry and for society at large. Banks, insurers, asset managers and other financial services providers are subject to a profound, lasting disruption, shaping the way value is created and how people will work in the decades to come.

Climate change and the role of the financial industry in the historical transformation toward greenhouse-gas neutrality is at the top of almost every CEO's agenda. The industry is subject to game-changing environment, social and governance regulation (ESG) and disclosure requirements and is adopting a role as a change agent to finance the climate transition. The climate agenda deeply impacts the industry's business and risk strategies, triggering fundamental changes to the way financial and non-financial risks are managed.

Since the COVID-19 outbreak in late 2019, society has seen a whirl of lockdowns and contact restrictions. The pandemic has also impacted businesses of all shapes and sizes across a range of industries, with the 2020 global gross domestic product down almost by 3.5%.[1] The financial industry has continued to prove its social and economic relevance during the pandemic, delivering vital aid to businesses and individuals at record speed, creating new processes and systems on the fly and shifting workforces and operations to remote conditions. COVID-19 accelerated digitisation to new heights, with some senior executives painfully realising that digital is not optional but a question of making the cut.

On top, regulatory agencies are ramping up their efforts to ensure corporations obey the rules – and imposing heavy penalties on those that fail to deliver. From 2009 to 2020, global regulators handed out almost $400 billion in fines for non-compliance.[2]

To emerge stronger from these challenging times, financial institutions must succeed on many fronts, with non-financial risk management being a critical component. This holds particularly true in times of geopolitical unrest such as the conflict between Russia and the Ukraine right now. For global financial organisations with a broad product portfolio across multiple geographical regions, the management of non-financial risks is complex, and pitfalls are looming: insufficient consistency in policy standards, a divergence in the regional execution, opaque risk exposure and a fragmented IT landscape, to name just a few. The need for a bank-wide, global non-financial risk management framework has become abundantly clear.

---

1 IMF 2021.

2 BCG 2021a.

This handbook is intended as a guide to establish a target operating model for non-financial risk management, primarily for the financial industry, and covers the entire risk management lifecycle. This includes a definition of non-financial risk, risk appetite frameworks, risk governance, top-down non-financial risk assessments, internal control frameworks, data and IT governance as well as conduct and ethics.

The editors are grateful to the contributors, who are all leading experts in non-financial risk management, compliance and ESG.

Frankfurt and Munich, February 2022

The editors Norbert Gittfried, Dr. Georg Lienke, Florian Seiferlein, Jannik Leiendecker and Dr. Bernhard Gehra

1 Introduction: Rising to the Challenges of Non-Financial Risk Management, Compliance and ESG

Prof. Dr. Douglas Arner, Dr. Bernhard Gehra, Jannik Leiendecker, Dr. Georg Lienke

Historically, financial institutions have focused many of their risk management efforts on financial exposures directly attributed to core business activities. However, in recent times, non-financial risk (NFR) management with an emphasis on compliance and environment, social and governance (ESG) risks has moved up the policy and executive agendas, amid new regulations, a range of compliance issues (some leading to significant fines) and an increasing pressure to act as change agents in the transition towards a decarbonised economy. A robust NFR framework is indispensable in case of crises, so that necessary quick and effective reaction measures can be taken. This became unmistakably clear in the conflict between Russia and the Ukraine, with unprecedented sanctions being imposed on Russia that heavily affect the global financial industry and non-financial sectors.

This handbook analyses the major success factors for meeting the requirements of modern non-financial risk management: an institution-specific target operating model (TOM) integrating all critical components – strategy, governance, risk management, information technology and data architecture including digitisation and artificial intelligence as well as ethics. The handbook has been written by senior NFR, compliance and ESG experts from key markets in Europe, the US and Asia, and it gives practitioners the necessary guidance to master the key challenges in today's global risk environment. Each chapter includes key regulatory requirements, major implementation challenges, practical solutions and industry examples.

1.1 New risks and challenges

Institutions face non-financial risks across a range of activities: from onboarding clients to running IT systems and carrying out daily operations. Amid a continuous flow of new risks, failures in these areas can have significant economic and reputational consequences, both for the institutions as well as their executives. Globally, compliance issues led to $394 billion in fines during the years 2011 to 2020, including $50 billion in 2018, 2019 and 2020 alone.[1] In response, financial institutions have dramatically enhanced their oversight capabilities, leading to a proliferation of risk managers, internal auditors, control special-

[1] BCG 2021a.

ists and compliance officers, each with their own unique backgrounds, perspectives and skill sets.

These teams of experts have tended to focus on specific areas, leading to the evolution of siloed and fragmented processes, the disjointed nature of which has itself become an operational risk. A lack of coordination has created gaps, overlaps and mismatches in the three lines of defence (3LoD) framework at most institutions. Risk functions today often produce different risk reports that apply different methodologies to analyse and quantify risk, making it difficult for executives to put risk categories into proportion and arrive at accurate implications for overall risk management. This comes on top of existing complexity: global financial organisations need to orchestrate separate product divisions, infrastructure functions (including risk management) and geographical regions, representing a range of legal entities in local jurisdictions as well as regulators and regulatory systems and requirements in multiple jurisdictions. At the same time, they need to weave in effective and efficient measures to manage non-financial risks. The challenges are significant, suggesting that a holistic, structured approach is critical.

1.2 A forward-looking solution for non-financial risk management in the financial industry

To continue to thrive in an increasingly challenging risk environment, financial institutions need to develop a sophisticated approach to non-financial risk management. This can be done by establishing an institution-specific non-financial risk TOM, which will subsequently allow for a proper definition of risks, creating an integrated view of the 3LoD and building an effective internal control system – informing a sensible executive decision-making that can prevent inevitable risks getting out of control.

This handbook outlines the key ingredients of a non-financial risk TOM for financial institutions. The book sections follow a consistent structure: chapters start with an individual introduction to the topic at hand, followed by a summary of key regulatory expectations across the EU, the US and Asia. Each chapter assesses operational challenges and complexities, and it delivers approaches to define solutions based on industry success factors. Chapters are augmented by practical, hands-on examples from seasoned practitioners. They conclude with the summaries of key takeaways.

1.3 Defining and aligning non-financial risk categories

Risks are inherent to every business model, so that a zero-risk tolerance approach is in fact counter-intuitive. Historically, financial institutions have focused their attention on financial risks, including credit risk, market risk, liquidity risk and funding risks, aggregating the remainder under a category most often labelled as operational risk. Recently, non-financial risks have evolved as an independent category for risk management, allowing for a more tailored approach to management of individual non-financial risks. *Chapter 2* provides a general definition of non-financial risk, delineates non-financial risk from financial risk, and provides definitions for categories and types of non-financial risk for financial institutions.

1.4 Establishing a non-financial risk appetite framework to prevent an undesirable risk-taking

Following the definition of non-financial risk, *chapter 3* provides a holistic approach to defining a non-financial risk appetite framework for financial institutions across three levels. This includes qualitative risk appetite statements for individual non-financial risk categories, outlining the level and types of risk that the financial institution is willing to take on in order to achieve its strategic objectives and business plan (level 1). Qualitative risk appetite statements are broken down into risk appetite metrics and corresponding thresholds, enabling institutions to set quantifiable tolerance levels for non-financial risk and underlying operational activities (level 2). Level 3 cascades the risk appetite framework to business lines and entity levels via pre-defined key risk indicators, facilitating the early detection of potential deviations from risk appetite objectives and potentially triggering timely interventions. The chapter also draws an outline of the corresponding governance that is required to operate a risk appetite framework.

1.5 Building key governance and organisational pillars for non-financial risk management

Three chapters outline the governance and organisational structures required for sustainable non-financial risk management, standing on three major pillars. The three lines of defence (LoD) model (*chapter 4*) defines the roles and responsibilities of the first LoD (front, middle and back office), the second LoD (risk control functions) and the third LoD (internal audit). The chapter focuses on the independence of second-LoD control functions and describes the concept of risk coordinating functions in the first LoD as a regulatory competence centre, coordination unit and interface to the second LoD.

'Global functional lead' (*chapter 5*) stands for a combination of strategic, governance and risk management elements defined by an institution that aim to enable a consistent execution of risk management activities across complex organisations. It comprises the central setting of global risk management standards by horizontal risk management functions and their execution by vertical product- or region-focused functions, with direct or indirect reporting lines into horizontal functions. A policy and procedure framework (*chapter 6*) intends to ensure that standards are met in the execution of an institution's business and operational activities. It builds a structural policy hierarchy, allocating the financial institution's documents including board directives, policies and procedures to different hierarchical levels. It structures them by risk types, business segments and relevant geographies.

1.6 Generating excellence in the non-financial risk management lifecycle

Three chapters describe the most essential components of a financial institution's non-financial risk management lifecycle.

Sophisticated institutions apply a top-down approach to non-financial risk assessment, using risk-type agnostic criteria to evaluate their exposure to non-financial risks and derive the proper implications for bank-wide risk management. Chapter 7 elaborates on the methodology for a top-down non-financial risk assessment.

A key element of effective risk mitigation is the underlying internal control framework. Controls can take a variety of forms, ranging from automated/manual process controls to the conduct of training sessions and the definition of internal policies and requirements. A comprehensive internal control framework needs to combine a top-down approach (focusing on controls addressing the most relevant risk types) with a bottom-up approach (whereby individual risks and controls are identified based on a detailed review of the underlying processes). *Chapter 7* comprises a deep dive on the top-down approach for the creation of an internal control framework.

Financial institutions are confronted with non-financial risks that are increasing both in number and severity, and they face non-financial risk exposure in almost every area of activity. In many institutions, this has resulted in a heterogenous reporting landscape for non-financial risks, with a variety of bottom-up, risk-specific reports from different functions and often diverging criteria for the measurement of risk. Hence, financial institutions are in an ever-stronger need of an overall non-financial risk reporting approach, spanning across risk types and consolidating the measurement of risk and the adequacy assessment of risk-mitigating controls. Only such a top-down report can give executive management the fact base and insights necessary to steer an institution effectively. *Chapter 8* describes an approach to risk-agnostic non-financial risk reporting.

Chapter 9 is a deep dive into investigation capabilities, combined with root cause analysis. Alongside the on-going harmonisation of European corporate law, individual jurisdic-