

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>.

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

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

1. Auflage 2022 © Frankfurt School Verlag / efiport GmbH, Adickesallee 32–34, 60322 Frankfurt a. M.

# Table of contents

Table of contents.....	V
Editors.....	XXI
Contributors.....	XXII
Foreword.....	XXVI
<b>1 Introduction: Rising to the Challenges of Non-Financial Risk Management, Compliance and ESG .....</b>	<b>1</b>
<i>Prof. Dr. Douglas Arner, Dr. Bernhard Gebra, Jannik Leiendecker, Dr. Georg Lienke</i>	
1.1 New risks and challenges.....	1
1.2 A forward-looking solution for non-financial risk management in the financial industry .....	2
1.3 Defining and aligning non-financial risk categories .....	2
1.4 Establishing a non-financial risk appetite framework to prevent an undesirable risk-taking .....	3
1.5 Building key governance and organisational pillars for non-financial risk management .....	3
1.6 Generating excellence in the non-financial risk management lifecycle	4
1.7 Using data, IT and artificial intelligence.....	5
1.8 Putting conduct and ethics at the centre of sustainable non-financial risk management .....	6
1.9 Environment, social and governance: Implications for effective risk management .....	7
<b>2 Definition of Non-Financial Risk in Financial Institutions .....</b>	<b>9</b>
<i>Martina Mietzner, Dr. Julia Gebhardt, Dr. Katharina Hefter, Jennifer Rabener, Dr. Carsten Wiegand</i>	
2.1 Introduction .....	9
2.2 History of non-financial risk and specifications by key regulators ...	11
2.2.1 A short history of non-financial risk .....	12
2.2.2 Existing non-financial risk specifications by key global and regional regulators and associations .....	15
2.3 Differentiation of financial and non-financial risk .....	16
2.3.1 Financial risk definition .....	17
2.3.2 Non-financial risk definition .....	18

2.4	Specific clusters of non-financial risk	18
2.4.1	Operational risk	21
2.4.1.1	Financial crime risk	21
2.4.1.1.1	Money-laundering/terrorist financing risk	22
2.4.1.1.2	Sanctions and embargoes risk	22
2.4.1.1.3	Bribery and corruption risk	23
2.4.1.1.4	Facilitation of tax evasion	23
2.4.1.2	Conduct risk	24
2.4.1.2.1	Market conduct risk	24
2.4.1.2.2	Client conduct risk	25
2.4.1.2.3	Employee conduct risk	25
2.4.1.3	Regulatory compliance risk	25
2.4.1.4	Fraud risk	26
2.4.1.4.1	Account-opening fraud risk	27
2.4.1.4.2	Debt/credit card fraud risk	27
2.4.1.4.3	Fraudulent paper-based payment transactions risk	28
2.4.1.4.4	Online banking fraud risk	28
2.4.1.4.5	Credit fraud risk	28
2.4.1.4.6	Theft risk	28
2.4.1.4.7	Embezzlement/breach of trust risk	28
2.4.1.4.8	Antitrust violation risk	29
2.4.1.4.9	Balance sheet manipulation	29
2.4.1.5	Information, Communication & Technology (ICT) and Cyber risk	29
2.4.1.5.1	Data confidentiality risk	31
2.4.1.5.2	Data availability risk	32
2.4.1.5.3	Data integrity risk	32
2.4.1.5.4	Information security risk	32
2.4.1.6	Data privacy and bank secrecy risk	33
2.4.1.6.1	Data privacy risk	33
2.4.1.6.2	Bank secrecy risk	34
2.4.1.7	Resilience risk	34
2.4.1.8	Outsourcing and vendor risk	35
2.4.1.8.1	Intragroup outsourcing risk	36
2.4.1.8.2	External outsourcing risk	36
2.4.1.8.3	Vendor risk	37
2.4.1.9	Tax reporting risk	37
2.4.1.10	Other operational risk	37
2.4.1.10.1	Human resources risk	37
2.4.1.10.2	Legal risk	37
2.4.1.10.3	Physical damage risk	38
2.4.1.10.4	Execution, delivery and process risk	38
2.4.1.10.5	Reporting risk	38
2.4.1.10.6	Accounting risk	39

	2.4.1.10.7 Project risk .....	39
	2.4.1.10.8 Competition law risk .....	39
	2.4.1.10.9 Model risk .....	39
2.4.2	Strategic risk .....	40
	2.4.2.1 Reputational risk .....	40
	2.4.2.2 Sustainability risk .....	41
	2.4.2.2.1 Climate change risk .....	41
	2.4.2.2.2 Human rights risk .....	42
	2.4.2.3 Business risk .....	42
	2.4.2.3.1 Forecasting risk .....	42
	2.4.2.3.2 Inorganic growth risk .....	43
	2.4.2.3.3 New business risk .....	43
	2.4.2.3.4 Investor relations risk .....	43
2.5	Conclusion and outlook .....	43
<b>3</b>	<b>Risk Boundaries – Setting an Analytical Risk Appetite Framework for Non-Financial Risks</b> .....	<b>45</b>
	<i>Federico Truffelli, Dr. Ulrich Göres, Lorenzo Fantini, Michele Rigoni, Luca Rancan</i>	
3.1	Introduction .....	45
	3.1.1 Regulatory requirements .....	45
	3.1.2 RAF in practice .....	47
3.2	RAF Level 1: Overall Risk Appetite Statement .....	49
	3.2.1 Overall statement .....	49
	3.2.2 Prohibited activities .....	51
3.3	RAF Level 2: Risk Appetite metrics .....	51
	3.3.1 Defining appropriate metrics .....	51
	3.3.2 Metrics: setting the thresholds .....	52
	3.3.2.1 Thresholds based on benchmark and historical internal loss data for a metric based on operational losses .....	53
	3.3.2.2 Thresholds based on residual risk levels for a metric based on risk assessment .....	54
3.4	RAF Level 3: Key Risk Indicators .....	55
	3.4.1 Selecting key risk indicators .....	55
	3.4.1.1 Candidate indicators identification .....	56
	3.4.1.2 Appetite tracking suitability .....	56
	3.4.1.3 Expert judgement .....	56
	3.4.2 KRIs: setting and calibrating the thresholds .....	60
	3.4.2.1 Threshold calibration based on historical data analysis and percentiles .....	60
	3.4.2.2 Threshold fine-tuning based on benchmarking and backtesting .....	62

3.5	RAF Governance .....	63
3.5.1	RAF design and update .....	64
3.5.2	RAF monitoring and reporting .....	65
3.5.3	RAF threshold breaches and escalation .....	66
3.5.4	Action plan definition .....	68
<b>4</b>	<b>The Three Lines of Defence Model: Key Success Factors for Effective Risk Management</b> .....	<b>71</b>
	<i>Dr. Oliver Engels, Marc Peter Klein, Peter Gürtlschmidt, Dr. Georg Lienke, Rei Tanaka</i>	
4.1	Introduction .....	71
4.2	Regulatory framework in selected key jurisdictions .....	72
4.2.1	European Union .....	72
4.2.2	United States of America .....	73
4.2.3	Hong Kong .....	73
4.2.4	Singapore .....	73
4.2.5	Risk-type-specific qualifications of the 3LoD model: financial crime prevention .....	74
4.2.5.1	EU: remaining country-specific variation in 1 <sup>st</sup> and 2 <sup>nd</sup> LoD mandate .....	74
4.2.5.2	United States of America: BSA Compliance officer ..	74
4.2.5.3	Hong Kong: Money Laundering Reporting Officer and Compliance Officer .....	75
4.3	Key roles and responsibilities of 1 <sup>st</sup> , 2 <sup>nd</sup> and 3 <sup>rd</sup> LoD .....	75
4.3.1	The first line of defence: risk owner .....	76
4.3.1.1	Scope of 1 <sup>st</sup> LoD mandate .....	76
4.3.1.1.1	Risk ownership .....	76
4.3.1.1.2	Implementation and execution of 1 <sup>st</sup> LoD controls .....	76
4.3.1.2	Allocation of 1 <sup>st</sup> LoD responsibility .....	76
4.3.1.3	1 <sup>st</sup> LoD risk-coordinating function (1.5 <sup>th</sup> LoD) .....	77
4.3.1.3.1	Coordination of risk management activities .....	77
4.3.1.3.2	Interface to 2 <sup>nd</sup> LoD .....	77
4.3.1.3.3	Regulatory advisor .....	77
4.3.2	The second line of defence: internal control functions .....	78
4.3.2.1	Scope of 2 <sup>nd</sup> LoD mandate .....	78
4.3.2.1.1	Standard setting .....	78
4.3.2.1.2	Testing of 1 <sup>st</sup> LoD controls .....	79
4.3.2.1.3	Risk assessment .....	79
4.3.2.1.4	Training and advisory .....	79
4.3.2.2	Risk materiality and corresponding intensity of 2 <sup>nd</sup> LoD risk oversight .....	79



4.3.2.3	Independence of 2 <sup>nd</sup> LoD risk oversight . . . . .	80
4.3.2.3.1	Organisational independence . . . . .	80
4.3.2.3.2	Functional independence . . . . .	80
4.3.2.3.3	Internal control functions performing 1 <sup>st</sup> LoD activities . . . . .	81
4.3.2.4	Key success factors for effective 2 <sup>nd</sup> LoD risk oversight . . . . .	82
4.3.2.4.1	Methodology consistency across 2 <sup>nd</sup> LoD functions . . . . .	82
4.3.2.4.2	Bodies and committees: adequate 2 <sup>nd</sup> LoD participation and information sharing . . . . .	83
4.3.2.4.3	Appointment of primus inter pares non- financial risk governance function . . . . .	84
4.3.3	The third line of defence: internal audit as provider of independent assurance . . . . .	85
4.3.3.1	Independent assurance . . . . .	85
4.3.3.1.1	Adequacy of risk management framework . . . . .	85
4.3.3.1.2	Design and operating effectiveness . . . . .	85
4.3.3.1.3	Compliance with regulatory requirements and internal standards . . . . .	86
4.3.3.2	Advising the board of directors . . . . .	86
4.4	Common pitfalls of the 3LoD model and precautionary measures . .	86
4.4.1	Insufficient risk ownership by 1 <sup>st</sup> LoD . . . . .	86
4.4.2	Lack of 2 <sup>nd</sup> LoD expertise . . . . .	87
4.4.3	Inadequate assurance by 3 <sup>rd</sup> LoD . . . . .	87
4.5	Conclusion . . . . .	88
<b>5</b>	<b>Global Functional Lead in Non-Financial Risk Management: Ensuring Consistency and Integration in Complex Organisations . . .</b>	<b>89</b>
	<i>Ulrike Brouzi, Dr. Michael Lange, P. Robert Mieszkowski, Jannik Leiendecker, Dr. Georg Lienke, Florian Seiferlein, Norbert Gittfried, Rei Tanaka</i>	
5.1	Introduction . . . . .	89
5.2	Regulatory framework in select key markets . . . . .	91
5.2.1	European Union . . . . .	91
5.2.2	United States of America . . . . .	91
5.2.3	Hong Kong . . . . .	92
5.2.4	Singapore . . . . .	92
5.3	Global functional lead: individual corporate parameters to consider .	92
5.3.1	Corporate culture . . . . .	92
5.3.2	Organisation's complexity . . . . .	93
5.3.3	IT landscape . . . . .	93
5.3.4	Geographical footprint . . . . .	93

5.4	Major components of global functional lead in non-financial risk management .....	93
5.4.1	Operating model: striking a balance between global standards and regional execution .....	94
5.4.1.1	Regulatory horizon screening .....	95
5.4.1.2	Setting of risk-specific standards .....	96
5.4.1.3	Training and advisory .....	97
5.4.1.4	Controls by the 1 <sup>st</sup> and 2 <sup>nd</sup> line of defence .....	97
5.4.1.5	Non-financial risk assessment .....	98
5.4.1.6	Non-financial risk reporting .....	99
5.4.1.7	Group risk oversight .....	99
5.4.2	Reporting lines: establishing implementation accountability in vertical functions .....	100
5.4.2.1	Solid reporting lines into local legal entity and branch .....	100
5.4.2.2	Dotted reporting lines into global risk management organisation .....	101
5.4.3	Meeting governance: supporting effective management of a global risk function .....	101
5.5	Conclusion .....	102
<b>6</b>	<b>Policies and Procedures: Framework and Governance Requirements in the Financial Sector .....</b>	<b>105</b>
	<i>Dr. Erasmus Faber, Björn Stauber, Dr. Georg Lienke</i>	
6.1	Introduction .....	105
6.2	Regulatory framework in selected key jurisdictions .....	105
6.2.1	European Banking Authority (EBA) .....	106
6.2.2	US regulators .....	106
6.2.2.1	The Federal Reserve .....	106
6.2.2.2	Office of the Comptroller of the Currency .....	107
6.2.3	Hong Kong Monetary Authority .....	107
6.2.4	Monetary Authority of Singapore .....	108
6.3	Policy framework: key implications for a target concept .....	109
6.3.1	Status quo: need for structured approach .....	109
6.3.1.1	Lack of a harmonised approach .....	109
6.3.1.2	Policy gaps and redundancies .....	109
6.3.2	Policy framework: design concept and hierarchies .....	110
6.3.2.1	Design concept: key hypotheses for an effective policy framework .....	110
6.3.2.1.1	Harmonised design approach .....	110
6.3.2.1.2	Completeness .....	110
6.3.2.1.3	Uniform naming convention .....	110
6.3.2.1.4	Precise wording .....	111
6.3.2.1.5	Assignment of responsibilities .....	111
6.3.2.1.6	Governance rules .....	111
6.3.2.1.7	Linkage to internal processes and controls .....	111

6.2.2.2	Suggested hierarchy levels: key criteria and examples	111
6.3.2.3	Level one: overarching risk strategies, policies and documents – risk and business segment agnostic . . . .	112
6.2.2.3.1	Key criteria . . . . .	112
6.3.2.3.2	Key risk type and business segment agnostic topics . . . . .	112
6.3.2.4	Level two: risk-type-specific policies and procedures	113
6.3.2.4.1	Key criteria . . . . .	113
6.3.2.4.2	Risk-type-specific documents . . . . .	113
6.3.2.5	Level three: customer-related and business-specific policies and procedures . . . . .	114
6.3.2.5.1	Key criteria . . . . .	114
6.3.2.5.2	Customer-related and business-specific topics . . . . .	115
6.3.2.6	Level four: policies and procedures in international locations . . . . .	115
6.3.2.6.1	Scope of applicability: subsidiary companies and branch offices . . . . .	115
6.3.2.6.2	Key criteria . . . . .	115
6.4	Policy governance, repository and workflow tool . . . . .	116
6.4.1	Approval of policies and procedures . . . . .	117
6.4.1.1	Level one: board of directors . . . . .	117
6.4.1.2	Level two: responsible board member . . . . .	117
6.4.1.3	Level three: senior management on N-1 level . . . . .	117
6.4.1.4	Level four: general manager or 2 <sup>nd</sup> LoD N-1 . . . . .	117
6.4.2	Authorship, ownership, creation as well as update of policies and procedures . . . . .	118
6.4.2.1	Document authorship . . . . .	118
6.4.2.2	Document ownership . . . . .	118
6.4.2.3	Document creation process . . . . .	118
6.4.2.4	Stringent management of update process . . . . .	118
6.4.2.4.1	Regular validation based on time intervals	119
6.4.2.4.2	Ad hoc updates . . . . .	119
6.4.3	Policy repository, including workflow tool: centralised management of policies and procedures . . . . .	119
6.4.3.1	Facilitation of access . . . . .	120
6.4.3.2	Document lifecycle management . . . . .	120
6.4.3.2.1	Regular validation of documents . . . . .	120
6.4.3.2.2	Ad hoc updates . . . . .	120
6.4.3.2.2.1	Changes in business and operating model . . . . .	120
6.4.3.2.2.2	Changes in regulatory framework . . . . .	121
6.4.3.3	Audit-proof change log . . . . .	121
6.5	Conclusion . . . . .	121

<b>7</b>	<b>Top-Down Risk and Control Assessment: A Forward-Looking Approach to Evaluate Company-Wide Non-Financial Risk Exposure</b>	<b>123</b>
	<i>Hurdogan Irmak, Burcu Nasuhoglu, Dr. Erasmus Faber, Lorenzo Fantini, Benedetta Testino, Jannik Leiendecker, Barbara Fojcik, Dr. Georg Lienke</i>	
7.1	Introduction	123
7.2	Top-down vs. bottom-up: different approaches based on desired outcomes	124
7.2.1	Approaches: risk-specific focus vs. overarching non-financial risk coverage	124
7.2.1.1	Bottom-up approach: risk-specific, granular focus	125
7.2.1.2	Top-down approach: overarching, holistic non-financial risk coverage	125
7.2.2	Potential outcomes: different scope of risk-coverage and level of granularity	126
7.3	Key success factors: maximising the effectiveness of top-down risk and control assessments	126
7.4	Regulatory framework, best practice and standard setter guidelines	127
7.4.1	COSO ERM framework	127
7.4.2	Bank for International Settlements	128
7.4.3	EBA and ECB	128
7.5	Methodology of top-down risk and control assessment: evaluation of inherent risk, control adequacy and residual risk	129
7.5.1	Non-financial risk taxonomy as a starting point	129
7.5.2	Measurement of inherent risk	129
7.5.2.1	Calculation of severity	130
7.5.2.1.1	Organisation-specific risk indicators	130
7.5.2.1.2	Industry adjustments	132
7.5.2.1.3	Weighting of risk indicators based on data source reliability	133
7.5.2.2	Calculation of likelihood	133
7.5.2.3	Inherent risk matrix	134
7.5.3	Measurement of internal control adequacy	134
7.5.3.1	Control indicators	135
7.5.3.2	Weighting of control indicators	136
7.5.3.3	Control rating	136
7.5.4	Determination of residual risk	137
7.6	Breakout: building an institution-wide internal control system	138
7.6.1	Introduction	138
7.6.2	Alternative path to building an internal control framework: top-down, risk-based approach	138
7.6.3	Five-step approach: building an internal control framework	139
7.6.3.1	Step 1: determination of NFR criticality	139
7.6.3.2	Step 2: mapping of key risks to process landscape	139
7.6.3.3	Step 3: definition of control objectives, key controls and control repository	140

7.6.3.4	Step 4: assessment of controls	140
7.6.3.5	Step 5: design NFR control report	141
7.7	Approach to handling residual risk	141
7.7.1	High residual risk: project and investment imperative to mitigating residual risk	142
7.7.2	Medium-high residual risk: action plan to reduce inherent risk exposure	142
7.7.3	Medium-low residual risk: continuous control testing and selected action requested	142
7.7.4	Low residual risk: periodic, risk-based controls	142
7.8	Integrated process to perform annual top-down risk and control assessment	143
7.8.1	Phase 1: pre-assessment by control functions	143
7.8.2	Phase 2: assessment by business senior management	144
7.8.3	Phase 3: validation and reporting	144
<b>8</b>	<b>A Top-Down Approach to Non-Financial Risk Reporting: Collaboration Across Risk Types for Sustainable Risk Steering</b>	<b>145</b>
	<i>Valérie Villafranca, Dr. Georg Lienke, Florian Seiferlein, Kai Gammelin, Dr. Katharina Hefter, Norbert Gittfried</i>	
8.1	Introduction: the imperative of top-down non-financial risk reporting	145
8.2	Regulatory framework in selected key markets	146
8.2.1	European Union	146
8.2.2	United States	147
8.2.3	Hong Kong	147
8.2.4	Singapore	148
8.3	Current state of non-financial risk reporting: formats with inconsistent scopes and methodologies	148
8.3.1	Operational risk reports	148
8.3.2	Additional 2 <sup>nd</sup> LoD reports on specific non-financial risk types	149
8.3.3	Reports on internal control system	150
8.4	Key parameters of top-down non-financial risk reporting: methodology, required input and results	150
8.4.1	Identification and evaluation of key risk indicators	151
8.4.1.1	Determination of key risk indicators, thresholds and potential input sources	151
8.4.1.1.1	Step 1: understand risk factors	151
8.4.1.1.2	Step 2: identify key risk indicators	151
8.4.1.1.3	Step 3: derive institution-specific thresholds	151

8.4.1.2	Example KRIs: financial crime risk, outsourcing risk and human resources risk .....	152
8.4.1.2.1	Key risk indicators for financial crime risk .....	152
8.4.1.2.2	Key risk indicators for outsourcing risk ..	154
8.4.1.2.3	Key risk indicators for human resources risk .....	154
8.4.1.3	Evaluation of key risk indicators .....	155
8.4.2	Assessment of key controls as risk-mitigating measures .....	156
8.4.2.1	Step 1: capturing and allocation of controls .....	156
8.4.2.2	Step 2: assessment of controls .....	158
8.4.3	Determination of residual risk and required risk-mitigating actions .....	159
8.4.3.1	High level of residual risk .....	160
8.4.3.2	Medium level of residual risk .....	160
8.4.3.3	Low level of residual risk .....	161
8.5	Reporting process and governance .....	161
8.5.1	Governance arrangements .....	161
8.5.1.1	Board of directors .....	161
8.5.1.2	Chairman of the supervisory board .....	161
8.5.1.3	Central reporting unit .....	161
8.5.1.4	2 <sup>nd</sup> LoD control functions .....	162
8.5.1.5	Operational risk department .....	162
8.5.2	Reporting process .....	162
8.6	Conclusion .....	163
<b>9</b>	<b>Internal Investigations into Corporate Misconduct: Applying an Investigative Approach to Enable Proactive Risk Oversight .....</b>	<b>165</b>
	<i>Lora von Ploetz, Florian Seiferlein</i>	
9.1	Introduction .....	165
9.2	Selected laws, regulations and standards .....	166
9.2.1	Supervisory sanction relief based on voluntary investigation and cooperation .....	168
9.2.1.1	Jurisdictions potentially reducing sanctions and enforcement actions due to effective investigation and cooperation .....	168
9.2.1.2	Jurisdictions not explicitly providing a bonus for self-disclosure and cooperation .....	170
9.2.1.3	Jurisdictions where investigations and cooperation do not change assessment of law enforcement .....	170
9.2.2	Statutory disclosure requirements .....	171
9.2.3	Investigation standards and requirements .....	172

9.3	Concept for proactive risk oversight using an investigative approach	173
9.3.1	Investigation process	174
9.3.1.1	Proactive risk management	175
9.3.1.2	Strategic and tactical investigations	177
9.3.1.3	Example: sanctions-driven investigations	178
9.3.2	Information sharing and global risk management	181
9.3.2.1	How to connect needles in the same haystack (in a financial institution)	182
9.3.2.2	How to connect needles in different haystacks (between different financial institutions)	183
9.4	Success factors and common pitfalls	185
<b>10</b>	<b>Technical Application and Data Architecture for Non-Financial Risk Management</b>	<b>187</b>
	<i>Kai Gammelin, Björn Stauber, Dr. Christian N. Schmid, Dr. Jan-Oliver Fröhlich, Annika Melchert, Daniel Wagner</i>	
10.1	Introduction	187
10.1.1	A fragmented IT landscape	187
10.1.2	IT's impact on data availability	190
10.1.3	Data availability across borders	190
10.1.4	Additional challenges associated with group companies	190
10.2	Regulatory requirements	192
10.3	Six challenges in NFR management and reporting	193
10.3.1	Challenge 1: the lack of a defined NFR-IT strategy	193
10.3.2	Challenge 2: responsibility for and execution of NFR reporting-related activities (operational unit vs. NFR management)	194
10.3.3	Challenge 3: consistency and transparency of IT architecture	195
10.3.4	Challenge 4: alignment of data architecture for transparency on data lineage	196
10.3.5	Challenge 5: implementing a solid IT target architecture	197
10.3.6	Challenge 6: cost-benefit considerations	197
10.4	A target IT architecture for NFR	197
10.4.1	The NFR architecture ecosystem	200
10.4.2	Dashboards and reporting	200
10.4.3	Other key enabling technologies	201
<b>11</b>	<b>Data Governance in Non-Financial Risk Management</b>	<b>203</b>
	<i>Björn Stauber, Dr. Christian N. Schmid, Dr. Jan-Oliver Fröhlich, Annika Melchert, Daniel Wagner</i>	
11.1	Introduction	203
11.2	Regulatory requirements	204
11.3	Data governance to support NFR management	204
11.3.1	Data structures	205
11.3.2	Target operating model (TOM)	206
11.3.3	Data policies	207
11.3.4	Data tools	207

11.4	Scaling up state-of-the-art NFR data governance .....	208
11.4.1	Specific roles and responsibilities .....	210
11.4.2	Tool optimisation .....	212
11.5	Conclusion .....	212
<b>12</b>	<b>Optimising Effectiveness and Efficiency: Deployment of Artificial Intelligence in Non-Financial Risk Management .....</b>	<b>213</b>
	<i>Dr. Jochen Papenbrock, Dr. John Ashley, Dr. Georg Lienke, Florian Seiferlein, Norbert Gittfried</i>	
12.1	Introduction .....	213
12.2	Financial sector digitisation: the front-to-back case for AI .....	213
12.2.1	Digital transformation of business and operating models ....	214
12.2.1.1	Changed customer expectations and behaviour ....	214
12.2.1.2	Increasing efficiency challenges .....	214
12.2.2	Impact of COVID-19 .....	214
12.2.2.1	Accelerator of digitisation .....	215
12.2.2.2	Modified risk environment .....	215
12.3	Regulatory approach to artificial intelligence .....	216
12.3.1	Overview .....	216
12.3.1.1	European Union .....	216
12.3.1.1.1	European Commission .....	216
12.3.1.1.2	European Banking Authority .....	217
12.3.1.1.3	National financial supervisors .....	218
12.3.1.2	United States .....	218
12.3.1.3	Hong Kong .....	219
12.3.1.4	Singapore .....	219
12.3.2	Summary of key regulatory expectations .....	219
12.3.2.1	Governance .....	219
12.3.2.2	Design and development .....	219
12.3.2.3	Ongoing maintenance .....	220
12.4	Machine learning algorithms: Key learning modes and examples ....	221
12.4.1	Supervised learning .....	223
12.4.2	Unsupervised learning .....	223
12.4.3	Reinforcement learning .....	223
12.4.4	Deep learning .....	224
12.5	Deployment of AI in non-financial risk management .....	225
12.5.1	Financial crime prevention: biometric customer identification, dynamic CRR calculation and AI-based transaction screening	225
12.5.1.1	Know your customer: automated biometric identification of customers .....	225
12.5.1.2	Dynamic calculation of customer risk ratings: faster reaction to material changes in client risk profiles ...	226
12.5.1.2.1	Automatic data import into the CRR system .....	226
12.5.1.2.2	Dynamic recalculation of customer risk ratings .....	227



12.5.1.3	Negative news screening: AI-supported reduction of screening efforts .....	227
12.5.1.3.1	Matching of customer names to negative news .....	227
12.5.1.3.2	Contextual pre-evaluation of news articles .....	228
12.5.1.4	Sanctions name screening: AI-supported reduction of false positive alerts and pre-assessment of screening alerts .....	228
12.5.1.4.1	Reduction of false positive alerts via feedback loop .....	229
12.5.1.4.2	Pre-assessment of generated alerts and optimisation of manual alert reviews .....	229
12.5.1.5	Sanctions transaction screening .....	230
12.5.1.6	AML transaction monitoring: deploying artificial intelligence to manual investigations .....	230
12.5.2	Prevention of market abuse: AI-based detection of irregularities in securities trading .....	231
12.5.2.1	Behaviour-based tracking of trading portfolios: AI-based detection of irregular transactions .....	231
12.5.2.2	AI-based assessment of trader's voice and email communication .....	232
12.5.3	Management of AI (model) risk: key discipline for data-driven financial institutions .....	232
12.5.4	AI4ESG: tech-driven sustainable finance .....	235
12.5.5	AI infrastructure for non-financial risk management .....	236
12.6	Conclusion .....	239
<b>13</b>	<b>Core Elements of Conduct and Ethics in the Context of Non-Financial Risk .....</b>	<b>241</b>
	<i>Dr. Barbara Roth, Dr. Erasmus Faber, Dr. Julia Gebhardt, Dr. Katharina Hefter</i>	
13.1	Conduct risk: definitions, characteristics and regulatory landscape ..	241
13.1.1	Conduct and compliance, ethics versus integrity .....	241
13.1.1.1	Finding common ground: definition of key terms ..	241
13.1.1.2	Conduct-based versus integrity-based ethics .....	243
13.1.1.3	An integrative approach for synthesising conduct-/compliance-based and integrity-based ethics .....	244
13.1.2	What is meant when we talk about conduct risk? .....	246
13.1.2.1	No universal definition .....	246
13.1.2.2	Three key topics: market, client and employee conduct risk .....	247
13.1.3	Conduct risk in the NFR taxonomy .....	249

13.2 Regulatory landscape .....	250
13.2.1 European perspective .....	252
13.2.1.1 European/UK regulators .....	252
13.2.1.2 Other European countries .....	257
13.2.2 US perspective .....	260
13.2.3 Asia-Pacific perspective .....	262
13.3 Why conduct risk matters .....	265
13.3.1 Increased regulatory scrutiny .....	265
13.3.1.1 Focus on regulatory oversight .....	265
13.3.1.2 Frequency of regulatory actions .....	266
13.3.2 Supervisory and legal actions .....	267
13.3.2.1 Actions against firms .....	267
13.3.2.2 Actions against individuals .....	268
<b>14 Managing Conduct Risk: Framework and Perspectives .....</b>	<b>271</b>
<i>Prof. Dr. Martin Schulz, Dr. Julia Gebhardt, Dr. Katharina Hefter, Rene Bystron</i>	
14.1 Trends and perspectives in respect of conduct risk in the regulatory context .....	271
14.1.1 Treating Customers Fairly (TCF) .....	271
14.1.2 Senior management regimes as emerging global trends in conduct risk .....	273
14.1.2.1 UK .....	273
14.1.2.2 Hong Kong and Singapore .....	275
14.1.2.3 Malaysia .....	275
14.1.2.4 Australia .....	276
14.2 Conduct Risk Management as integral part of ESG .....	277
14.2.1 G like conduct .....	277
14.2.2 New legislative focus and recent regulatory developments ...	277
14.2.3 Activities at the EU level .....	278
14.2.4 Optimising ESG risk management .....	280
14.3 Managing conduct risk .....	281
14.3.1 The Conduct Risk House .....	281
14.3.2 Building a Conduct Risk framework .....	282
<b>15 Successful ESG Transition: Implications and Challenges for Effective Risk Management .....</b>	<b>285</b>
<i>Anita Varshney, Jannik Leiendecker, Aytech Pseunokov</i>	
15.1 Introduction .....	285
15.2 Regulatory frameworks in selected key jurisdictions .....	287
15.2.1 General overview .....	287
15.2.2 European Union .....	288
15.2.2.1 Non-Financial Reporting Directive & Corporate Sustainability Reporting Directive .....	289
15.2.2.2 Sustainable finance taxonomy .....	290

---

---

15.2.2.3 EU Disclosure Regulation .....	293
15.2.2.4 EU Prudential Regulations .....	293
15.2.3 United States .....	295
15.2.4 Hong Kong .....	298
15.2.5 Singapore .....	299
15.3 Sustainable finance: upcoming challenges for companies .....	300
15.4 Target picture: effective management of ESG risk .....	303
15.4.1 ESG strategy .....	303
15.4.2 Governance and organisation .....	305
15.4.3 ESG risk steering .....	307
15.4.4 Identification of enabling factors .....	310
15.4.5 ESG as an opportunity .....	311
15.5 Conclusion .....	312
Bibliography .....	315



## 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 Leindecker** 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 Gammel, 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%.<sup>1</sup> 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.<sup>2</sup>

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.

---

<sup>1</sup> IMF 2021.

<sup>2</sup> 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 Gebra, 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.<sup>1</sup> In response, financial institutions have dramatically enhanced their oversight capabilities, leading to a proliferation of risk managers, internal auditors, control special-

---

<sup>1</sup> 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 func-

tions 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-