Governance, risk and compliance (GRC) survey analyses for 7th Risk Summit

UNIVERSITY OF CAMBRIDGE
Judge Business School

Centre for
Risk Studies

21st of June 2016

GRC survey participation offered to all invitees of Cambridge Risk Summit

Approach

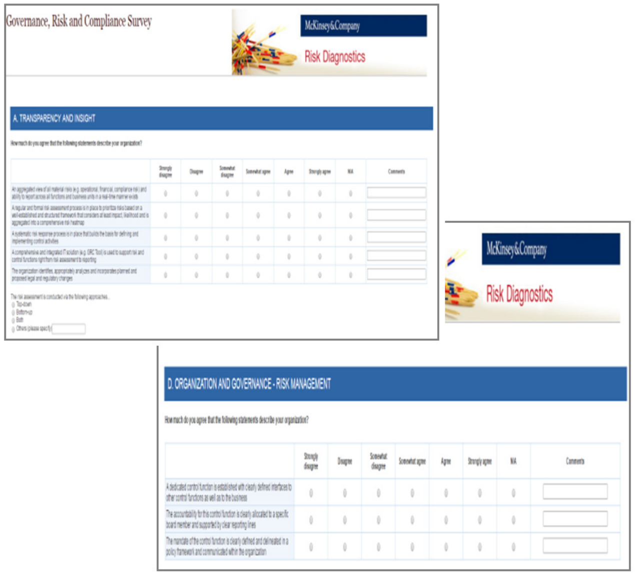
- Survey structured around **comprehensive GRC framework** with 5 dimensions
- Benchmarking against best practices and providing first **insights for improvement potential**, not approaching statistical evidence
- **Aligned with industry standards** and calibrated to enable comprehensive peer benchmarking

Set-up

- **Online-survey** with **additional interviews** with key stakeholders
- Ring-fenced **diagnostic team** conducting benchmarking analysis

Participants

- **50+ participants** thereof **~20 corporates ~20 financial institutions**, **~10 academic institutions** and **~5 others**



Governance, Risk and Compliance Survey

McKinsey&Company

Risk Diagnostics

A. TRANSPARENCY AND INSIGHT

How much do you agree that the following statements describe your organization?

	Strongly disagree	Disagree	Somewhat disagree	Somewhat agree	Agree	Strongly agree	N/A	Comments
An aggregated view of all material risks (e.g. operational, financial, compliance risk) and ability to report across all functions and business units in a real-time manner exists	○	○	○	○	○	○	○	
A regular and formal risk assessment process is in place to prioritize risks based on a well-established and structured framework that considers at least impact, likelihood and is aggregated into a comprehensive risk heatmap	○	○	○	○	○	○	○	
A systematic risk response process is in place that builds the basis for defining and implementing control activities	○	○	○	○	○	○	○	
A comprehensive and integrated IT solution (e.g. GRC Tool) is used to support risk and control functions right from risk assessment to reporting	○	○	○	○	○	○	○	
The organization identifies, appropriately analyzes and incorporates planned and proposed legal and regulatory changes	○	○	○	○	○	○	○	

The risk assessment is conducted via the following approaches...

○ Top-down
○ Bottom-up
○ Both
○ Others (please specify)

McKinsey&Company

Risk Diagnostics

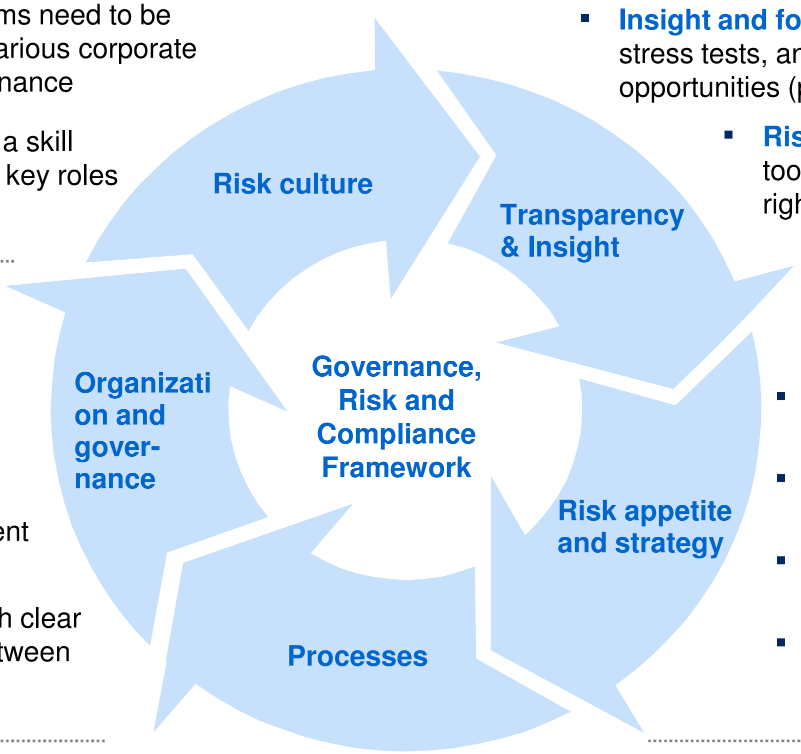
D. ORGANIZATION AND GOVERNANCE - RISK MANAGEMENT

How much do you agree that the following statements describe your organization?

	Strongly disagree	Disagree	Somewhat disagree	Somewhat agree	Agree	Strongly agree	N/A	Comments
A dedicated control function is established with clearly defined interfaces to other control functions as well as to the business	○	○	○	○	○	○	○	
The accountability for this control function is clearly allocated to a specific board member and supported by clear reporting lines	○	○	○	○	○	○	○	
The mandate of the control function is clearly defined and delineated in a policy framework and communicated within the organization	○	○	○	○	○	○	○	

SOURCE: GRC survey 2016

McKinsey GRC survey addresses all dimensions of an effective risk management framework



Risk culture

Transparency & Insight

Risk appetite and strategy

Processes

Organization and governance

Governance, Risk and Compliance Framework

- **Culture:** ensure soundness of risk culture across entire organization (perform culture diagnostic)
- **Norms:** new risk norms need to be embedded through various corporate processes and governance
- **Skill building:** implement a skill enhancement program for key roles

- **Taxonomy:** establish common vocabulary for the different risks
- **Risk register/risk heatmap:** characterize and prioritize risk based on probability, impact and preparedness
- **Insight and foresight:** use business-specific scenarios, stress tests, and early indicators, to understand risks and opportunities (potentially also for key customers and peers)
- **Risk Models:** build simple model as support tool for business decisions – tools have no right in itself!
- **Reporting:** focus on key risks and provide clarity on these to allow actionable measures

- **Natural ownership:** decide which risk you are the natural owner of and which not
- **Risk capacity:** understand how much risk you can take
- **Risk appetite:** decide with how much you risk-taking you feel comfortable
- **Risk strategy:** decide on actions to transform your risk profile including trade-off with corresponding cost

- **Archetypes:** define mandate of the risk function
- **Organization & governance:** design risk organization across entire organization and ensure appropriation of top management
- **Risk function profile:** establish clear allocation of responsibilities between risk taking and controlling units

- **Risk-related decisions:** embed risk in business decision making rather than pure compliance-oriented paper pushing

Risk optimization: embed in each major strategic decision *before* launch/positive decision

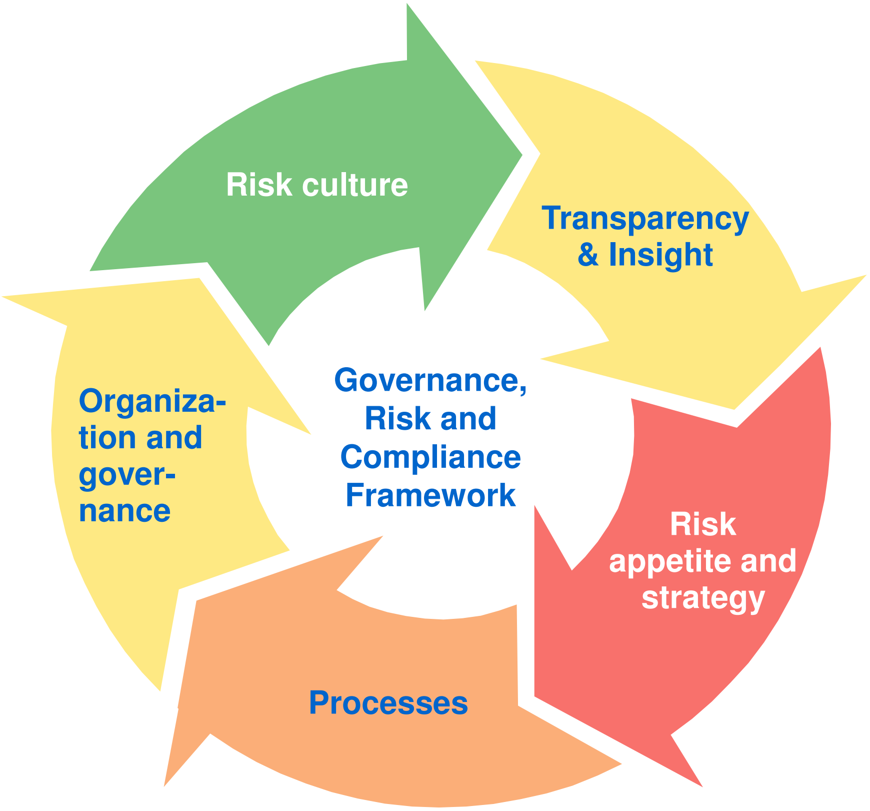
Processes: design and execute core business processes and operations on a risk-informed basis

SOURCE: McKinsey Risk Management Practice

Results: Overall risk culture strong compared to other elements of the GRC framework

Average of scores

Relative weakness 🟥🟧🟨🟩 Relative strength


Risk culture
Transparency & Insight
Risk appetite and strategy
Processes
Organiza-tion and gover-nance
Governance, Risk and Compliance Framework

SOURCE: GRC survey 2016

Results: Strengths and weaknesses across the five elements of the GRC framework

🟩 Strenghts
🟥 Weaknesses

Key observations	GRC framework	Key observations
▪ Most participants are able to identify, analyze and incorporate planned and proposed legal and regulatory changes ▪ Regular and formal risk assessment process is in place to prioritize risks based on likelihood & impact	Transpa-rency & insight	▪ Participants partly lack comprehensive and integrated IT solution (e.g. GRC Tool), aggregated view of all material risks ▪ Ability to report across functions & BUs can be enhanced
▪ Policies and limits are up to date and an explicit risk strategy is in place to ensure sound risk and control understanding	Risk appetite & strategy	▪ The risk appetite statement needs to be effectively linked to strategic decisions and ensure proper cascading throughout the organization
▪ Risks are appropriately incorporated in budgeting/ planning process and strategic decisions ▪ Well-defined control standards for anti-trust, bribery & corruption, financial reporting, M&A and investments activities in place	Processes	▪ Role of risk needs to be enhanced for capital planning processes ▪ Control function needs to have an effective role in managing risk esp. fraud & theft, tax, data privacy
▪ Internal control function has a clearly defined interfaces to other control functions as well as to the business ▪ Mandate of the internal control function is clearly defined and delineated in a policy framework	Organization and governance	▪ GRC function needs to have a more clearly defined interface to other control function & businesses ▪ There is scope to enhance the mandate & policy framework of this function
▪ Employees in the organization have a clear understanding of current and emerging risks and how to aggregate them ▪ People feel a personal accountability for risk, irrespective of their role	Risk culture	▪ The feedback culture including initiating discussion about difficult topics and challenging current practices is not very advanced and needs more attention

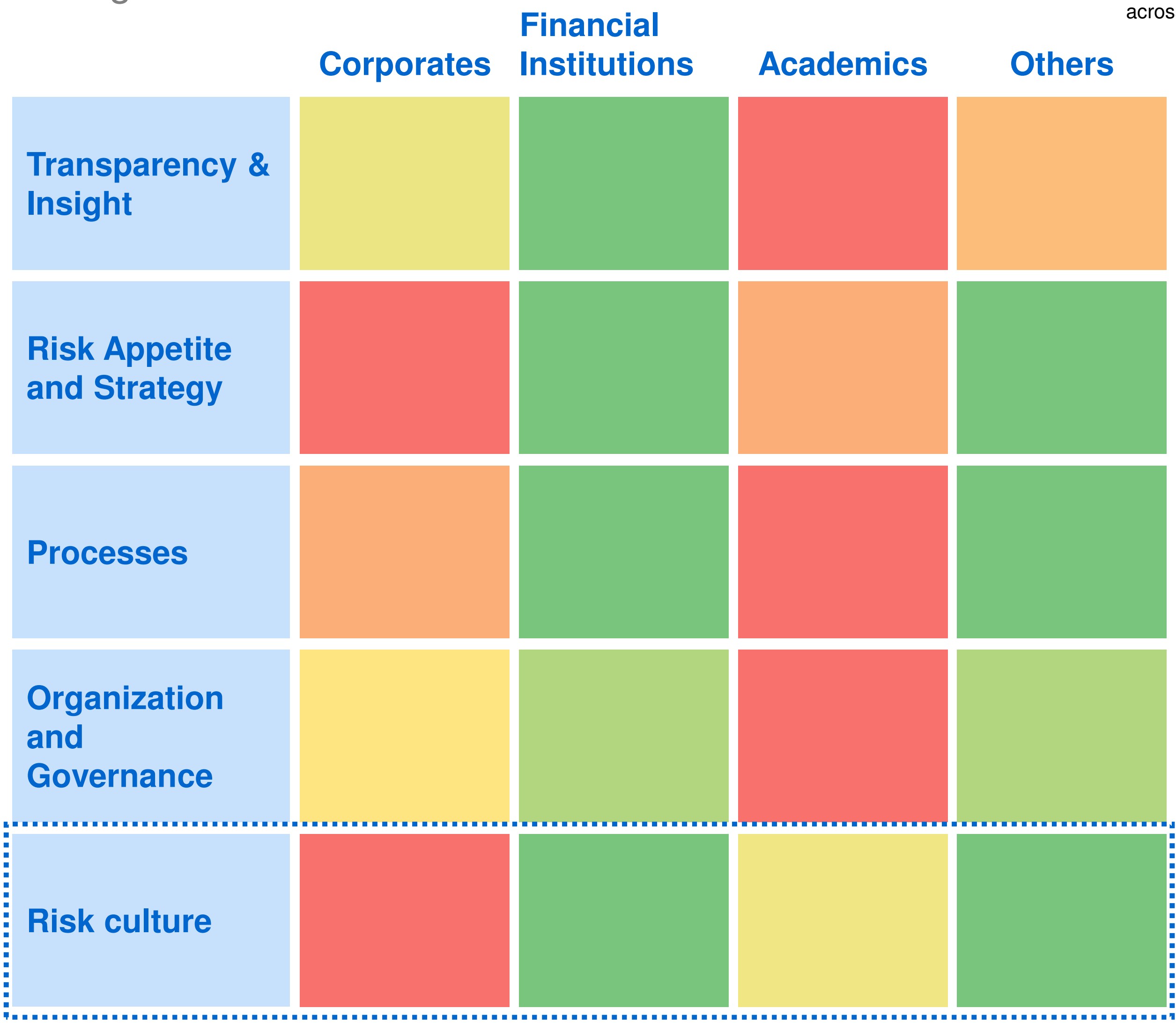
SOURCE: GRC survey 2016

Results: A comparison of the different subgroups of participants shows financial institutions as most mature in terms of GRC capabilities

Average of scores

Relative weakness across dimension 🟥🟨🟩 Relative strength across dimension

⬚ Further detailed on next slide



	Corporates	Financial Institutions	Academics	Others
Transparency & Insight	🟨	🟩	🟥	🟧
Risk Appetite and Strategy	🟥	🟩	🟧	🟩
Processes	🟧	🟩	🟥	🟩
Organization and Governance	🟨	🟩	🟥	🟩
Risk culture	🟥	🟩	🟨	🟩

- The banking industry is performing relatively better to others because of -
  - Continued expansion of the breadth and depth of regulation (e.g. OCC heightened expectations, Basel III/IV, stress testing)
  - Most banks have started to digitalize their core processes
  - Incorporate advanced analytics, bid data, machine learning in day to day decision making
- However, corporates and academics on the other hand need to really invest on digitalization, advanced analytics, improve stress testing, develop a stronger risk culture etc.

SOURCE: GRC survey 2016

Results: Detailed insights into cultural dimension of GRC framework

Relative weakness across dimension 🟥🟧🟨🟩 Relative strength across dimension

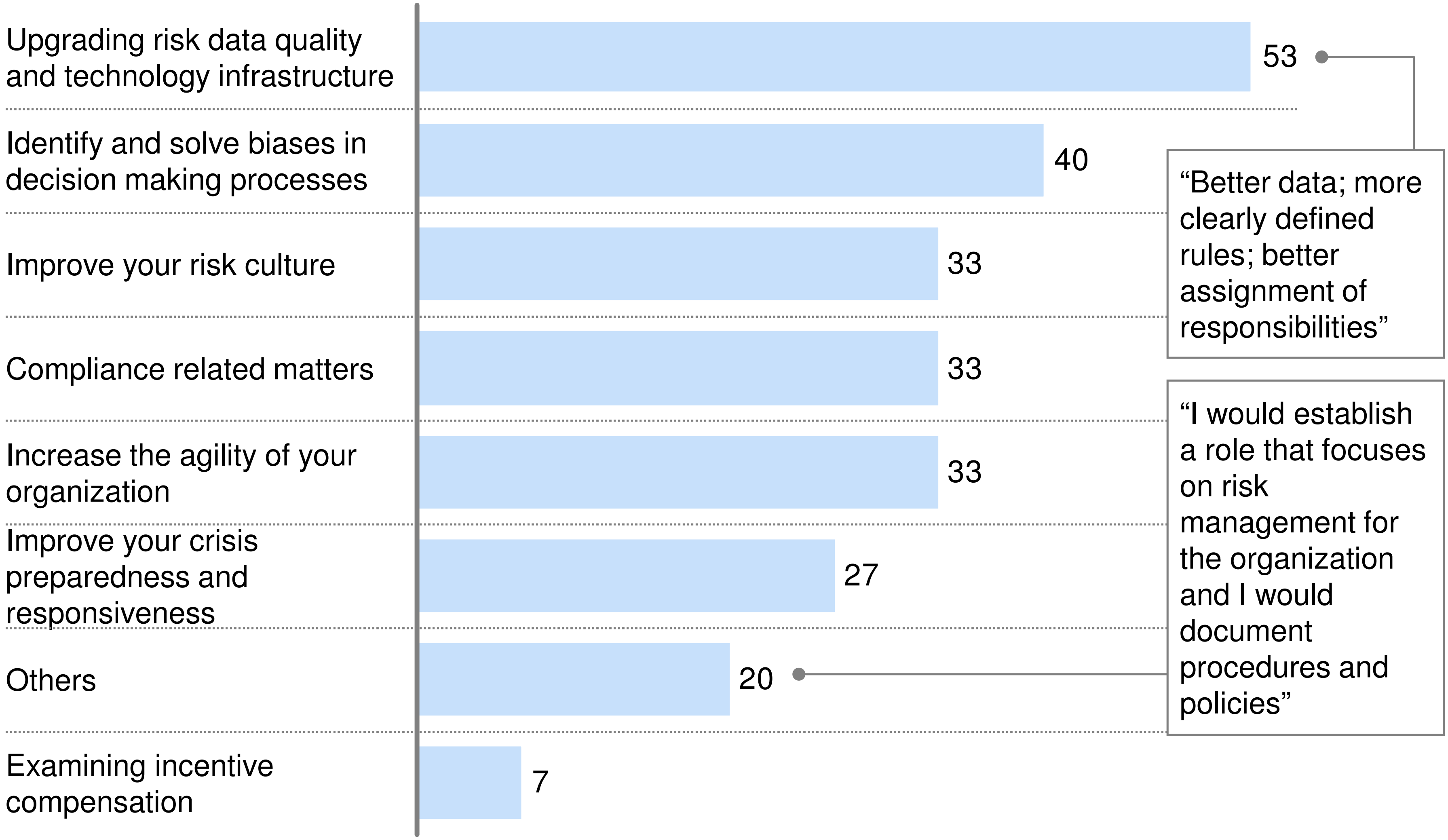
Average of scores

Risk culture dimensions		Corporates	Financial Institutions	Academics	Others
Transparency	Level of insight	🟥	🟩	🟧	🟩
	Tolerance	🟥	🟩	🟨	🟩
	Communication	🟨	🟩	🟨	🟥
Acknow-ledgement	Confidence	🟩	🟩	🟥	🟥
	Openness	🟨	🟩	🟥	🟨
	Challenge	🟧	🟩	🟩	🟥
Responsive-ness	Speed of response	🟩	🟩	🟧	🟥
	Level of care	🟨	🟩	🟨	🟥
Respect	Cooperation	🟥	🟧	🟩	🟩
	Adherence to rule	🟥	🟩	🟧	🟩

SOURCE: GRC survey 2016

Results: Data quality and biases in decision making as top priorities for risk function in next 3 years

Percentage of respondents



"Better data; more clearly defined rules; better assignment of responsibilities"

"I would establish a role that focuses on risk management for the organization and I would document procedures and policies"

SOURCE: GRC survey 2016

Results: Examples how to address observed spots of weakness

EXAMPLES

		Example levers
A	Transparency and insight	▪ Enhance **risk reporting**, e.g., define **top-down set of reporting metrics** and **group-wide MIS**; de-duplicate reports; introduce risk dashboard
B	Risk appetite and strategy	▪ Agree consistent **risk appetite metrics** and cascade **risk appetite framework** and methodology throughout organization
C	Processes	▪ Harmonize **policies and guidelines** for risk approval; establish policy advisory panel
D	Organization and governance	▪ Review and define **interfaces** between GRC and other control functions and businesses
E	Culture	▪ Develop a targeted **risk curriculum** to **enhance risk awareness and knowledge** (e.g., including staff rotations and on-the-ground experience for risk function)

SOURCE: GRC survey 2016

McKinsey contacts

Dr. Sven Heiligtag

Partner, Hamburg

+49 40 3612 1346

Sven_heiligtag@mckinsey.com

Please reach out to us in case of further questions or if you should be interested into a customized feedback report

Dr. Susanne Maurenbrecher

Risk expert, Hamburg

+49 40 3612 1452

Susanne_maurenbrecher@mckinsey.com

SOURCE: McKinsey Risk Management Practice