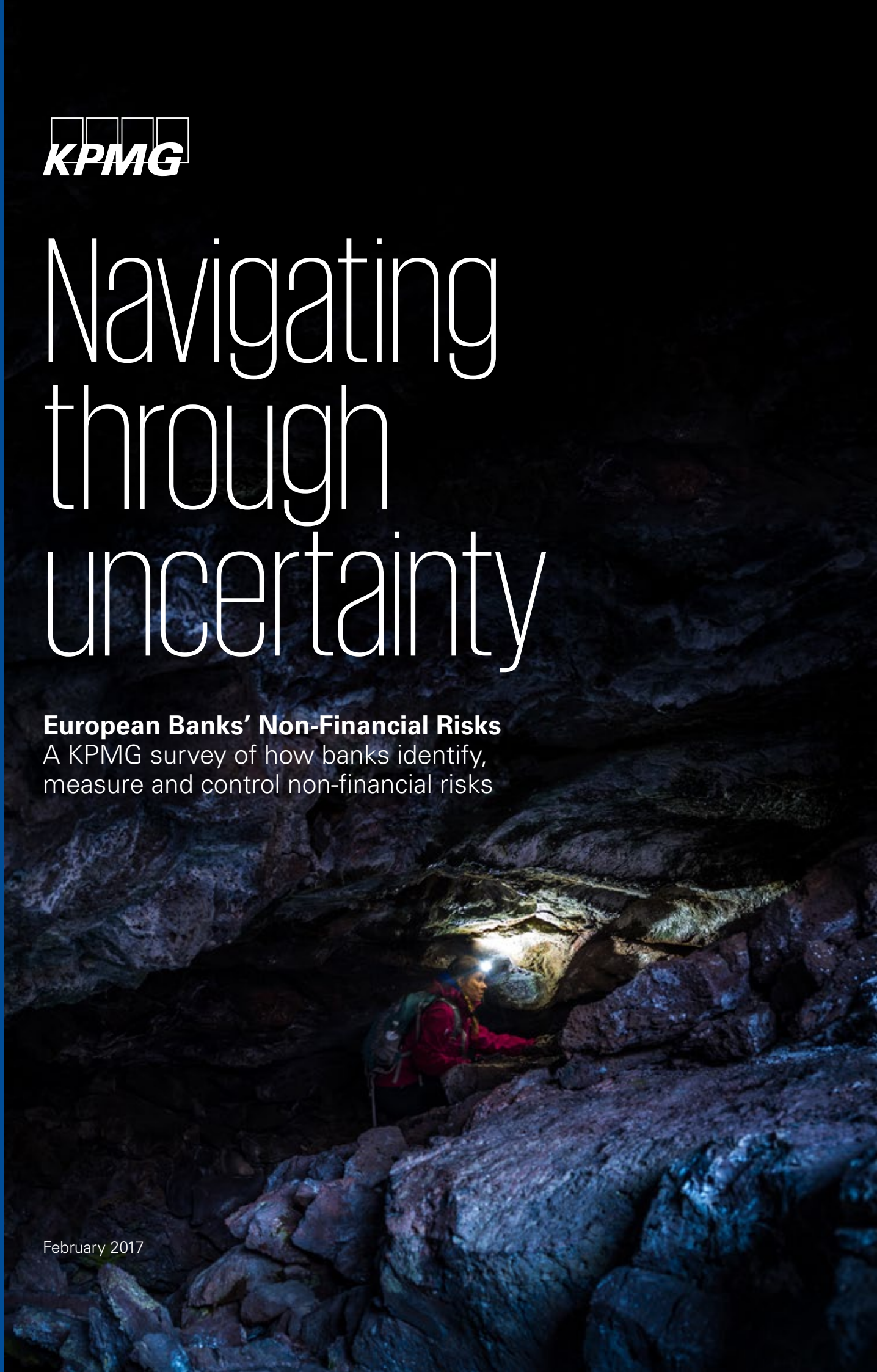
KPMG

Navigating through uncertainty

European Banks' Non-Financial Risks
A KPMG survey of how banks identify, measure and control non-financial risks



February 2017

Contents

Introduction

Costs and charges arising from banks' non-financial risks have increased sharply in recent years. In part this reflects the compensation and litigation costs relating to misconduct, but it has also been driven by the costs of IT failures and cyber attacks. Recent and prospective regulatory requirements and supervisory actions not only impose additional compliance costs but also require banks to take a more strategic view of how they identify, measure and control their non-financial risks.

KPMG professionals wanted to understand better how banks are responding to these developments and to provide banks with an opportunity to share and compare their views with peers across the market. We therefore undertook a survey last year to review how banks identify, measure and control their non-financial risks. This covered operational risk generally; detailed sub-categories of operational risk; and reputational, strategic and business risks. Thirty-six European banks responded to the survey, of which 33 are supervised by the European Central Bank and three are outside the Single Supervisory Mechanism.

The survey results highlighted the importance of banks' non-financial risks. Nearly half of the respondents reported that such risks accounted for more than 10 percent of their banks' total losses, and that operational risk represented more than 10 percent of risk weighted exposures.

In this Report we present the main findings from the survey, covering how banks view their existing frameworks for non-financial risks; the areas where banks are looking to make improvements; the challenges posed by regulation and supervision, risk culture, risk appetite and risk ownership; the focus on IT and compliance risks; and the scope for banks to pay more attention to their business and strategic risks.

> KPMG wanted to understand better how banks are responding to these developments and to provide banks with an opportunity to share and compare their views with peers across the market.

Non-financial risk

For the purposes of this Report, non-financial risks comprise all risks that are not credit, market, counterparty, interest rate or liquidity risk. They encompass operational, reputational, strategic and business risks, as well as disturbances in the management of financial risks. Non-financial risks include disturbances in the regular processes of running a bank, and risks that arise from reacting to internal or external changes or from the failure to do so.

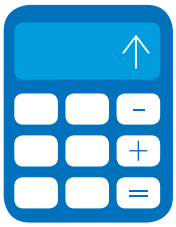
Key findings from the survey

1.

Non-financial risks are important

- Non-financial risks make a significant contribution to banks' losses and capital requirements.
- Regulatory capital requirements for non-financial risks are expected to increase, in particular through the ICAAP/ SREP process and Pillar 2 capital add-ons.
- Supervisory scrutiny of how banks manage, control and monitor their non-financial risks is also expected to increase.

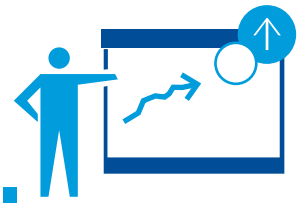
2.



Banks are planning to develop their frameworks for non-financial risks

- Nearly all banks are planning to enhance their frameworks for non-financial risks, with almost half planning a comprehensive overhaul.
- Regulatory and supervisory pressures are key drivers here, but banks are also responding to internal drivers such as internal audit findings and the scope for cost reductions.
- In many banks risk management capabilities for non-financial risks are less well developed than for financial risks.

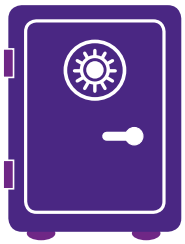
3.



The assessment and measurement of non-financial risks is the main area for improvement

- Many banks identify the assessment and measurement of non-financial risks as a key area for improvement.
- This may reflect in part the limitations of the advanced measurement approaches to operational risk, and the prospect of regulators removing the use of internal modelling approaches to the calculation of regulatory capital requirements for operational risk.

5.



Many banks do not specify an effective risk appetite for non-financial risks

- Risk appetite statements typically cover non-financial risks only at group or legal entity level, not at business unit or department level.
- Limitations in risk metrics (beyond capital requirements and observed losses) make it difficult for banks to identify where and when non-financial risks are increasing beyond risk appetite.

7.

Many banks are addressing non-financial risks primarily through an emphasis on IT and compliance risks

- A focus on IT and compliance risks is evident in banks' self-identification of non-financial risks and in their internal audit programmes, internal risk reporting, and risk management processes.
- This is not surprising given the regulatory focus on these aspects of non-financial risks, and the impact of new technologies.

4.

Banks also identify the need to align more effectively the elements of managing non-financial risks, to enhance risk reporting and to strengthen risk culture

- Many banks are seeking to take a more consistent and comparable approach to the management of different types of non-financial risk.
- Risk reporting of non-financial risks is often not comprehensive and not comparable in its coverage.
- Banks recognise that non-financial risks need to be included within the increasing focus on risk culture.

6.

Risk ownership and challenge under the three lines of defence model remain unclear

- Many banks find it difficult to identify who owns non-financial risks, particularly in the business (the first line of defence).
- Where risks are managed in the second line of defence this can hinder the ability of second line control functions to act as an independent challenger of a front line risk owner.

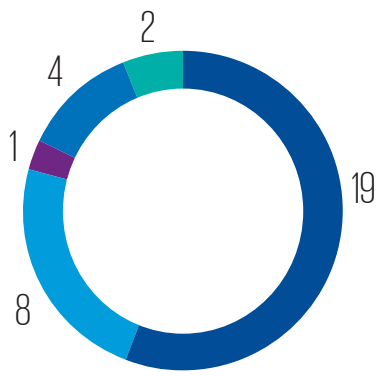
8.

Strategic and business risks remain out of focus in most banks' frameworks for non-financial risk

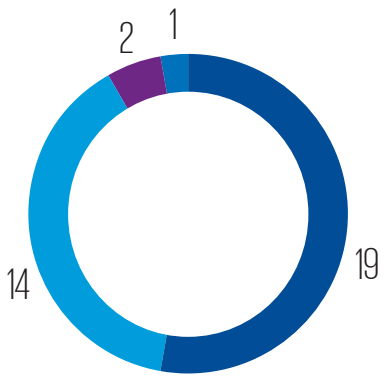
- Most banks find it difficult to identify, measure and control their strategic and business risks.
- This requires greater consideration by banks, not least as many of them struggle to identify viable and sustainable business models and to respond to technological and market developments, and as supervisors focus increasingly on banks' profitability and business models.

1. The importance of non-financial risks

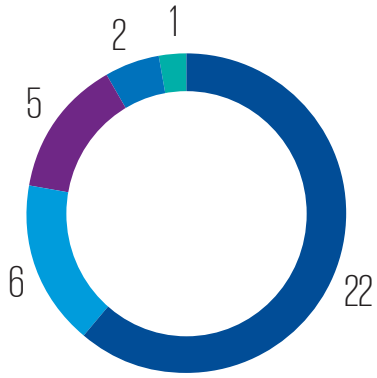
a. Losses from non-financial risks as a proportion of the bank's total losses:



b. Regulatory capital charges against operational risk as a proportion of the bank's Pillar 1 capital requirement:



c. Internal (ICAAP) capital requirement for non-financial risks as a proportion of the bank's total internal capital requirement:



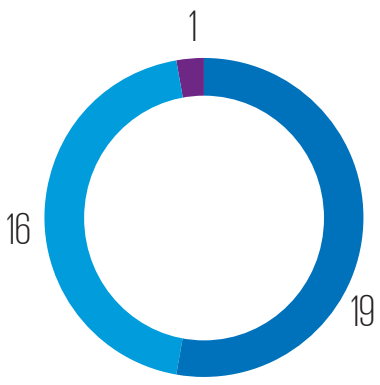
The importance of non-financial risks is evident from their contribution to banks' losses and capital requirements. Losses arising from non-financial risks represent more than 10 percent of total losses in nearly half of the banks in the sample, and more than 20 percent of total losses in one-fifth of the banks in the sample.

Banks also reported that they expect capital requirements against non-financial risks to increase, in some cases by between 50 and 100 percent, and that supervisory scrutiny of these risks would intensify.

■ <10% ■ 10-20% ■ 20-30%
■ 30-50% ■ >50%

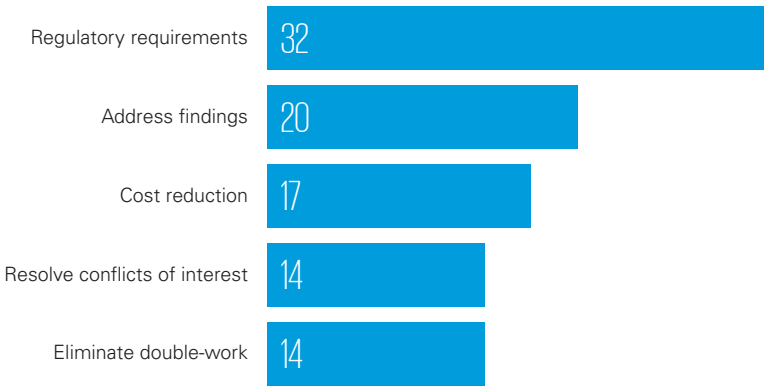
2. Enhancing banks' frameworks for non-financial risks

a. Number of banks planning to develop further their framework for non-financial risks:



■ Yes, but limited to selected areas
■ Yes, comprehensively
■ Not decided yet

b. Main drivers of the further development of the framework for non-financial risks:



Almost all banks in the sample are planning to develop further their frameworks for non-financial risks, with almost half the banks planning a comprehensive enhancement.

The main driver of this is regulatory requirements, but many banks are also enhancing their frameworks to improve their risk management and to reduce costs.

3. Main areas for further development

Areas of focus for the further development of banks' frameworks for non-financial risks:

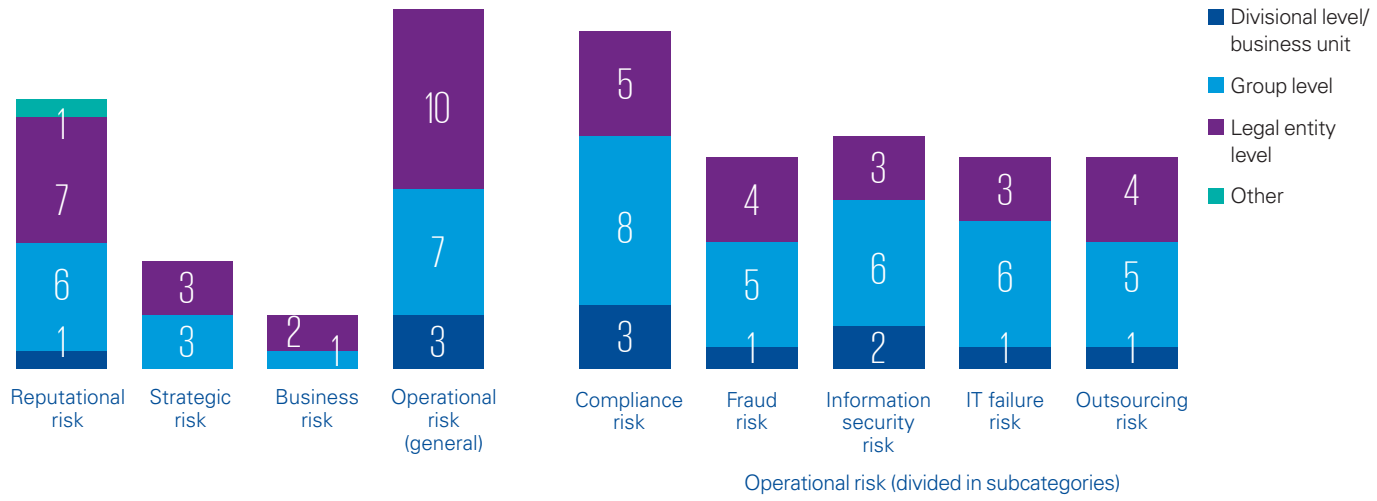
Half the banks in the sample identify the assessment and measurement of non-financial risks as a key area for improvement. This may be because banks are placing greater emphasis on capturing the build-up of non-financial risks where there may not be an initial financial impact and where capital may not be an effective mitigant, for example vulnerabilities in core banking systems.

Banks also identify the need to align more effectively the management of different types of non-financial risks, including the ways in which these types of risk are defined, owned, challenged and reported.

Banks recognise that the increasing focus on risk culture is at the heart of covering non-financial risks.

4. Setting risk appetite for non-financial risks

Organisational level at which risk appetite is defined:



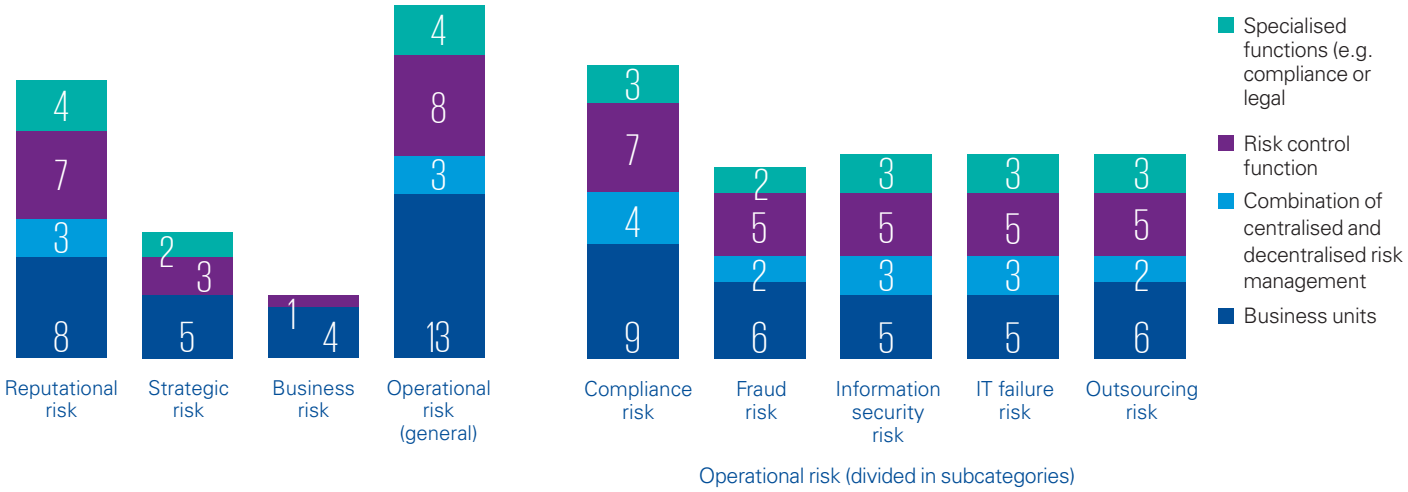
Most banks in the sample do not set a risk appetite for all types of non-financial risk.

Even where risk appetites are defined for non-financial risks, this is usually done only at group or legal entity level, not at divisional or business unit level.

This in turn limits the extent to which risk appetite statements can support the management of non-financial risks through metrics (beyond capital requirements and observed losses) that would enable a bank to identify where and when non-financial risks threaten to breach risk appetite.

5. Risk ownership

First line of defence responsibilities for managing non-financial risks:



The relatively low number of responses suggests that for some banks the ownership and management of non-financial risks other than overall operational risk and compliance risk is currently not well established in the business (the first line of defence).

Moreover, around half the banks responded that non-financial risks are managed by either a risk control function or by a combination of centralised and decentralised risk management. This allocation of risk management suggests that the first line of defence does not own these risks, or that ownership may be unclear, and may hinder the ability of second line control functions to provide independent challenge to a front line risk owner.

6. Identification of specific non-financial risks

a. Sub-categories of non-financial risk identified by banks:

b. Non-financial risks subject to audits by internal audit, external audit or supervisors over the last two years:

Where banks in the sample self-identified non-financial risks most were compliance and IT risks. This focus on IT and compliance risks is evident in banks' internal audit programmes, internal risk reporting and risk management processes.

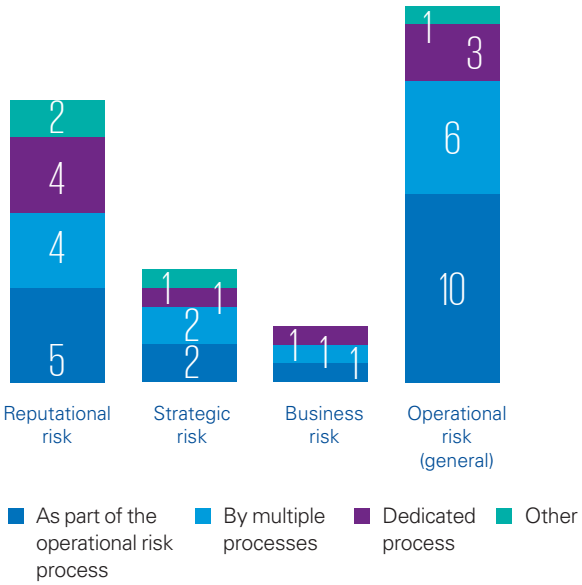
This is not surprising, given the regulatory focus on these aspects of non-financial risks, the impact of new technologies, and strategic moves to digital platforms and offerings.

Conclusions and key issues for banks

7. Strategic and business risks

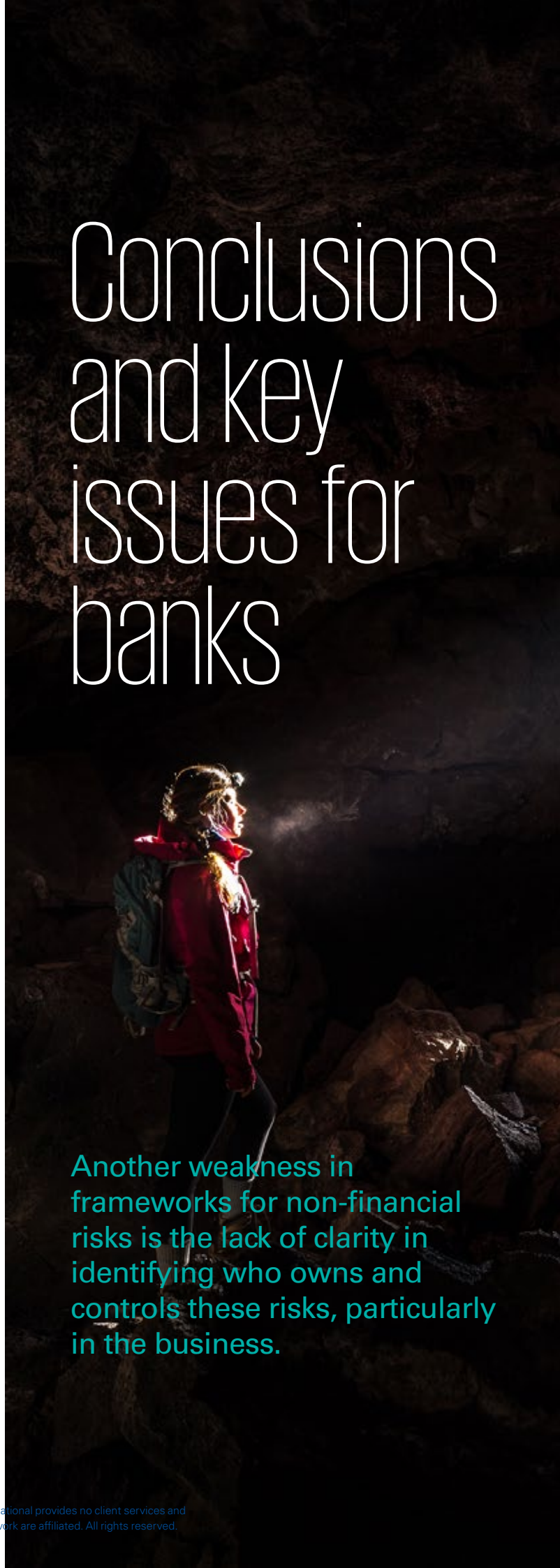
a. Organisational level at which risk appetite is defined:

b. Tracking risk management measures:



For most banks in the sample, their frameworks for the management of non-financial risks do not capture strategic and business model risks. Banks appear to find it difficult to identify, measure and control these risks.

Banks need to place more emphasis on assessing these risks, not least as many of them struggle to identify viable and sustainable business models and to respond to technological and market developments, and as supervisors focus increasingly on banks' profitability and business models.



Another weakness in frameworks for non-financial risks is the lack of clarity in identifying who owns and controls these risks, particularly in the business.

These survey results highlight the importance of non-financial risks and the ways in which banks are identifying, measuring and controlling these risks.

Regulatory and supervisory pressures

Perhaps not surprisingly, **regulatory and supervisory pressures stand out in the survey as key drivers** of banks' management of non-financial risks. Most banks expect regulatory capital requirements for non-financial risks to increase, in particular through the ICAAP/SREP process and Pillar 2 capital add-ons.

Banks are also seeing intensified supervisory scrutiny of how they manage their non-financial risks, including through the increasing supervisory focus on banks' profitability and business models and on risk culture within banks.

Enhancing frameworks for non-financial risks

Nearly all banks are planning to enhance their frameworks for non-financial risks, with many planning a comprehensive overhaul. While banks identify regulatory requirements as the most important driver here, it is clear that internal and external audit findings are also a key driver.

The objective for banks should be to reduce and to manage more effectively their non-financial risks – and thereby to reduce future losses arising from these risks.

Many banks identify the assessment and measurement of non-financial risks as the most important area for improvement. Banks need to place greater emphasis on capturing the build-up of non-financial risks where there may not be an initial financial impact and where capital may not be an effective mitigant, for example vulnerabilities in core banking systems.

Another area for improvement is the **need for banks to align more effectively the management of different types of non-financial risks**, including the ways in which these types of risk are defined, owned, challenged and reported. For example, many banks are seeking to take a more consistent and comparable approach to the management of different types of non-financial risk.

The identification of these areas for enhancing non-financial risk frameworks is also consistent with banks focusing mostly on **compliance and IT risks**, reflecting not only the priorities of auditors and supervisors but also technological innovation and the threat of cyber attacks.

Banks also recognise that an increasing focus on risk culture is an important element in managing their non-financial risks.

Limitations in frameworks for non-financial risks

Most banks' frameworks for non-financial risks do not effectively cover strategic and business risks, which banks seem to find difficult to identify, measure and control. Banks need to focus more on this, particularly as many of them seek to identify viable and sustainable business models in a changing economic, technological and market environment.

Many banks do not specify an effective risk appetite for non-financial risks. Their risk appetite statements typically cover non-financial risks only at group or legal entity level, not at business unit or department level, while limitations in risk metrics (beyond capital requirements and observed losses) make it difficult for banks to identify where and when non-financial risks are increasing beyond risk appetite.

Another weakness in frameworks for non-financial risks is the **lack of clarity in identifying who owns and controls these risks,** particularly in the business (the first line of defence). In some banks some of these risks are managed in the second line of defence or through some combination of the first and second lines, which can run counter to the role of second line control functions to provide independent challenge.

Banks are enhancing their non-financial risk frameworks, in particular with respect to:

- Assessment and measurement
- Coverage of strategic and business risks
- Specific and effective risk appetite
- Implementation of the three lines of defence model
- Focus on risk culture

Key issues for banks

The results of our survey suggest that banks' senior management should be asking themselves some key questions about how they identify, measure and control their non-financial risks.

Q. Is my framework for non-financial risks adequately covering all the major non-financial risks my bank is facing?

Non-financial risks take heterogeneous forms. They require specific expertise from multiple areas to manage them effectively. Specific risk management processes that cover the particularities of the bank's major non-financial risks should be established.

Q. Do I understand the impact of strategic decisions on my risk profile?

Strategic decisions are likely to have a significant impact on the overall risk profile of a bank. Strategic risk is itself a major non-financial risk, but may not be well understood by a bank.

Q. Do upgrades of my framework for non-financial risks improve my ability to mitigate and control risk and thereby reduce future losses?

Enhancing frameworks for non-financial risk purely in response to regulatory and supervisory pressures, and to internal and external audit findings, may not enable banks to maximise the effectiveness of their frameworks in reducing risks and future losses.

Q. How does my focus on the risk culture of my bank read across to non-financial risks?

It is important to understand and shape the prevailing risk culture, and to assess the impact of this culture on non-financial risks. Indeed, a strong and positive risk culture is the most fundamental risk mitigation tool available for non-financial risks. Strengthening the risk culture of a bank should not focus solely on its impact on financial risks such as credit and market risk.

Q. Do I encourage the business and its support units to own non-financial risks?

Unclear roles and responsibilities in the management of non-financial risks, and shifting ownership to the second line of defence, is likely to impair risk ownership by the first line of defence and to weaken the risk culture.

Q. Does my appetite for non-financial risk support decision making?

A clearly stated risk appetite linked to specific limits and controls should allow risk owners to understand when they are in line with a bank's risk strategy and appetite – and when they are not. Risk appetite metrics need to be cascaded down to the level where decisions are made and risk is mitigated.

Q. Do I focus too much on the financial impact of NFR events?

The measurement and assessment of non-financial risks should not focus only on the immediate financial impact of an event. Forward-looking assessments should also take account of the non-financial impacts of events such as disturbance in IT systems and reputational loss. Banks also need to scan the horizon for the potential emergence of non-financial risks.

Q. Is my reporting across the sub-categories of non-financial risk consistent?

Applying different methodologies across heterogeneous non-financial risks can lead to inconsistent reporting, with a potential for unclear or contradictory recommendations for the management of these risks.

Contact us:

Dr. Holger Spielberg
Partner
Financial Services
KPMG in Germany
T: +49 89 9282 4870
E: hspielberg@kpmg.com

Andrea Colombo
Associate Partner
Financial Risk Management
KPMG in Italy
T: +39 34 8308 0010
E: andreacolombo@kpmg.it

Daniel Quinten
Partner, Co-Head KPMG's ECB Office
EMA region
KPMG in Germany
T: +49 89 9282 4910
E: dquinten@kpmg.com

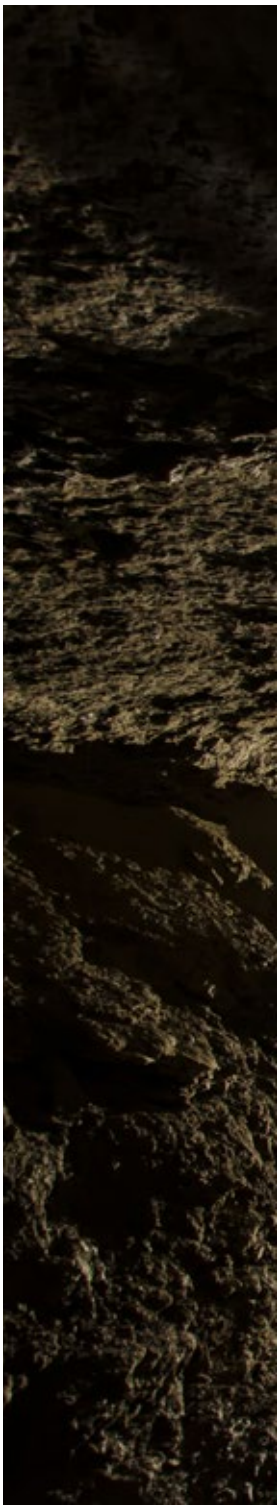
Dr. Henning Dankenbring
Partner, Co-Head KPMG's ECB Office
EMA region
KPMG in Germany
T: +49 69 9587 3535
E: hdankenbring@kpmg.com

Fiona Fry
Partner
Head of EMA FS Regulatory
Centre of Excellence
KPMG in the UK
T: +44 20 7694 2364
E: fiona.fry@kpmg.co.uk

Clive Briault
Senior Advisor
EMA FS Regulatory Centre
of Excellence
KPMG in the UK
T: +44 20 7694 8399
E: clive.briault@kpmg.co.uk

Prof. Dr. Thomas Kaiser
Director
Financial Services
KPMG in Germany
T: +49 69 9587 6283
E: thomaskaiser@kpmg.com

Carsten Zecher
Senior Manager
Financial Services
KPMG in Germany
T: +49 69 9587 2316
E: czecher@kpmg.com



kpmg.com

kpmg.com/socialmedia

kpmg.com/app

Create Graphics | CRT076011 | February 2017