Deloitte.

BU CF Deloitte Banking Union Centre in Frankfurt

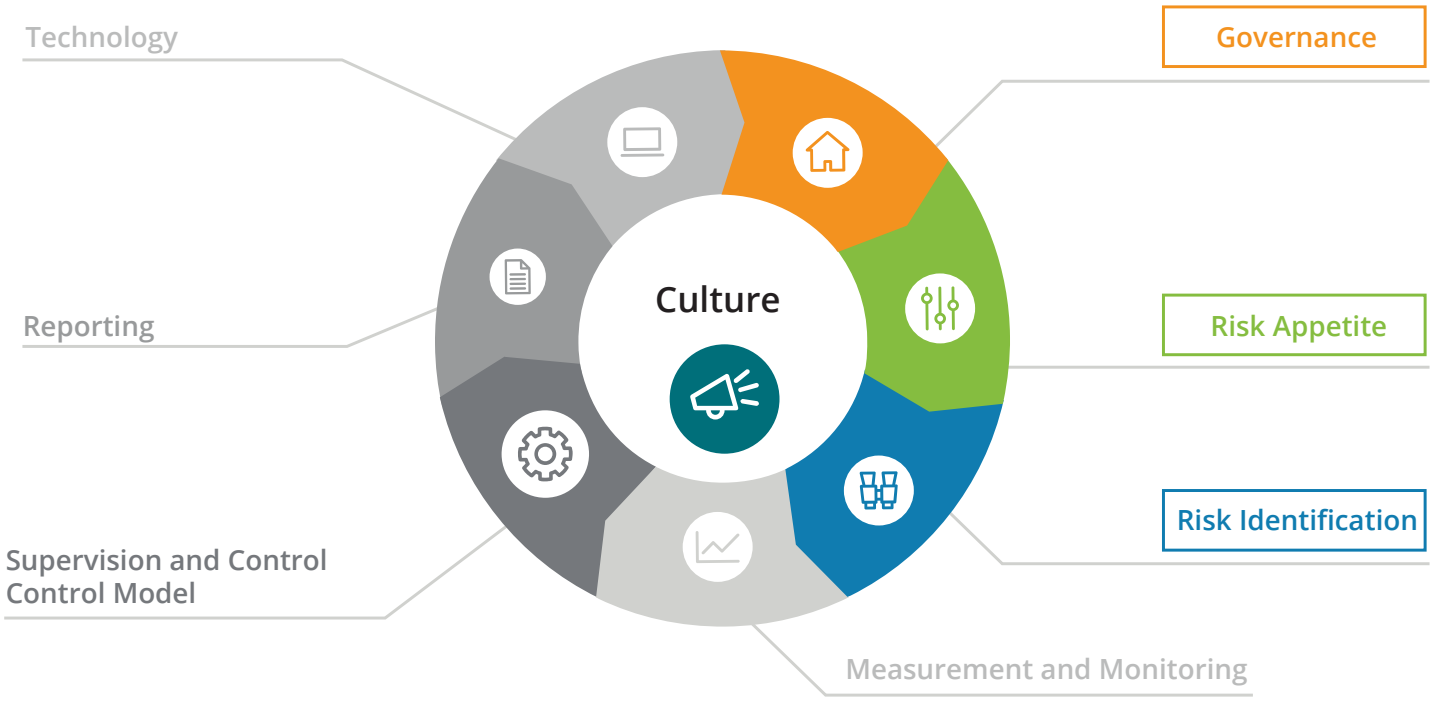
Non-Financial Risk Management Insights Series

Issue #4 – A risk culture built to last

Risk culture refers to the norms, attitudes, and behaviors related to risk awareness, risk taking, and risk management in an organization. Risk culture's significance increases for non-financial risk (NFR), as it can be difficult to create policies and procedures to manage all of them. Shortcomings in conduct, compliance, and other elements of non-financial risk are often the result of a risk culture gone sideways. Since the financial crisis, regulators have been dialing up the accountability. In this issue, we unpack the risk culture dimension of the NFR framework, including ways to assess it.

Non-Financial Risk Management

A Deloitte series explores the eight dimensions of managing non-financial risk.



- The pressing case to design and implement a Non-Financial Risk Management Framework
- Issue #1 – Risk taxonomy and risk identification
- Issue #2 – Risk appetite
- Issue #3 – Governance

Introduction

The financial services industry has had its share of misconduct scandals in recent years. From market benchmark manipulation to fake accounts and front-running, the result has been billions of dollars in fines[1] and even, in some cases, legal consequences for employees.

Misconduct is just one problem of non-financial risk that can stem from a risk culture gone sideways. Values and beliefs drive culture and determine behaviors that an entire organization brings to risk and risk management. It starts with the organization's purpose, is influenced by the "tone at the top" and extends all the way through the core principles or values that employees exhibit in their day-to-day work. Employees need to know what to do when no one else is watching – and this emanates from a superior risk culture.

Risk culture has been a relevant topic in the financial services industry for many years. Facing greater scrutiny from regulators, financial institutions have begun to reexamine the drivers that can affect their ability to maintain standards of conduct, meet evolving regulatory expectations, and earn the public's trust. In the discussion that follows, we will explore what it takes to evaluate and improve risk culture in the context of NFR.

[1]Elisa Martinuzzi, "The next round of bank scandals will be personal," Bloomberg, May 20, 2019, https://www.bloomberg.com/opinion/articles/2019-05-20/bank-scandals-turn-to-non-financial-misconduct

Deloitte's definition of an effective risk culture includes a culture of compliance, in which everyone understands the organization's approach to risk management and compliance, takes personal responsibility to manage risk in everything they do, and encourages others to follow their example. We think of corporate culture as all-encompassing in an organization, and risk culture as a specific portion of the overall corporate culture that includes a culture of compliance.

First, though, let's take a closer look at the regulatory environment.

Evolving regulatory expectations

"Culture and ethics," onetime Eurozone bank supervisor Daniele Nouy observed, "are at the heart of banks' decisions in terms of risk-taking and safe and sound management practices."[2]

This sums up the perspective of regulatory agencies around the globe. The Financial Stability Board has considered reforms to risk governance and compensation structures, both of which hold significant influence over risk culture. They have also asked organizations to consider ways to improve market structure, standards of practice, and incentives. Another international body, the Group of Thirty, has recommended ongoing, active management of culture as part of a firm's business strategy.

In the UK, the Financial Conduct Authority has pursued business attestations on the soundness of the control environment for conduct and fraud risk in foreign exchange wholesale sales and trading. Additionally, the Chartered Institute of Internal Auditors encourages firms to include risk and control culture reviews as part of their annual audit plan. Meanwhile, Australia's prudential regulator released Prudential Standard CPS 220, which intensifies scrutiny of culture and non-financial risks. The Australian Prudential Regulation Authority has increased minimum capital requirements for banks that fall short of meeting appropriate thresholds for corporate culture and governance risks.

Challenges

As the focus on NFR tightens, regulators are cracking down—and turning their attention to individual accountability and liability in the C-suite and Board. In effect, they are raising the stakes to get risk culture right.

However, it is not widely understood what an effective risk culture looks like. As an intangible, culture can be hard to quantify. One avenue to capturing observations is to conduct studies specifically designed to reveal NFR concerns. Important information can also be found in artifacts such as culture-related training modules, turnover rates and compensation structures (including incentives). But this is easier said than done for organizations that lack the data and analytics resources for an effective assessment.

Then there is execution. After identifying potential vulnerabilities in the existing risk culture, it is important to clearly define what the culture needs to become, complete with a plan for getting there. The plan can even include and highlight competitive advantages resulting from an enhanced risk culture. Typical levers for culture transformation include:

Leadership. Leaders shape the organization's risk culture and serve as role models for exemplary behavior. They regularly and consistently include NFR references and terminology in their communications, with an eye to highlighting NFR as a legitimate area that deserves attention and focus. This extends to communicating the conduct expected of employees while empowering them to support the organization's mission, vision, and values. For example, leadership might hold town hall meetings to explain different aspects of a positive risk culture and how they link to everyday work.

Organizational design. The number of layers in an organization, along with the hierarchical processes in place, can affect cultural norms by determining how employees make decisions. Both the operating model and the organizational structure must make room for clear roles and responsibilities related to risk culture. Also key: a sense of accountability, which can reinforce the desired culture and support effective NFR management. One way to convey this is with a "three lines of defense" model that guides the implementation of incentives and responsibilities across key NFRs.

Talent and rewards. A leading area of impact is in human resources. Recruiting, onboarding, orientation, succession and retention are where organizations select those who fit their desired culture and set expectations. Additionally, compensation, including financial and non-financial incentives, can have a significant effect on the behaviors that drive risk culture. Consider, for instance, the potential cultural effects of changing the bonus structure to emphasize bottom-line results instead of sales.

Governance and business systems. Culture has a symbiotic relationship with governance, policies, and procedures, making it critical that these reinforce the vision for managing NFR as broadly as possible. Investment prioritization, strategic planning, budgeting, and product or service launch decisions also should take place in the context of an effective risk culture. Community investment and corporate social responsibility programs are examples of how governance can support risk culture, in this case by mitigating NFR related to the organization's reputation.

Other potential levers include "tone in the middle", purpose, and diversity and inclusion, to name a few. Risk culture transformation therefore demands a relentless focus on strategy and the ability to work across all areas of the organization.

[2] Danièle Nouy, "Towards a new age of responsibility in banking and finance: Getting the culture and the ethics right," presented at Goethe Universität in Frankfurt, November 23, 2015. https://www.bankingsupervision.europa.eu/press/speeches/date/2015/html/se151123.en.html

Our approach

To get a sense of where an organization's risk culture currently stands, specifically in the context of non-financial risks, it helps to know what questions to ask (and keep asking). Here are five conduct risk questions to start with:

1. Do your business practices create an incentive for individuals to behave in ways that can lead to misconduct?
2. Are your NFR controls robust enough to adequately discourage and detect wrong behaviors or bad outcomes?
3. Is your control environment forward-looking, so that it can head off cases of misconduct and non-compliance across key NFRs?
4. Do people in the organization identify and assess NFRs in their day-to-day activities?
5. Are the consequences for taking unacceptable risks, including NFRs, applied proactively and consistently?

The questions may seem diverse, but they are all aimed at gauging a handful of conditions:

- **Risk competence**—the collective risk management competence of the organization
- **Motivation**—the reasons why people manage risk the way they do
- **Relationships**—how people in the organization interact with others
- **Organization**—how the organizational environment is structured, and what is valued

These are the main influencers of an organization's risk culture. Each of them has associated key performance indicators, as the illustration shows. Together, they provide a structured, holistic lens through which risk culture may be objectively understood.

Deloitte's Risk Culture Assessment Framework

This framework [3] aims to serve as a starting point and reduce the complexity of measuring, strengthening and reporting on risk culture. At the same time, it combines human capital and risk management perspectives to give a richer, more comprehensive understanding of the ways risk culture and overall broader culture are instilled throughout an organization.

A typical implementation challenge includes deploying cost effective and repeatable mechanisms to gather credible evidence for each indicator.

[3] "Culture: why does it matter?," February 5, 2019, https://insidenow.deloitte.lu/culture-why-does-it-matter/article/

Conclusion

Risk culture is an essential dimension of managing non-financial risk. Recognizing this, regulators are increasing their scrutiny of the norms, attitudes, and behaviors that financial services leaders cultivate in the course of managing risk while doing business.

The conclusion is that policies alone are not enough to ensure the long term sustainable competitive advantage of an organization. Financial institutions must understand their culture and how it affects risk awareness, risk taking and risk management within the organization. Beyond that, the leadership team must create the vision for risk culture and take an active role in making it a reality.

Other dimensions of NFR may be more tangible, but that only underscores the importance of tone from the top in building a strong, sustainable non-financial risk culture. An effective framework will bring clarity and focus to the effort, paving the way for a risk culture that holds up under day-to-day work pressures as employees pull together to achieve the organization's goals.

Contacts

Ricardo Martinez
Principal | Risk & Financial Advisory
Deloitte & Touche LLP
rimartinez@deloitte.com

Gerhard Schröck
Partner | Risk Advisory & Leader BUCF
gschroeck@deloitte.de

Narayan Raghavan
Senior Manager | Risk & Financial Advisory
Deloitte & Touche LLP
nraghavan@deloitte.com

Deloitte.

Issued 4/2020