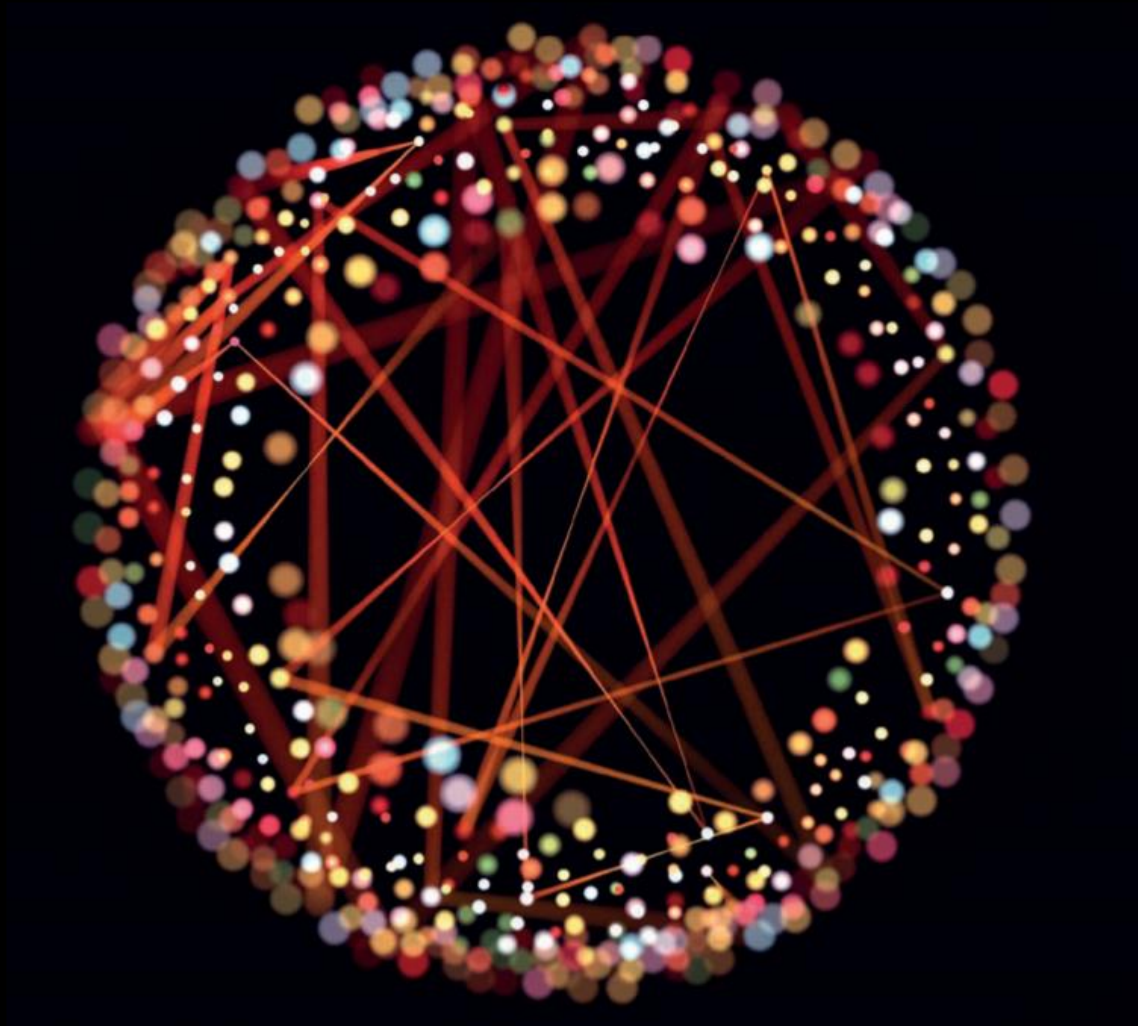
Deloitte.



Non-Financial Risk Governance

NFR in today's environment

Irina Arsinte - June 2018

Risk Advisory

Today's external environment

Financial Institutions operate in a complex and competitive environment driven by four main external forces

EMERGING TECHNOLOGIES

Technology innovation is changing the way clients interact with the Bank, by creating **new FinTech trends and revenue pools**, but also new paradigms in banking organization

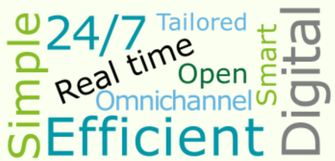
- ***Instant Lending***
- ***AI/ Cognitive***
- ***New Payments***
- ***RPA***
- ***Blockchain***
- ***Internet of Things***

NEW PLAYERS

Technology innovation is **reducing the entry barriers**, by letting new competitors to emerge in the Banking Sector and forcing **Banks to rethink themselves**

A NEW GENERATION OF CUSTOMERS

Customers are becoming **more powerful**: they have more data, more choices, more influence. To match this power, companies must shape their business around customer journeys



REGULATORY PRESSURE

In the last years **banking regulations** became **stricter**, especially about risk management topics, by imposing both **threats and opportunities**

MIFID II

PSD2 (Open Banking)

IV/V AML Directive

Basel III/IV

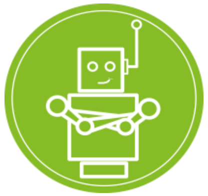
GDPR

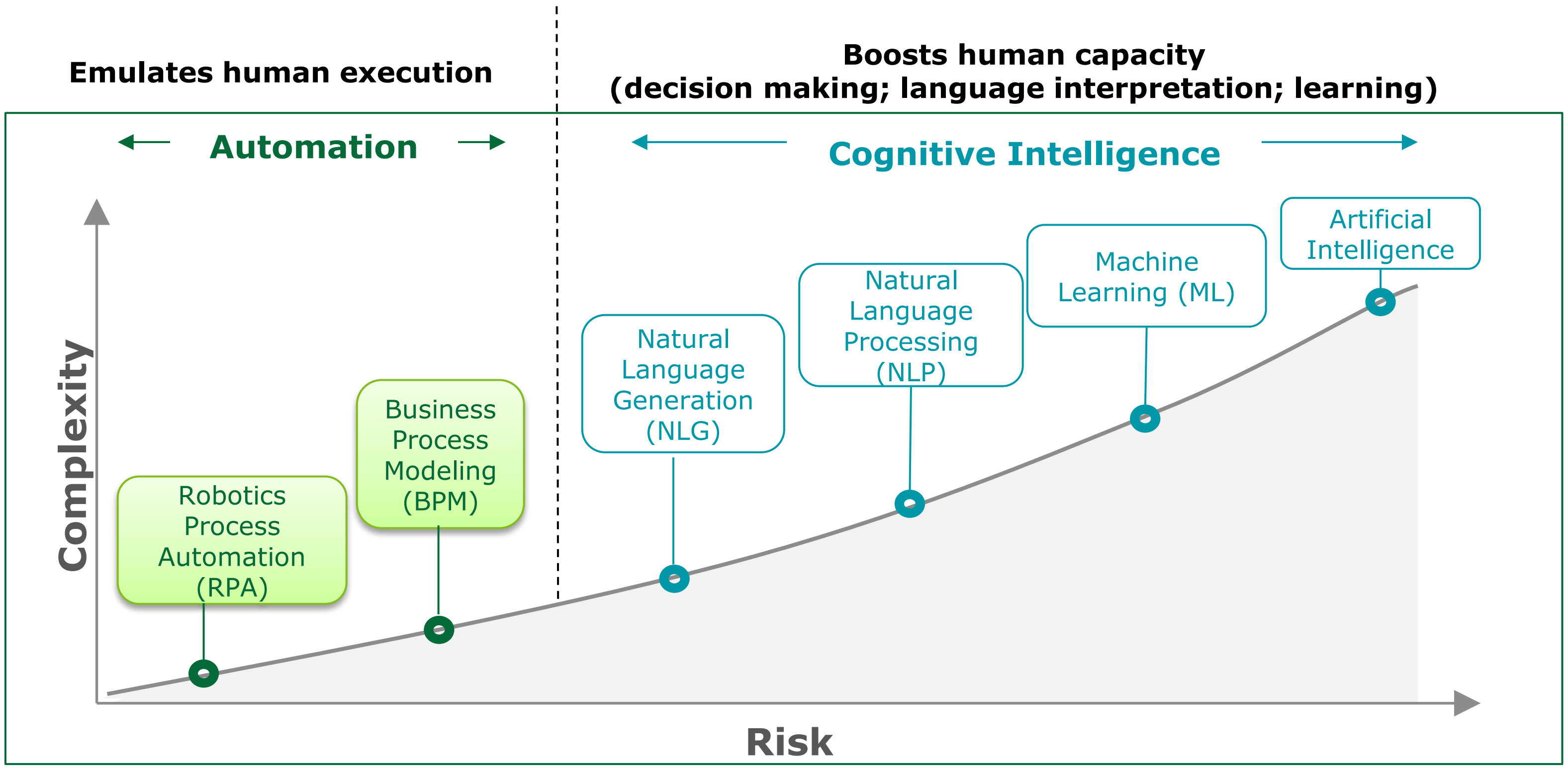
New technologies in Banks' front-offices and operations

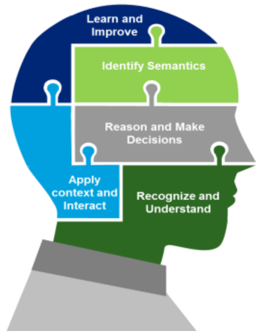
Automation and Cognitive solutions introduce new, complex risks

How to ensure smart technology **adheres to policies**?

What **oversight/assurance** is needed across the 3 Lines of Defense?







NFR in the current context

Non Financial Risk management is becoming more relevant

Economic and reputational impact

- The NFR's economic impact can be high, and it can produce operative, legal and reputational implications

Supervisory focus

- **Expectations on NFR** were included in recent stress tests of EBA and SREP letters.
- **Proactivity from the Entities** is expected.
- NFR to be accounted for in ICAAP/ILAAP as **"material risks"**

Difficulties in measurement and monitoring

- **A standard** methodology for measurement and management **does not exist** for all NFR. Therefore entities need to develop and implement their own methodology, preferably in an **homogeneous** way, measuring and monitoring **all risks**.

Needed involvement from multiple areas

- A correct management of NFR **impacts** most of the **Organisation**.
- An integrated risk management **improves efficiency** avoiding duplicities and getting a better **governance** of its own.

Managing NFRs is increasingly important

Taxonomy Non Financial Risks*

	Current management	Future Focus	Impact
Operational Risk	◕	→	◕
Conduct Risk	◔	↑	●
Compliance Risk	◑	↑	●
Cyber Risk	◕	↑	●
IT Risk	◕	↑	◕
Strategic Risk	◑	↑	◕
Model Risk	◑	↑	◕
Legal Risk	●	→	◕
Third-Party Risk	◕	→	◑
Reputational Risk	◔	↑	●

● High level of management / High Impact ○ Low level of management / Low Impact ↑ High focus → Medium focus

Sample self-assessment questions to initiate change

- Does the entity have an NFR risk inventory?
- Is there an existing Risk Appetite Statement approved by the Board of Directors of the Entity for NFRs?
- Is the board and senior management aware of and involved in management of NFRs?
- Has the entity defined a three lines of defence model for managing NFRs?
- Has the entity differentiated the management structure for financial risk management and NFR?
- Has the entity established a methodology for the measurement and monitoring of NFRs?

* Deloitte BRIM® extract

An integrated NFR Management Framework

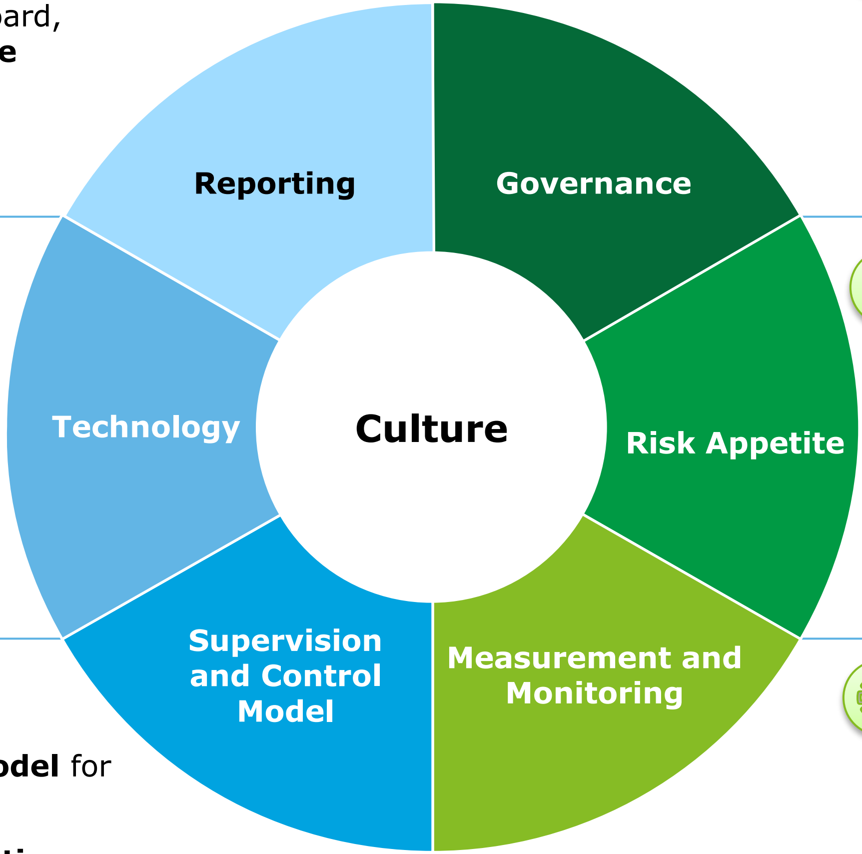
NFR management is still unduly fragmented, involving lots of functions, methodologies, systems, reporting, and people

Reporting

- Internal: enhance value to Board, through a **common language**
- External: **supervisory expectations**

Governance

- **Roles** and **responsibilities** definition across the 3 lines of defense (LoD)
- Decision making



Technology

- **Systematic** and automated management of Non Financial Risks, favouring scalability and **flexibility**

Risk Appetite

- Incorporation of NFR to the **Risk Appetite Framework** of the Entity
- **Integration** in **management** and **lining up** with the Entity's **strategy**

Supervision and Control

- **Definition** of the **Control Model** for every Non Financial Risk
- **Control Model homogenization** for every Non Financial Risk
- **Efficient management** of the **Model**

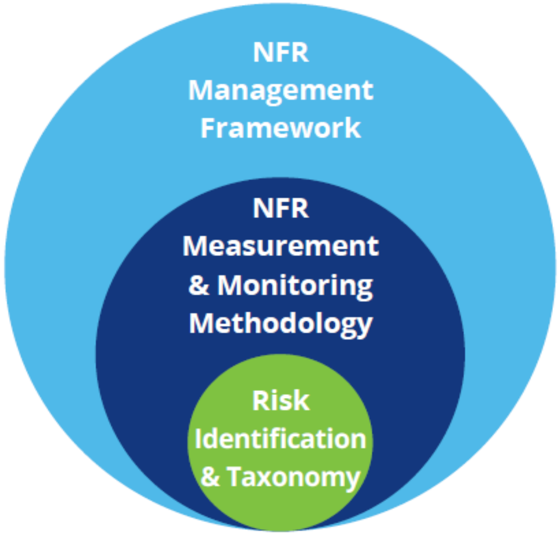
Measurement and Monitoring

Implementation of a model to guarantee the risk measurement in an homogeneous and objective manner:

- Risk **Taxonomy**
- Thresholds, **metrics** and objective scorings
- **Capital** impact

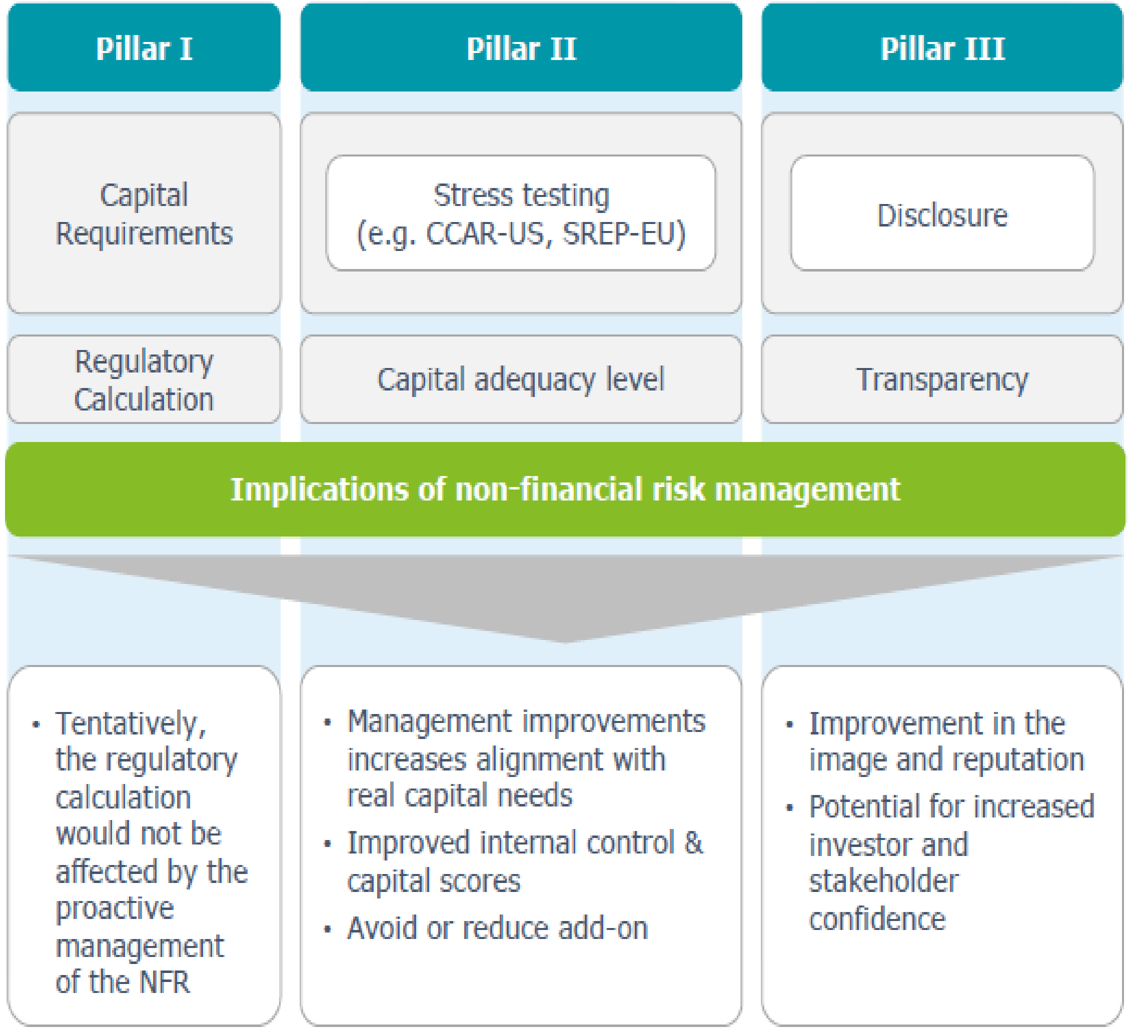
Measuring NFR

Potential economic capital implications derived from implementing a NFR Management Framework



A NFR Management Framework will allow banks to:

- Link NFRs to the bank´s Risk Appetite
- Articulate and communicate the NFR approach and resulting benefits on risk culture and conduct
- Quantify relevant NFRs, define related limits, thresholds and triggers
- Assign clear roles and responsibilities
- Strengthen top-down communication, bottom-up reporting and external disclosure
- Extend NFR to all supporting policies, processes and controls and identify required technologies



Risk Appetite

An integrated Risk Appetite Framework, covering financial and non-financial risks, is fundamental to informed decision-making and steering an institution

Principle

- The term 'Risk Appetite' refers to the aggregate level of risk and the types of risk an institution is willing to assume.
- Business lines should have appropriate processes and controls in place to ensure that risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the institution's risk appetite.

Importance

- The RAF represents the foundation for a holistic risk management throughout the institution.
- The development of an appropriate risk culture is highly dependent on the effectiveness of the RAF.
- Turning RAF into measurable key risk indicators allows the firm to identify and determine the relative positions of its risk capacity, risk profile and risk appetite when pursuing its strategy and business model and to take corrective actions when necessary

Formalisation

- The SSM Supervisory Statement on governance and risk appetite proclaims that 'formalisation of the RAF is a prerequisite for effective implementation'.
- This formalisation should include the link between the RAF and other strategic processes such as ICAAP, ILAAP, the recovery plan and the remuneration framework.
- Furthermore, the responsibilities of all shareholders with respect to the RAF must be documented in accordance with the organizational structure of the bank.

Supervisory expectations

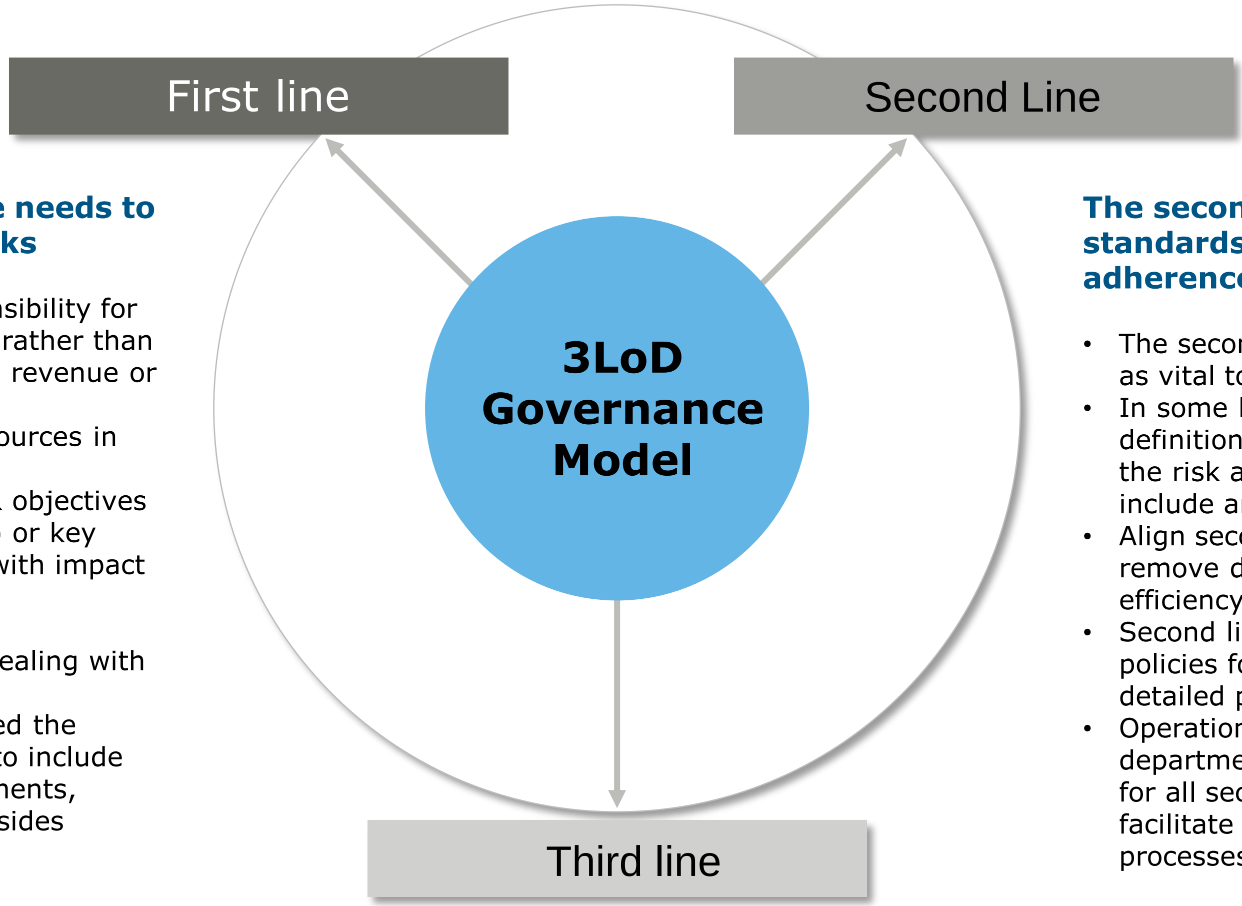
European regulatory bodies, including the Single Supervisory Mechanism (SSM) published in June 2016 clear guidelines and expectations for developing and establishing a comprehensive RAF:

- Institutions need to define quantitative or qualitative metrics and statements with a current and forward-looking view, in order to reflect all material financial and non-financial risks facing the organization
- Limits need to be introduced for each metric and cascaded down across all entities and business lines; additionally, they should be calibrated to reflect the amount of risk the institution is willing to take
- The RAF should help promote an adequate risk culture and conduct and ensure that risk appetite is fully taken into account during regular reviews or changes to the bank's business model or strategy

NFR Governance Framework

3LoD Responsibilities

Overall roles and responsibilities regarding NFRs are less clear than for financial risks



The first line of defense needs to own and manage its risks

- Ownership and the responsibility for risk and risk assessment, rather than focusing entirely on sales, revenue or cost management
- Strengthening control resources in the first line
- Introducing front-line NFR objectives -key risk indicators (KRIs) or key control indicators (KCIs) with impact on compensation
- Map end-to-end process accountability to help in dealing with NFR.
- Some banks have extended the definition of the first line to include IT and operations departments, where most of the NFR resides

The second line sets control standards and monitors adherence to them

- The second line areas should be seen as vital to the bank's business model
- In some banks have extended their definition of the second line beyond the risk and compliance functions to include areas such as legal and HR
- Align second-line responsibilities to remove duplication and increase efficiency
- Second lines need to define clear policies for each risk type and more detailed procedures and guidelines
- Operational risk management department is usually a coordinator for all second-line functions and facilitate various enterprise-wide processes (e.g. RCSA)

The third line of defense is internal audit

- checks on the adequacy of the first two lines

NFR Governance Framework

Board Responsibilities and Engagement

We see Boards increasing their engagement in various ways, by having dedicated NFR board meetings or by creating a committee dedicated to NFR

Board-level information on NFR needs to strengthen

The quality of the board meetings debates will crucially depend on the input information from all lines of defense regarding NFR on:

- Quantitative and qualitative risk indicators monitored and potential breaches in tolerance levels
- Major incidents and near misses, and their impact in terms of financial, capital and reputational implications
- The results of risk and control self-assessments
- Internal and external audit repots on NFR

Board engagement with NFR Appetite

Boards should particularly be engaged in the development of the NFR appetite, to help them effectively steer the institution in the right direction:

- Boards should demand that the risk appetite be better embedded and operationalized. Such operationalization requires that risk-appetite statements link with meaningful KRIs.
- Realistic limits and thresholds for incidents and losses needs to be established.
- Boards should also ensure that the risk appetite statements are cascaded down to divisions/functions

Supervisory pressure on boards

- New EBA guidelines on internal governance comes to underline more the roles and responsibilities of the board and committees
- And there are also the personal consequences for senior managers, individual accountability, for misconduct or failure to comply with laws and regulations.
- Collective suitability guidelines issued by EBA, encourages continuous improvement and enhancement of skills so we might see increased training on NFR.

Risk Culture

Regulators pay specific attention to risk culture

Regulators are increasingly demanding institutions to highlight the role culture plays in the effectiveness of its risk management and control environment.

While regulators do not prescribe a firm's culture, they expect boards to take responsibility and leadership for establishing and overseeing a sound risk culture.

Any indication of poor culture can lead to a more intrusive supervisory scrutiny and increase the regulatory pressure.

"a firm's culture can defeat its formal governance"
- Financial Stability Board (FSB)

"institutions should develop and maintain a positive attitude towards risk control and compliance within the institution…"
- European Banking Authority's (EBA)

What are supervisors looking for?

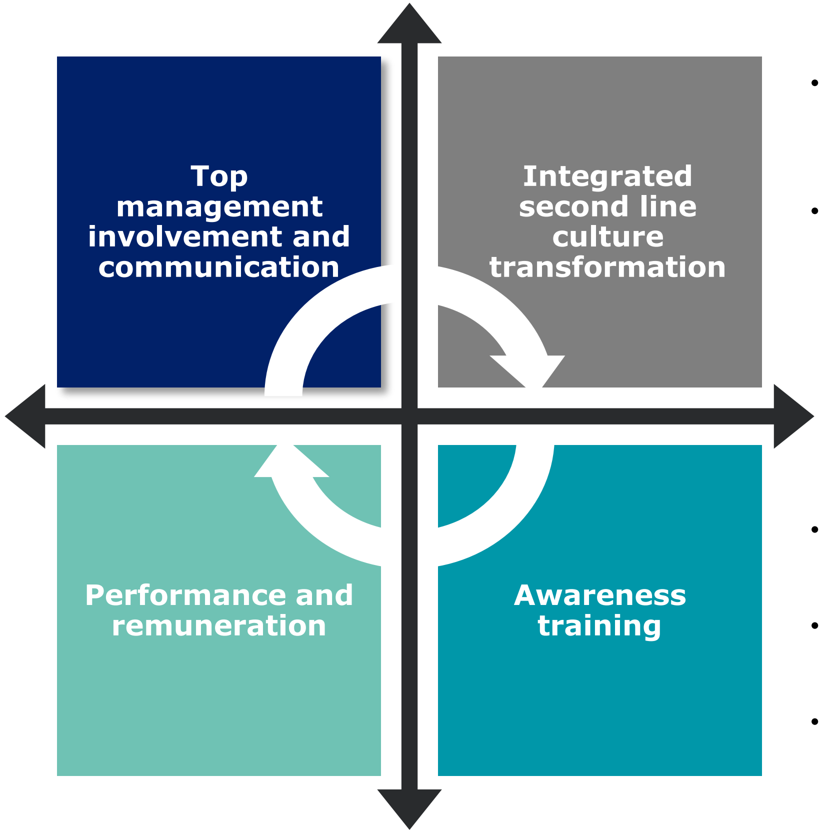
- An **internal governance framework** with a clear organisational structure and well defined lines of defense
- An enterprise-wide **risk management and control framework** and processes to support it
- A comprehensive **risk appetite framework** that includes all material risks, including non-financial risks, with well defined limits and KRIs
- Evidence that the board has satisfied itself that **internal governance and control arrangements are effective**
- **Internal audit** includes cultural issues in its engagements and is conducting culture-specific reviews
- Evidence **the heads of internal control functions** have **full and direct access to the board** and report regularly to the board
- Evidence or high quality MI to demonstrate that **policies and controls are not regularly breached or over-ridden** by undesirable behaviours and root cause analysis is performed, to identify potential systems and control enhancements.

Risk Culture

However strong the risk framework might be, NFR management will fail unless it is supported by a culture that acknowledges its importance

To achieve this kind of cultural shift, banks need to focus particularly on the following key areas

- This is a key driver of risk culture transformation.
- Senior-management involvement and role modeling will be especially important
- in organizations where senior managers champion NFR management, a strong risk culture emerges.



- The various functions need to integrate their culture-transformation efforts, as standalone efforts in individual functions do not work.
- Collaboration is needed to integrate parallel risk-assessment and culture frameworks across operational risk, compliance, and other NFR functions

- Incentives must become clearer, and breaches in conduct rules must lead to immediate and real consequences.
- Getting this right is critical in aligning business practices with risk appetite and in improving the effectiveness of controls and remediation.
- The second-line functions need to go from pushing out policies to building motivation to support real behavior change around the most critical risks.

- NFR identification and mitigation needs to become routine in every first-line organization.
- banks must introduced NFR training, especially for operational risk, into their working culture
- Educate company–wide personnel and encourage a new set of behaviors to help protect de bank against NFRs and to highlight gaps and weaknesses

Culture drives conduct

Establish a formal conduct and culture program, to formalize the importance of a risk-aware culture and encourage ethical behavior by employees

Culture

Norms

Habitual behaviors and mindsets in the absence of regulations or compliance rules

"It's the way things get done around here"

Risk Culture

Risk Taking

Attitudes, decisions and behaviors relating to how **risk is understood and managed**

"It's what I do when nobody is watching"

Conduct Risk

Outcomes

Business practices that can adversely affect customers, the organization, other employees and the marketplace

"It's the impact of my actions"

Thank you!

"**Risk appetite frameworks** should cover a wide range of risks, both financial and non-financial. Banks must integrate them closely into the entire organisation.

They must link them to the overall **strategy**; they must extend them to all levels of the organisation; and they must align them with **remuneration policies**. Without this, risk appetite frameworks will remain mere blueprints that have no impact on actual risk-taking."

Danièle Nouy, Chair of the Supervisory Board of the ECB,

Speech extract from the banking supervision conference, "Governance expectations for banks in a changing financial environment",Frankfurt, 22 March 2018