McKinsey & Company

Strategic Perspective on Non-financial Risk Management

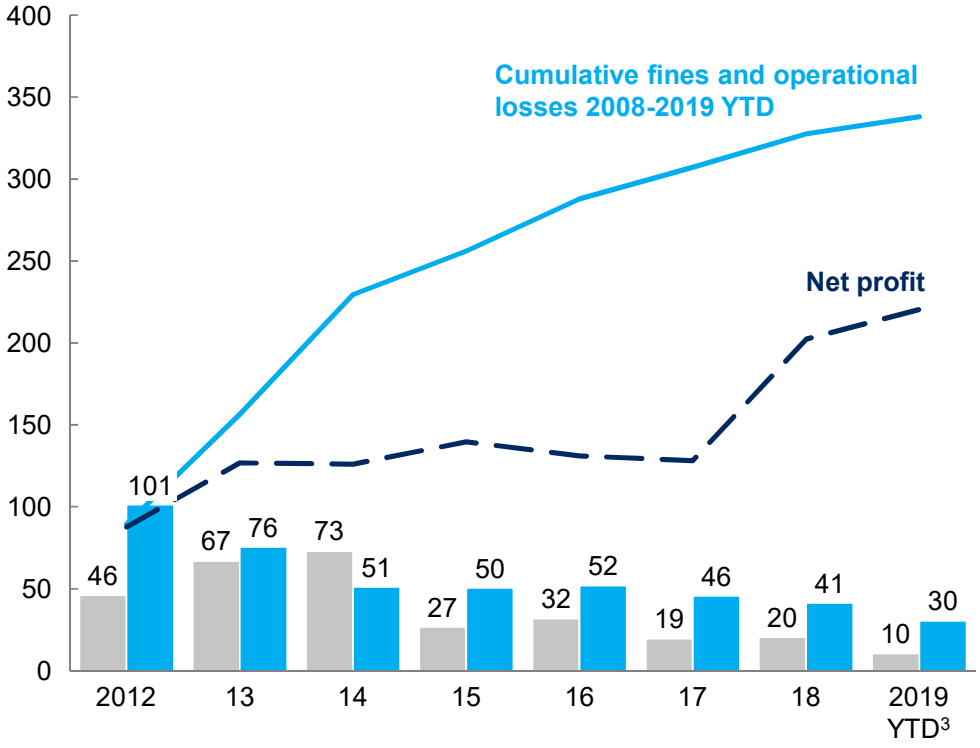
CFS FIRM CONFERENCE NON-FINANCIAL RISK
FRANKFURT, MAR 12, 2020

NFR dominate the risk profile of many larger banks - NFR currently incur approx. USD ~10-20bn to global US and European banks

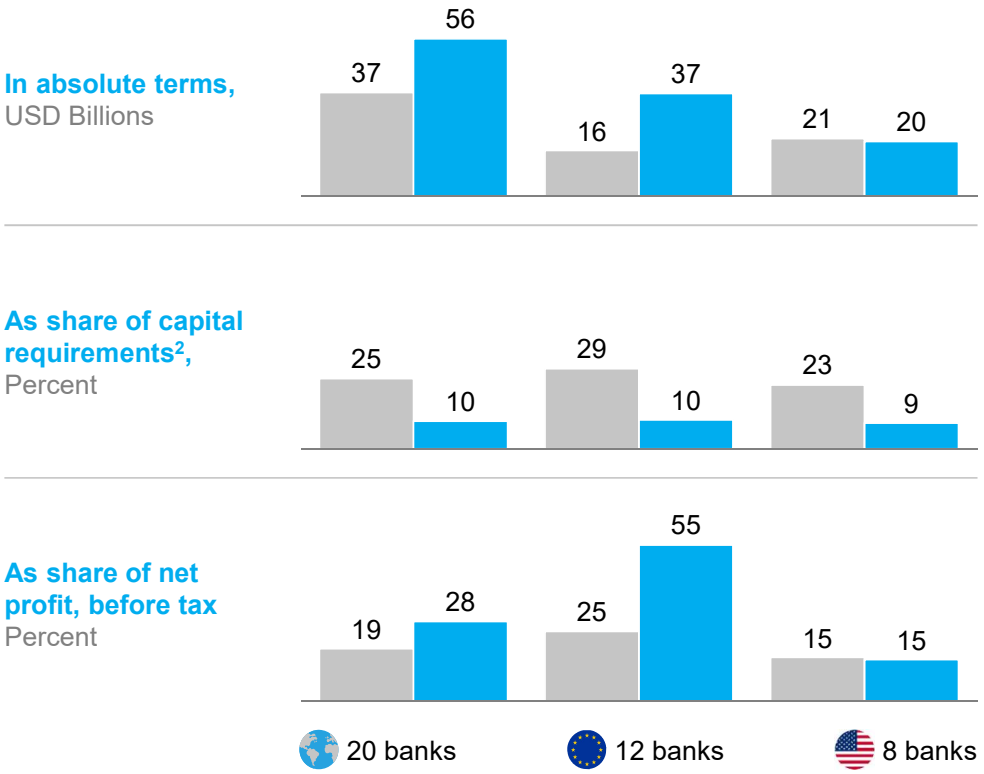
Compliance and oprisk losses[1] | Credit risk provisions/impairments

Operational and compliance vs. credit losses largest US and EU banks[1]

USD Billions, 2012-2019 YTD



Averages



1 More broadly operational risk losses, fines and litigation gathered from press and public sources
2 Minimum capital requirements defined as 8% of respective risk weighted assets for operational and credit risk and credit risk weighted assets
3 Beginning of November 2019; Net profit LTM including Q3 2019; Credit impairments as of YTD Q3 2019; Net profit LTM Q3 2019

SOURCE: S&P Market Intelligence; Company reporting

NFR management is a question of quality management of a bank‘s processes/business model

Examples major NFR risk events 2012-2019	Underlying process control failures
PPI UK mortgages (USD ~44bn)	**Misselling**/insufficient advisory and marketing practices supported by misaligned incentives to act against customer interests
US/Australian private customers fees-for-no-services (Australian banks costs for bad behaviour USD ~3.8bn up to USD ~7.4bn)[1]	
IT-outages/data issues UK retail businesses (USD >1.1bn from 2012 to 2019)	**IT failures** - maintenance/upgrading as well as general infrastucture problems
Sanctions violations in int./trade finance businesses (USD >14.7bn from 2008 to 2019)	**Insufficient KYC and transaction monitoring processes**
AML violations (USD 8.2bn in 2019)	
Tax avoidance schemes (USD >8.9 bn fines from 2008 to 2019)	**Insufficient consideration of tax requirements** and control over business practices; misaligned incentives
FX/Libor/benchmark rigging (USD ~7.7bn)	**Insufficient wholesale conduct controls** (market integrity/ wholesale control requirements); **misaligned incentives**

1 Australian banks' cost of bad behavior according to Shaw and Partners' bank analyst Brett Le Mesurier

CROs with increasing responsibility for Compliance risks in Europe (similarly in the US and APAC)

Direct reporting line to CEO | Direct reporting line to CRO | Other ExCo members

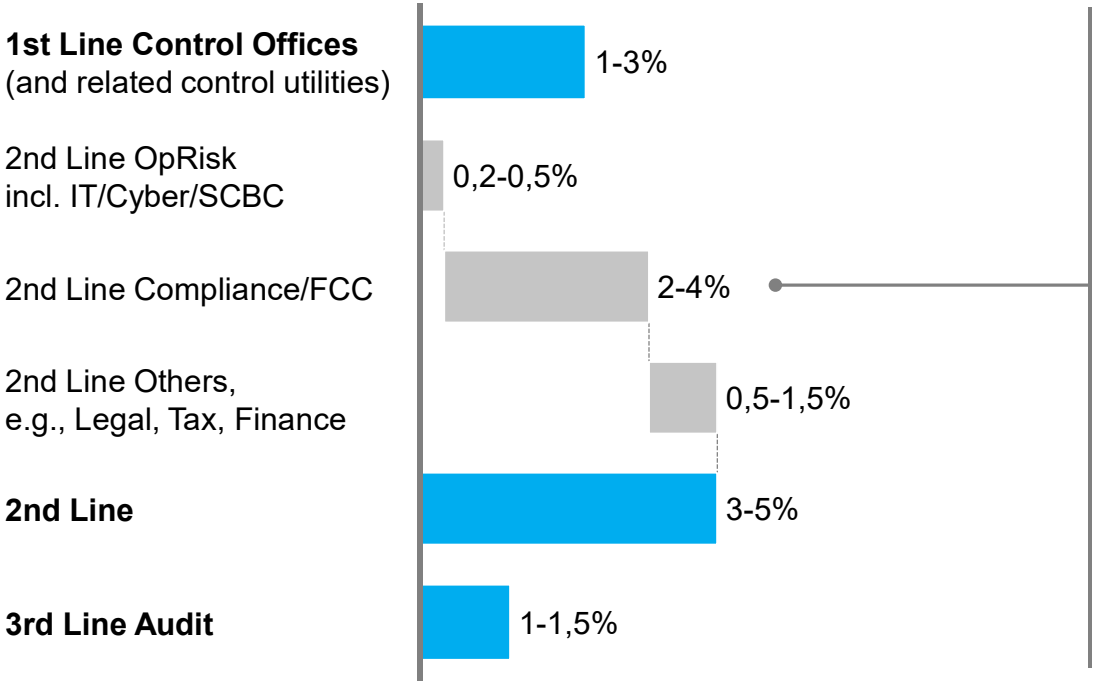
Bank	OpRisk	Compliance (Reg/FCC)	Legal	IT/Cyber Risk
ABN Amro	CRO	CRO	CRO	*Rarely disclosed, most commonly split between CRO (Line 2) and COO/CTO with separate IT-Risk/CISO teams (Line "1b")*
RBS	CRO	CRO	General Counsel	
Lloyds	CRO	CRO	General Counsel	
Santander	CRO	CRO	General Counsel	
ING	CRO	CRO	General Counsel	
Nordea	CRO	CRO	CLO[1]	
Swedbank	CRO	CEO	CEO	
SEB	CRO	CEO	CEO	
Danske Bank	CRO	CCO	CEO	
UniCredit	CRO	CCO[2]	CLO[1]	
Credit Suisse	CRO	CCO	General Counsel	
Barclays	CRO	CRO	General Counsel	
Deutsche Bank	CRO	CRO	CAO[3]	
Standard Chartered	CRO	CRO	General Counsel	
Commerzbank	CRO	Compliance, Legal, HR		
UBS	CRO	CCO / Reg Affiars	General Counsel / CAO	
HSBC	CRO	CRO / CEO (FCC)	CLO[1]	

1 Chief Legal Officer 2 Currently in transition to be united under one ExCo member 3 Chief Administrative Officer

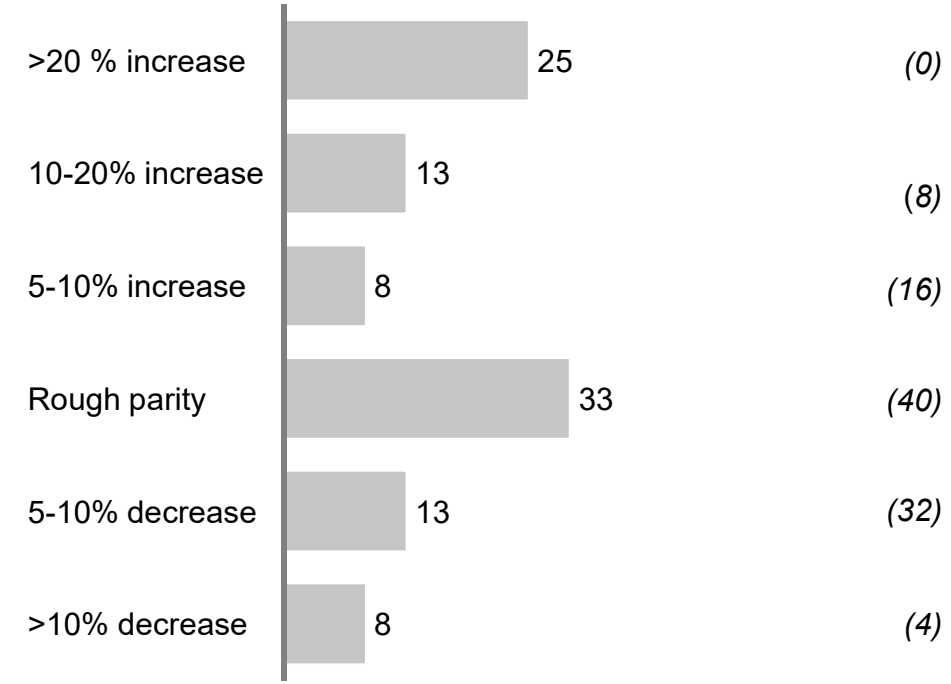
SOURCE: Corporate publications; Websites

Size of NFR functions has grown substantially for international banks – particularly for 2nd line compliance and financial crime, totalling 5-10% of FTE capacity

Indication for global banks on 1st line, 2nd line, 3rd line NFR teams, as % of total bank FTE



Past change to compliance costs over previous two years – 2016/17 (2018e in brackets), % of respondents



SOURCE: McKinsey Compliance 360 Benchmarking Survey 2018

The approach to NFR has evolved across several stages for global banks, in particular regarding the role of central OpRisk teams, but also the applied means and key objectives

Current stage of most banks

Traditional setup	**OpRisk as an additional capital measure to provide a cushion; with an unrelated approach to Compliance/Financial Crime**
Integrated 2nd Line NFR Mgt	**Focus on governance and group-wide standards; first dedicated 1LoD organisations emerging as well as integrated NFR approaches**
Risk type specialization	**NFR management pushed into specialized risk areas (both 1st/2nd line) with central OpRisk team providing a (lean) umbrella function**
1st Line led quality / cost Mgt	**Significant enhancements of the NFR operating model – processes, systems, data to manage process/IT quality and costs more broadly**

There have been significant advancements in moving from operational to an integrated non-financial risk management approach

- **Formalization of 3LoD governance models**
- Broadening of CRO mandate
- Enhanced NFR committee structures
- Group-wide NFR taxonomies
- Strengthening of policy framework

- OpRisk as single framework owner (often / not always)
- **Investment into core risk processes**, **e.g., issue management, assurance, RCSA, reporting**
- Specific tools for OpRisk, Compliance
- Extended analytical / tool capabilities

- I**nvestments into core control processes, mostly remediation** focused
  - Conduct risk / regulatory compliance
  - Financial Crime
  - IT, Cyber risk, data protection
  - Others (model risks, change risks, …)

- Codes of conduct
- (Online) trainings
- Risk culture measurability, reporting
- Adjustments to incentive systems, sanctions framework

70% of CROs feel they had *good transparency* on operational risks[1]

1 McKinsey/ORX study, The Future of Operational Risk

However, there are still significant challenges to be addressed to ensure impact in managing a bank's NFR profile

- **Formal vs. effective governance**
  - **2nd line** as control vs. **advisory function**
  - **1st line accountability** and setup – **role and capabilities of Control Offices**
  - **Insufficient different-iation** by risk types
  - **Poliferation of policies**

- **Cost/benefit or impact of risk processes, e.g. top-down driven risk appetite vs. Bottom-up RCSA**
- **Forward looking/impact driven, in-business views Identification / reporting**
- **Integrated NFR operating model,** ie of risk processes and standards across 2nd lines – **"single platform"**

- **1st line embedding – moving from control to quality management**
  - **Complexity reduction: processes/IT**
  - **Business transforma-tion – digitization/data**
- **Industrialization of controls**
  - **Front-to-back/utilities/…**
  - **Automation/AI/…**

- **Effective instruments to enhance culture**
  - **Senior management involvement** (tone from the top, sanction mechanisms, incentives)
  - **Effective interventions** to drive cultural change beyond communication and trainings

Only 30% of CROs feel to have an *effective management* approach[1]

1 McKinsey/ORX study, The Future of Operational Risk

Industry and regulators need to further align on effective industry standards

Current topics identified by the Working Group of German Banks on Non-financial Risk Management	Additional topics as discussed in international industry fora (US/UK)
Organisation and Governance incl. accountabilities and resourcing	**Integration of NFR frameworks** regulatory/FC compliance and IT/cyber/data risks
Risk assessment approaches and consolidation	**Cross-risk categories:** reputational, supplier, change risks, conduct
Risk appetite and tolerance for non-financial risks	**Control management:** governance, management approaches and integration into NFR frameworks
Risk culture to prevent non-financial risks	**NFR standards:** risk/control taxonomies, risk assessment standards
Learnings from other industries on non-financial risk management	**Levers from automation, AI** to enhance NFR approaches