



Banking Operational Risk & Internal Control Framework

**A comparative peer analysis and
insights into the latest industry trends**

[kpmg.fr](https://www.kpmg.fr)

June 2021



Banking Operational Risk & Internal Control Framework

Summary

Executive Summary	7
Glossary	11
1. Performance Trends in the banking sector	12
2. Regulatory Requirements related to Internal Control & Operational Risk Management	26
3. Internal Control Framework & Operational Risk Management Benchmark	30
4. The main drivers of action	50
5. How KPMG can assist you	54
6. Benchmark methodology	58
7. KPMG Team & Contacts	62

Purpose

On 7th December 2017, the Basel Committee approved revised methods for calculating operational risk capital requirements, replacing existing approaches with a new and unique standard approach. This approach – known as the Revised Standardized Approach – will come into effect in January 2023, thereby replacing the current three calculation approaches – Basic (BIA), Standard (TSA), and Advanced (AMA).

The new Revised Standardized Approach could lead to a potential increase in capital for a number of banking institutions. Consequently, a robust and efficient internal control framework (ICF) will be even more essential to limit operational losses and thus, reduce the amount of risk weighted asset (RWA), and therefore the amount of capital required.

In this context, KPMG France led a benchmark of initiatives and practices related to the internal control framework and operational risks management. The following topics were addressed:

- Governance & Organization
- Risks & Controls Framework
- Operational Risk Management
- Deployed Tools
- Regulatory Challenges

This benchmark presents the responses we received from 12 panel banks in Europe and the United States, as well as best practices we have observed in strengthening the internal control framework in conformance with regulatory expectations and to help banks better manage operational risk.

Vicky Papaevangelou

Partner
Consulting Bank
KPMG France

**Nicolas Coudrieau**

Senior Manager
Consulting Bank
KPMG France

**Carine Demonio**

Senior Manager
Consulting Bank
KPMG France





Executive summary



Performance trends in the banking sector in 2019

KPMG performed an analysis of European banks based on publicly available information in regard to their balance sheet, net banking income, and capital reserves in 2019.

KPMG also compared the panel of these banks with each other by studying two criteria:

- the RWA OR / RWA ratio, which measures the contribution of operational risk in the RWA of each bank;
- the EBT/ RWA OR ratio, which measures the level of risk taken by a bank to generate a certain level of income.

The analysis revealed four major concentrations in terms of operational risk capital allocation: banks with a low operational risk profile, banks with a medium risk profile driven by a high level of operational risk, banks with a medium risk profile driven by a low level of income, and banks with a high risk profile.

With the revised standardized approach, it will be essential for banks to go further in managing their operational risk, whether by indirectly reducing the amount of RWA if losses are taken into account or demonstrating to supervisors that their current capital level is sufficient to face potential losses.

Governance & organization

- In the majority of banks, there is one single department managing both operational risk and internal control.
- In most banks, LOD1 is responsible for executing controls and rating risk anomalies. Some banks have dedicated staff for LOD1, which allows LOD2 to play more of a supervisory role.
- For optimization and efficiency purposes, in some banks, a part of LOD2 staff joined LOD1 within the Business and Services Units.
- In some banks LOD2 certify the LOD1 control results, notably discrepancies and action plans.
- Heterogeneous LOD2 organizations : in our panel, there were between one and five LOD2 organizations, which include Finance, Risk, Compliance, Legal or Tax.
- The Internal Control Framework (ICF) is generally monitored by LOD2 but owners are operational BU/SU departments – LOD1 is in charge of updating the ICF.
- Control Testing Utility Units have been implemented, which are independent and accompany LOD1 & LOD2.
- 33% of banks have incorporated data and analytics within LOD2 and LOD3.

Risk management

- Two taxonomy types are implemented :
 - A Risk Taxonomy set up according to the Basel regulatory framework. It is deployed to include a broader RCSA and includes IT and Compliance Risks within the operational risk taxonomy;
 - Different levels on the taxonomy linked together : Level 1 based on Basel requirements, Level 2 by topic, and Level 3 detailed according to BU/SU needs.
- Almost all banks have a unique RCSA exercise, including IT risks & Compliance.

GRC approach

Most banks :

- Implemented an integrated Internal Control "ICF" Framework linking the Processes to related Risks and mitigating Controls;
- Have mapped their Business and Services' Activities to Processes;
- Adopted a top down approach mainly.

Tools & other topics

- 1 bank has a holistic ICF tool, and gave access to the ECB - this includes processes, risks, control. environment (both LOD1 and LOD2 controls), control anomalies, action plans, internal losses and incidents (including IT incidents), RCSA, quality insurance indicators, KRI, etc.
- In general, most banks have adopted an integrated tool. Some of them are still using several tools per topic (action plans, risk events, reporting tool, etc.).
- The tools are developed mainly in-house, or on SAP or Open Pages.
- Enablon, Archer and Metrix Stream are other common ERM tools deployed.

Challenges

The main challenges for banks is to implement an holistic approach in terms of Internal Framework and operational risk management linked to organization, people, IT tool, and reporting.

Glossary

Word/Abbreviation	Definition/Signification
AMA	Advanced Measurement Approach for RWA calculation
BIA	Basic Indicator Approach for RWA calculation
TSA	Standard Approach for RWA calculation
CET1	Common Equity Tier 1
CRR	Capital Requirements Regulation
ECB	European Central Bank
EU	European Union
GRC	Governance, Risk and Control
ICF	Internal Control Framework
ILM	Internal Loss Multiplier
LOD1	First Line Of Defense
LOD2	Second Line Of Defense
LOD3	Third Line Of Defense
L1C	Level 1 Control
L2C	Level 2 Control
NFR	Non Financial Risk
OR	Operational Risk
RCSA	Risk and Control Self Assessment
RWA	Risk-Weighted Assets

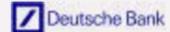
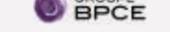
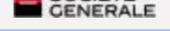
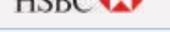
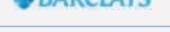
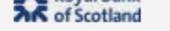
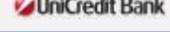
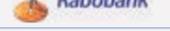
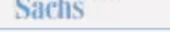
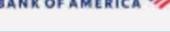


Performance trends in the Banking sector

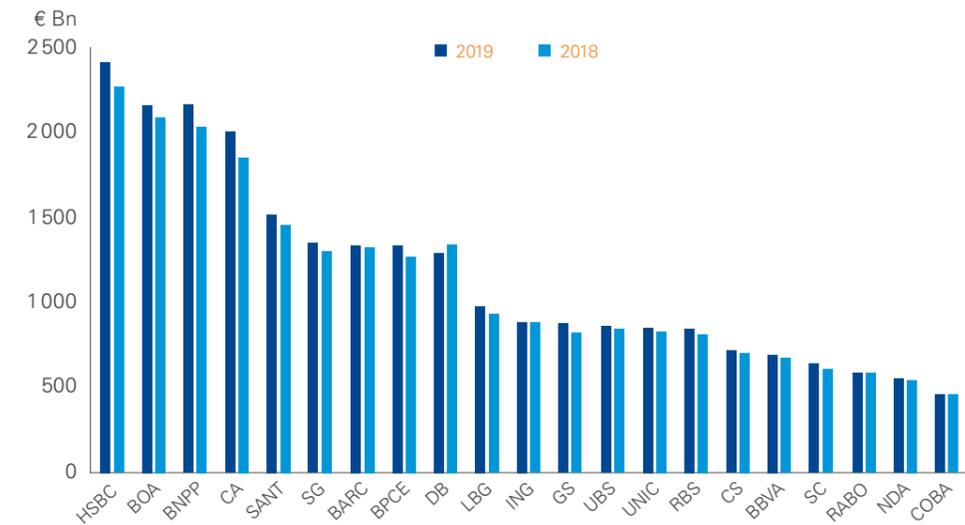
- Banking performance trends..... 14
- Different operational risk profiles17
- Current calculation approaches to assess capital requirements for operational risk 19
- New calculation approach to assess capital requirements for operational risk 21
- Expected impacts of the new approach to assess capital requirements for operational risk 23

Banking performance trends

List of analyzed European banks with publicly available information in regard to their balance sheet, net banking income, and capital reserves (based on 2019 annual reports).

Institution	Name	Country
 Deutsche Bank	Deutsche Bank (DB)	
 Commerzbank	Commerzbank (COBA)	
 Santander	Santander (SANT)	
 BBVA	Banco Bilbao Vizcaya Argentaria (BBVA)	
 BNP PARIBAS	BNP Paribas (BNPP)	
 GROUPE BPCE	BPCE Group (BPCE)	
 CRÉDIT AGRICOLE	Credit Agricole Group (CA)	
 SOCIÉTÉ GÉNÉRALE	Société Générale (SG)	
 HSBC	HSBC (HSBC)	
 BARCLAYS	Barclays Group (BARC)	
 Standard Chartered	Standard Chartered (SC)	
 Royal Bank of Scotland	The Royal Bank of Scotland (RBS)	
 LLOYDS BANK	Lloyds Banking Group (LBG)	
 UniCredit Bank	UniCredit Group (UNIC)	
 UBS	UBS (UBS)	
 CREDIT SUISSE	Credit Suisse Group (CS)	
 Rabobank	Rabobank (RABO)	
 ING BANK	ING Group (ING)	
 Nordea	Nordea Group (NDA)	
 Goldman Sachs	Goldman Sachs (GS)	
 BANK OF AMERICA	Bank of America (BOA)	

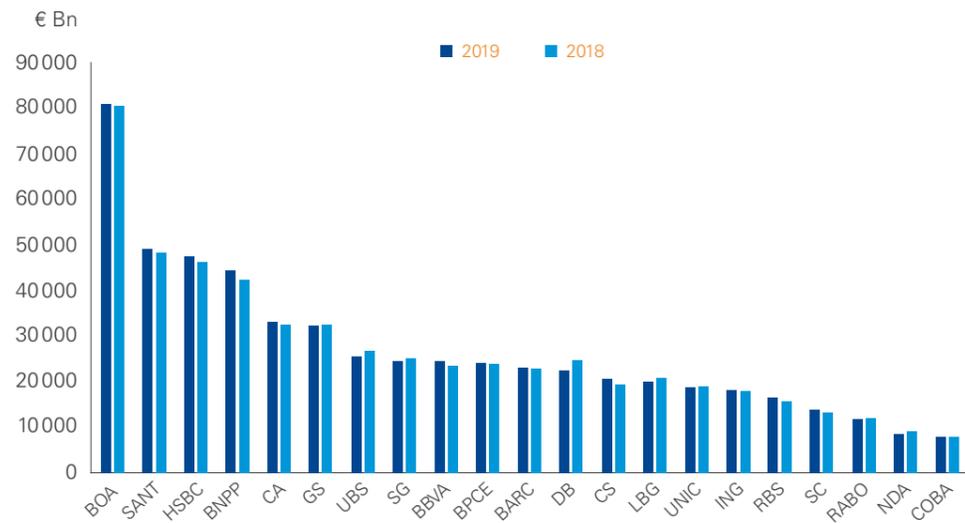
Evolution of balance sheet size between 2018 and 2019 in billions of euros



Source: publicly available 2019 annual reports

2019 saw a slight increase of 3.6% in the size of the balance sheet for almost all studied banks, explained by an increase in cash reserves and volume of credit granted.

Evolution of net banking income between 2018 and 2019 in thousands of euros

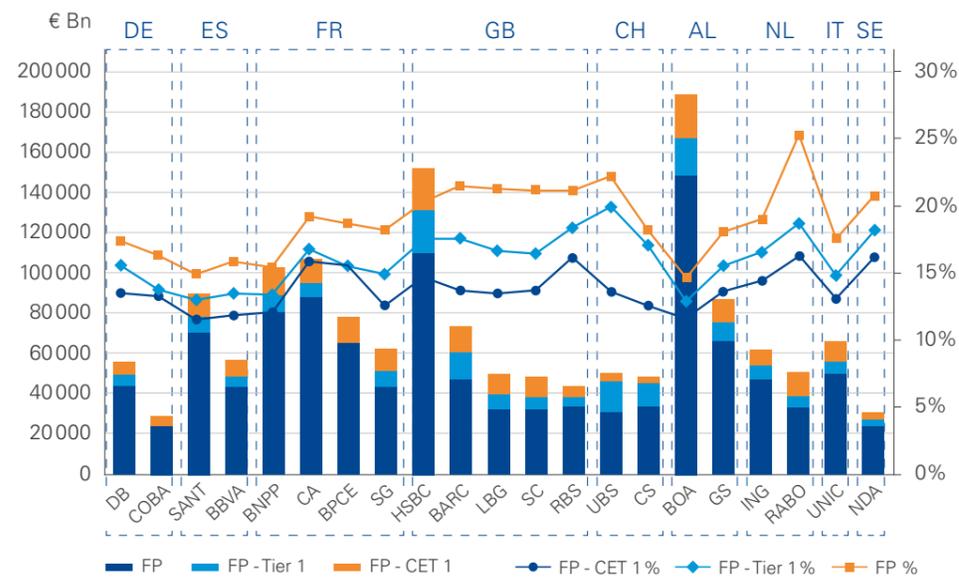


Source: publicly available 2019 annual reports

In 2019, Net Banking Income (NBI) remained stable with a slight increase of 0.6%. However, there was a slight decrease in NBI for Deutsche Bank, Nordea, Lloyds Bank, UBS, and Société Générale.

Credit institutions notably resisted the low interest rate environment and early repayments as part of the ECB's accommodative policy.

Capital structure and regulatory ratios in 2019



Source: publicly available 2019 annual reports

In 2019, European banks maintained their level of capital reserves above regulatory requirements (CET1: 4.5%, Tier 1: 6%, solvency ratio: 8%).

Within the European banking industry, UK banks on average were among the best capitalized due to more stringent regulatory requirements.



Different operational risk profiles emerge

Cross-mapping EBT/OR RWA and OR RWA/RWA in 2019 (annual reports source)

KPMG compared the panel of banks with each other by studying two criteria:

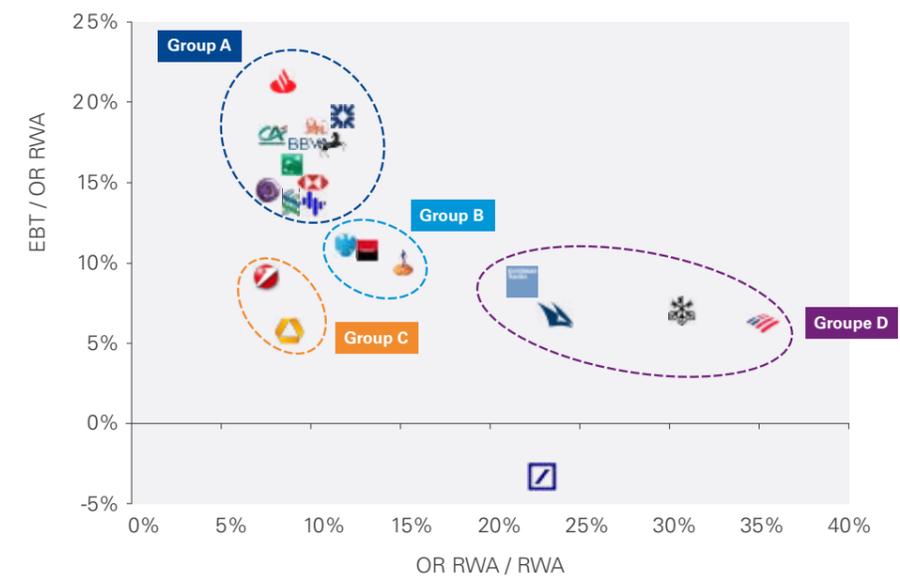
- the **RWA OR / RWA ratio**, which measures the contribution of operational risk in the RWA of each bank,
- the **EBT / RWA OR ratio**, which measures the level of risk taken by a bank to generate a certain level of income.

Group A comprises banks with a relatively low operational risk profile with a higher level of income in comparison to their risk level (above average) and the share of the operational risk in the RWA is lower.

Group B comprises banks with a medium risk profile driven by a higher share of operating risk. For certain banks, this is explained by their higher level of corporate and investment services activities than other banks, which requires more risk control measures.

Group C comprises banks with a medium risk profile derived from a low level of income. This is explained in particular by an excessively high cost of risk due to credit risk.

Group D comprises banks with a high risk profile, which can be further explained in particular by their business model, mainly focused on private banking and asset management activities.



Source: publicly available 2019 annual reports



INSIGHTS

Group analysis:

- **Group A:** low operational risk profile
- **Group B:** medium operational risk profile, driven by a higher level of operational risk (due to wholesale activities)
- **Group C:** medium operational risk profile, driven by a low level of income
- **Group D:** relatively high operational risk profile due to its business activities



CONTRIBUTING FACTORS

Business lines with the strongest contribution:

- Retail and commercial banking activity: in particular for NDA, LLYO, BCPE and CA
- Investment banking and corporate banking: in particular for DBK, CBK, SG, HSBC, BARC or GS
- Asset management: for UBS and CS

N.B. The RWA includes credit, market, and operational risks. Within the panel, on average, credit risk accounts for 70-80% of the total RWA, operational risk for 10-20% and market risk for less than 10%.

Please note that the comparison of institutions is limited due to differences in the calculation methods used by each bank.

Current calculation approaches used to assess capital requirements for operational risk

Three calculation approaches with an increasing level of complexity and risk sensitivity*

The first approach, the Basic Indicator Approach (BIA), is calculated by multiplying the income indicator (i.e. service commissions, revenue, interest and similar income, etc) with a coefficient of 15%, the value of which was set by the Basel Committee in 2001, having determined that the operational losses represented, on average, 15% of the income of banks.

Next, the Standard Approach (TSA) uses the same income indicator multiplied by a beta coefficient which varies according to the type of activity (e.g. retail activity is 12%, negotiation and sale is 18%). To use this approach the bank must notify the regulator and justify that it maintains a risk evaluation and management system.

Finally, the Advanced Methodology Approach (AMA) is the subject of debate today. It is based on backward-looking data, which includes internal and external loss data and an external and internal environment factor (e.g. control results), as well as forward-looking data, which incorporates scenario analysis and feeds into model statistics leading to an assessment of the RWA for each entity. This method allows for significant flexibility because each business line may decide on the "severity" and "frequency" of parameters that feed into the scenarios, which indirectly makes it possible to optimize capital requirements.

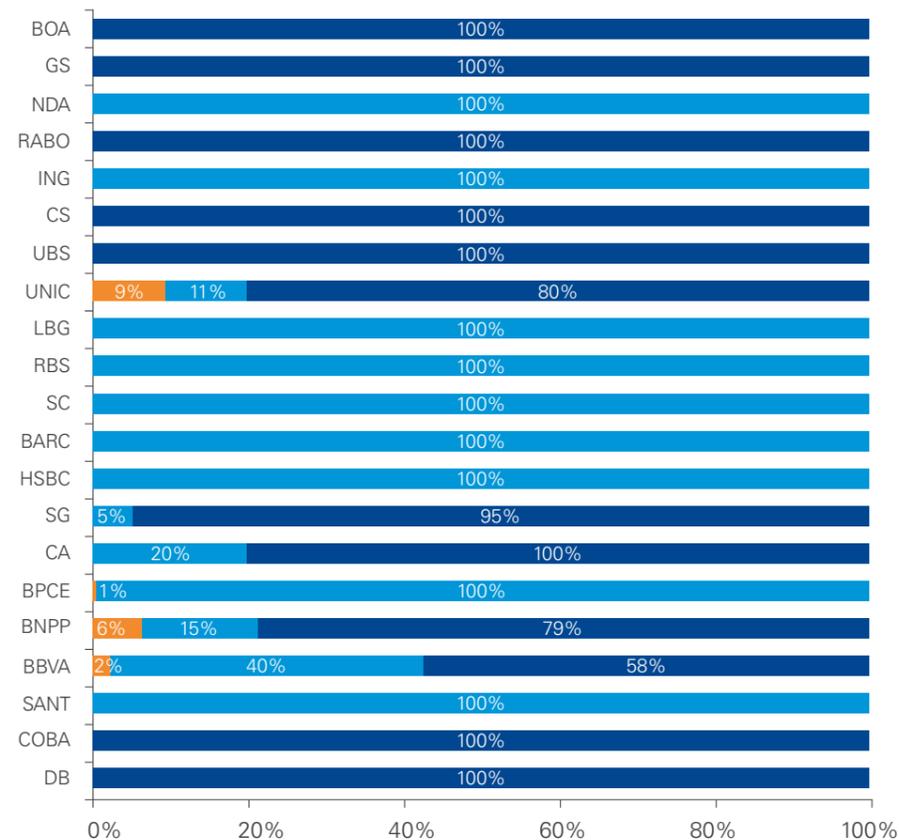
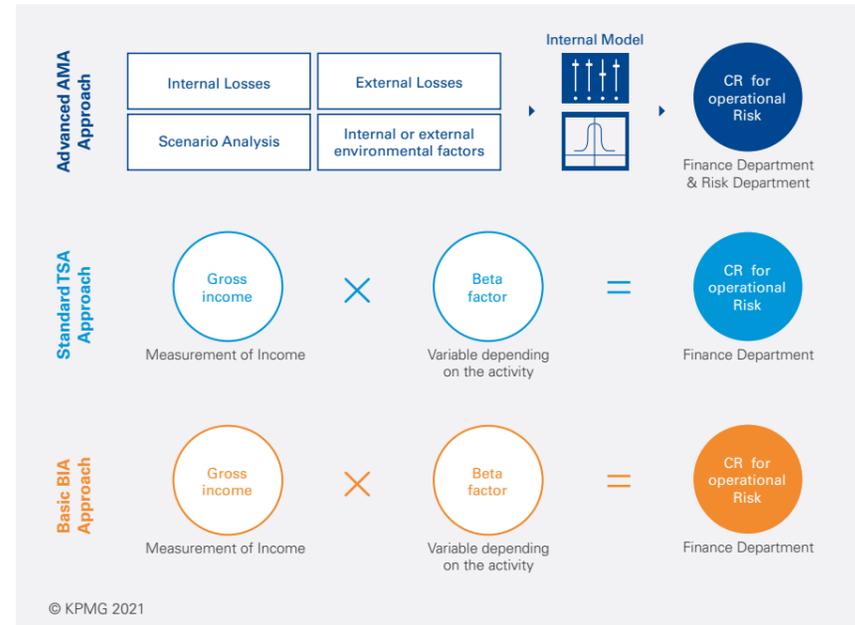
To use the Advanced Methodology Approach (AMA), the bank must apply for authorization from its local regulator (in France, the ACPR) and justify its quantitative criteria – including at minimum the history of its losses in the past 5 years – and qualitative criteria, in particular:

- Existence of an independent function dedicated to operational risk
- Periodic inspection of the independent function dedicated to operational risk
- Existence of procedures for data validation, data flows, regular reporting of risk exposure or losses to management
- Involvement between the risk department (calculation of RWA exposure) and the finance department (allocation of the RWA exposure)

*CRR Rgl UE n°575-2013 Prudential Requirements



Overview of current approaches and percentage of use within each bank in 2019 (annual reports source)



New calculation approach to assess capital requirements for operational risk

Overview of the Revised Standard Approach

The Basel III agreements, signed in December 2010, played a pivotal role following the financial crisis of 2007, leading banks to become more resistant to potential shocks by strengthening the level of their capital reserves. After addressing the solvency ratios, the Basel Committee sought to overhaul the method of calculating risk-weighted assets (RWA) to complete its reform efforts of the banking regulatory framework.

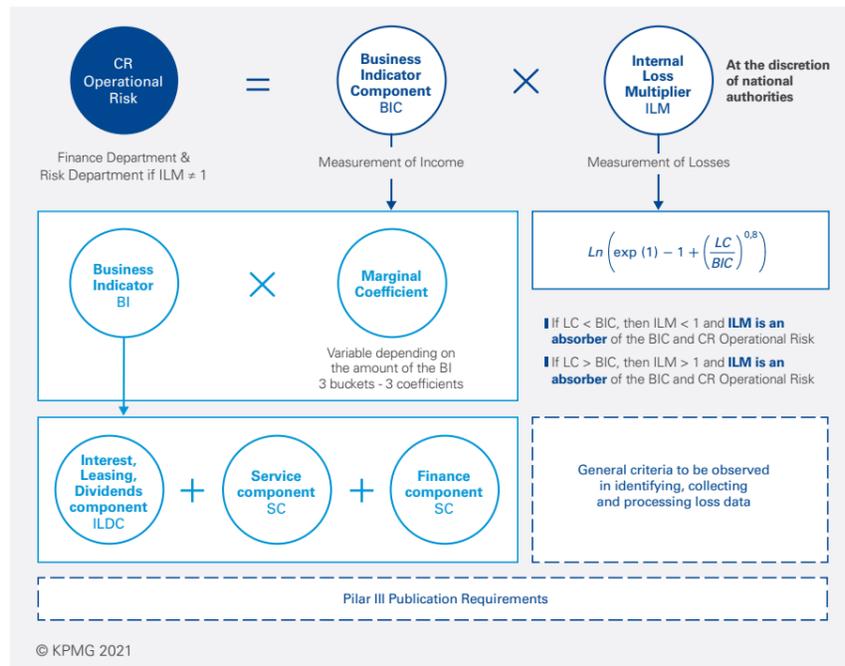
On 07 December 2017, the Basel Committee approved the revision of methods for calculating capital requirements for operational risk, replacing existing approaches with a new and unique standard approach, entering into force in January 2023.

The Operational Risk Component will contain a Business Indicator Component (calculated by a Business Indicator and Marginal Coefficient which will be separated into three buckets depending on banking income, ranging from 18% for net banking income above 30 billion euros to 12% for net banking income less than 1 billion euros) and an Internal Loss Multiplier.

The Internal Loss Multiplier (ILM) varies according to a loss component equal to 15 times the average annual losses linked to operational risk over an observation period of 10 Years, as well as according to the Business Indicator Component.

The status of incorporating the ILM is currently subject to ongoing discussion between the ECB and the national authorities.

Overview of the New Approach



GOALS OF NEW APPROACH

- Aim for simplicity
- Improve comparability between establishments
- Increase risk sensitivity

Dec. 2017

• Publication of Basel III finalization agreements

Jan. 2022

• Initial date of entry into force

Jan. 2023

• Revised date of entry into force due to COVID-19

Expected impacts of the new approach to assess capital requirements for operational risk

Expected Impacts

The new approach to assess capital requirements for operational risk will have direct operational impacts on the improvement of data quality, transformation of the prudential data production process, and adaptation of the regulatory reporting process.

At this stage, the ILM is not defined yet.

The EBA performed an impact analysis estimate, which shows an increase in capital (“Policy advice on the Basel III reforms: operational risk EBA-Op-2019-09b | 2 August 2019”).

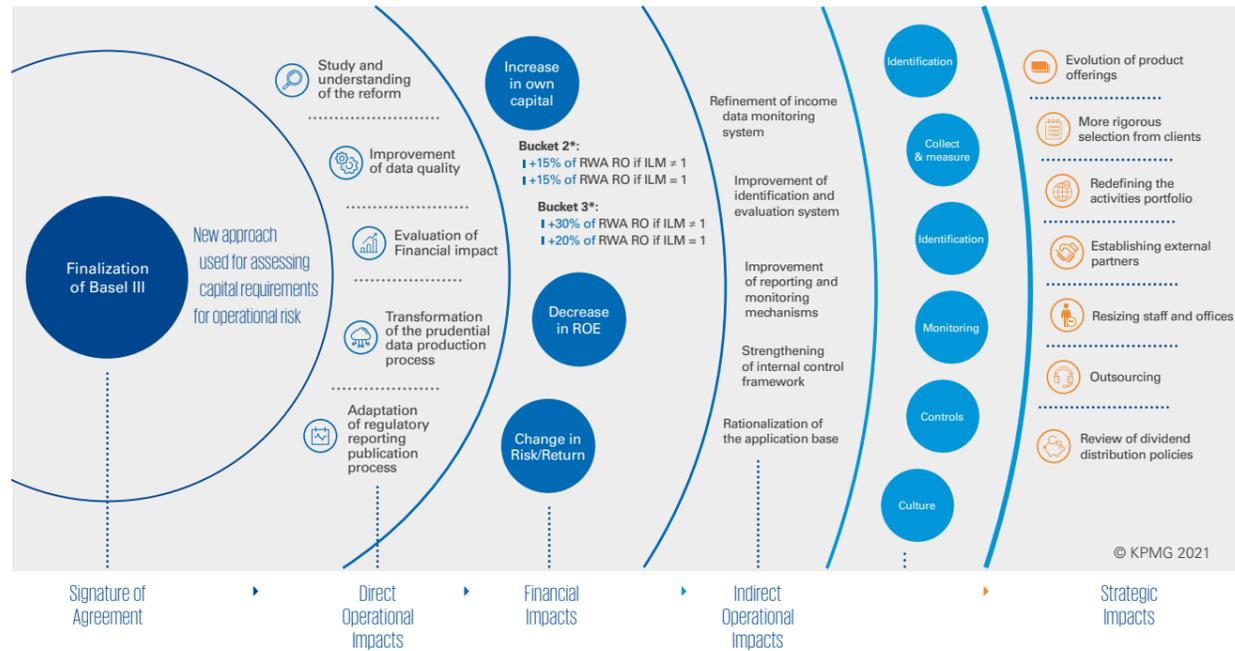
The EBA found that if the ILM is equal to 1, bucket 2 banks are estimated to increase their capital relating to operational risk RWA by 15 percent.

Likewise for bucket 3 banks, this may lead to a 20 to 30 percent increase in the RWA of operational risk.

Most banks of the panel confirmed this expected increase in capital requirements.

Consequently, this may result in a decrease in Return on Equity.

However, even though the ILM is equal to 1, a robust internal control framework will result in a better management of operational risks, thus less losses and improved compliance with regulatory requirements.



* The bucket depends on the size of the bank's business.
 Source : EBA-Op-2019-09b | 2 August 2019.

In the next section, we present our benchmark on the Internal Control Framework and operational risks management including best practices for a clear governance, rationalized risk management system, improved use of data & analytics, and reporting.



2



Regulatory
Requirements
related to
Internal Control &
Operational Risk
Management

Regulatory Requirements related to Internal Control & Operational Risk Management

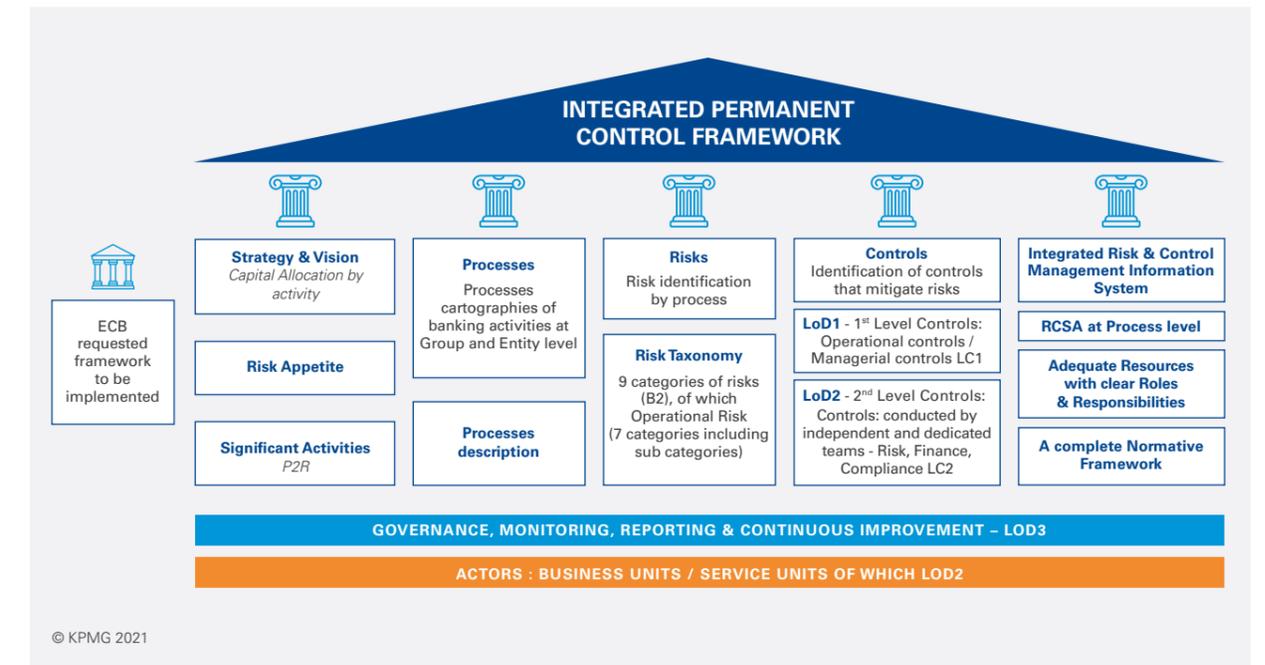
(EBA/GL/2017/11 – 21 March 2018)

The ECB requires banking institutions to put in place an integrated permanent control framework, which, as described below, includes:

- **Strategy and Risk Appetite related to activities;**
- **Description of processes corresponding to these activities, the related risks, and the key controls to mitigate these risks;**
- **The definition of roles and responsibilities at all levels of the hierarchy and in particular of LOD1, LOD2 and LOD3;**
- An integrated tool that allows for a RCSA at the process level and reports relating to the functioning of internal control and operational risk management.

This set-up must cover the Group and its entities with an established governance with clear roles and responsibilities, reporting from an integrated tool, monitoring, as well as continuous improvement plans.

This set-up is required for banks that calculate operational risk using the standard TSA approach and the advanced AMA approach and will be required for the Revised Standard Approach that will enter into force in January 2023.



3.



Internal Control Framework & Operational Risk Management Benchmark

- 1. Governance & Organization..... 34
- 2. GRC Approach 39
- 3. Risk Management – taxonomy and assessment..... 40
- 4. Tools 43
- 5. Regulatory & Challenges..... 44
- 6. Permanent Control Maturity Matrix 46
- 7. ECB recommendations on internal control-lessons learned... 48

Panel Banks

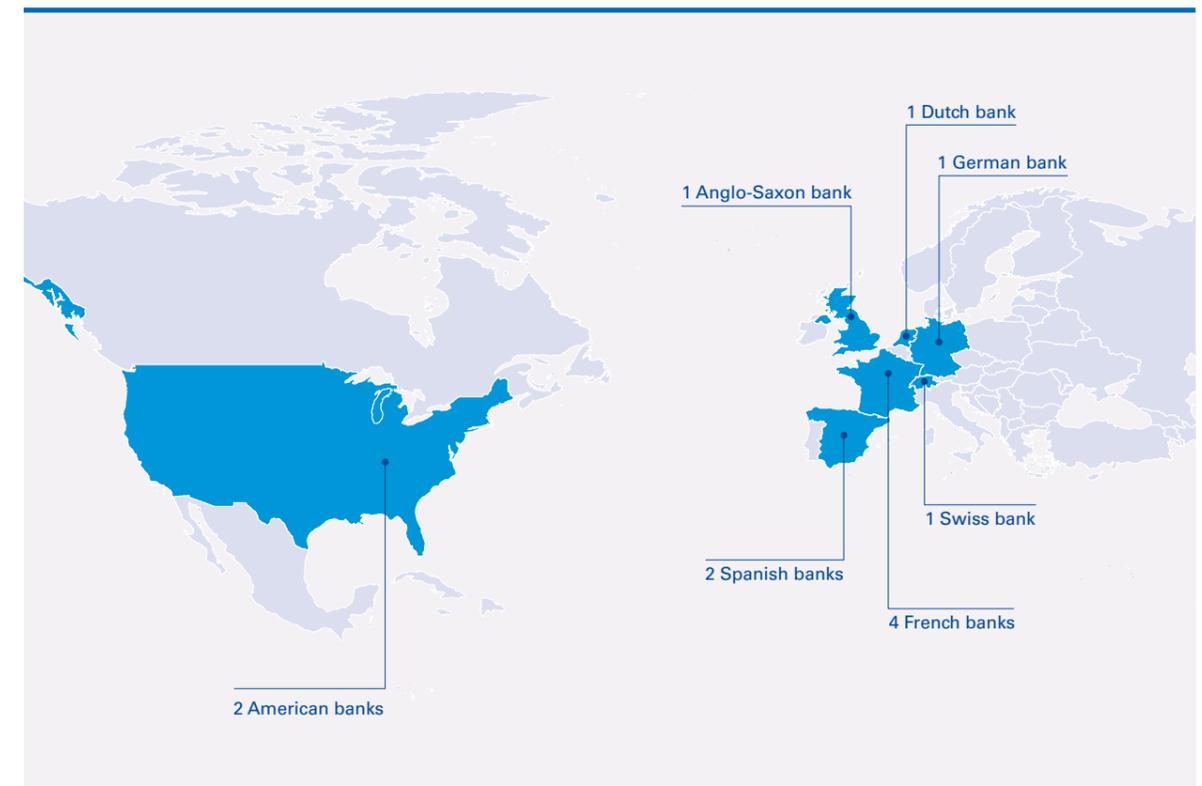
In order to identify the state of maturity of the internal control framework & operational risk management across a panel of banks and identify best practices to align with regulatory expectations, reduce operational risk, and create a robust permanent control framework, KPMG France created a questionnaire to provide a benchmark of initiatives and practices.

The benchmark contained 55 questions on the following topics:

- Governance & Organization
- Risks & Controls Framework
- Operational Risk Management
- Deployed Tools
- Regulatory Review

In total 12 banks participated in our benchmark, including 4 French banks, 2 American banks, 2 Spanish banks, 1 British bank, 1 Dutch bank, 1 German bank, and 1 Swiss bank.

The questionnaire can be found in the Appendix.



1. Governance & Organization

Which department leads the review of your ICF ?

What is the frequency of its review ?

We observe that all the banks of our panel conducts a review of their internal control framework at least annually.

The Risk LOD2 department is a frequent leader in the ICF review, often assisted by the Compliance department for all non-compliance risks related topics.

We observe that Each LOD2 is solicited based on its areas of expertise, and the proposed updates, inventoried throughout the year, are validated through dedicated process, risk and/or control committees.

In terms of best practices, we observe that setting up a single department for both operational risk and internal control ensures a consistent holistic approach between processes, risks, and controls covered.

For banks splitting the two functions in their organization, it is key that both Risk and Internal Control work closely and collaboratively to manage the review of the ICF, so that they can capitalize on the results of the RCSA to continuously improve their ICF.

BANKS	Risk	Compliance	Permanent Control	Comments
Bank A 			X	A dedicated Permanent Control department and 3 LOD2 Compliance, Risk & Finance
Bank B 	X			5 LOD2 Compliance, Legal, Tax & Finance while Permanent Control is within Operational Risk department 3 committees: 1 process review committee, 1 risk committee, 1 organization committee
Bank C 	X			Risk & Permanent Control department
Bank D 			X	
Bank E 	X	X		
Bank F 	X	X		
Bank G 	X			Risk with 2nd LoD staff involved
Bank H 				
Bank I 	X	X		Predominantly Risk (i.e. Non-Financial Risk Management department) and Compliance
Bank J 	X	X		Risk including credit, market and operational risks
Bank K 	X	X		They are in charge to set the standards, requirements, methodologies, taxonomies, controls.



INSIGHTS

- The governance behind the update of the ICF is heterogeneous
- The Risk Department is a frequent leader on ICF topics
- The ICF review is handled by one or many departments
- The ICF review is conducted at least annually



BEST PRACTICES

- Two departments manage closely the ICF review, Operational Risk and Permanent Control department, to capitalize on the RCSA contribution
- One single department for both Operational risk and Internal Control

**How is the LOD1 organized ? Are there controls dedicated staff ?
What are the duties of LOD1 ? Control Execution and/or Risk Anomalies Assessment ?**

We found that 75% of the panel is in charge of performing controls and assessing risk level of anomalies identified in the control execution. In the remaining 25%, the second level of defense (LOD2) is in charge of assessing the operational risk anomalies.

Some of the banks deployed dedicated staff to carry out controls within LOD1 in order to homogenize and further improve the controls execution and formalization standards across their different businesses and functions.



In terms of best practices, the execution of operational controls and the assessment of anomalies should not be dissociated and should be carried out by LOD1.

Because the LOD1 carries out operational controls and is most familiar with the operational process that it is evaluating, it is in the best position to assess anomalies observed when executing the control. Accordingly, control executions should be centralized at LOD1 in order to avoid misunderstanding between LOD1 and LOD2.

In practice, this means that LOD1 must execute the controls under its remit by following defined guidelines, providing a rating and a risk level, and reporting the identified incidents in operational risk management tools to allow for remediation and action plans and escalation.

Moreover, assistance from LOD2 experts to formalize and track controls is recommended in order to ensure the level of the quality of reviews performed by LOD1. Such experts may have an advisory or support role during the control campaign.

© KPMG 2021



INSIGHTS

- LOD1 assesses the control execution at 100% in our banking panel.
- A majority of our panel (75%) is also in charge to assess risk anomalies identified in the control execution. Of the 25% remaining banks, LOD2 is responsible for assessing risk anomalies.



BEST PRACTICES

- The assessment of the control execution and the assessment of risk anomalies should not be dissociated.
- The best practice is to centralize the control execution and anomaly rating at LOD1 to avoid misunderstanding between LOD1 and LOD2. Moreover, LOD1 has a closer understanding of business topics.

How is your LOD2 organized ? Which department are part of your LOD2 ?

Out of 80% of the banks studied, the Risk Department is considered as the primary LOD2 function for the internal control framework, along with Compliance. KPMG also noted that Finance, Legal, and Tax are less represented at LOD2 with respect to the internal control framework (less than 50% of the panel banks). KPMG also observed that 2 banks had created an LOD2 dedicated to the environmental and social risks, and that one bank had grouped its different LOD2 department into one "Sox department".

One bank also reported having created a permanent control unit independent from LOD1 and LOD2, in charge of reviewing the LOD1/LOD2 organization consistency, removing redundancies, with targeted ambitions of reducing permanent control costs.

BANKS	Risk	Finance	Legal	Tax	Compliance	Sox department	HR	Audit	Credit review	ESG	Engineering
Bank A	X	X			X						
Bank B	X	X	X	X	X						
Bank C	X				X						
Bank E	X	X	X		X						
Bank F						X*					
Bank G	X	X	X		X		X			X	X
Bank H	X				X						
Bank I	X				X						
Bank J	X			X	X	X					
Bank K	X	X	X		X		X	X	X	X	
Bank L	X		X	X	X		X				

*This department includes Compliance, Operational Risk, and IT RISK.

© KPMG 2021



INSIGHTS

- Heterogeneous organization on each of the panel banks. In 80% of the banks studied, the Risk department is considered as a LOD2, as well as the Compliance department.
- Finance, Legal & Tax are less represented in the LOD2 position
- Independent unit dedicated to review of LOD1 & LOD2 organization (case of 1 American bank)

How many people are dedicated to LoD2 / LoD3 in FTE number compared to the total staff of the bank ?

Data & Analytics: Is there a department specializing in the processing and analysis of LoD1 and LoD2 control data ?

In terms of LOD3, most banks on the panel dedicated 0.6% to 1% of all bank personnel.

In terms of LOD2, the percentage of staff are more heterogenous across banks, even though only 3 banks have more than 5% staff dedicated to LOD2.

LOD2 includes 2 categories of roles: (1) experts, who set forth guidelines, instructions, or advisory roles, and (2) LOD2 controllers of LOD1.

In terms of data & analytics, KPMG found that 33% of panel banks have a data & analytics department specializing in the processing of and analysis of control data. This is an area of ongoing development for most banks within our benchmark, most of which are working on incorporating the use of data & analytics and to facilitate the automation of controls.

-  LOD2 is 0,5%* to 4%* and LOD3 is 0,6% to 0,65%* (4 banks)
-  LOD2 is 0,5%* to 11%* and LOD3 is 0,7% to 0,9%* (2 banks)
-  LOD2 is 0,5%* to 2%* and LOD3 is 0,8% to 1%* (3 banks)

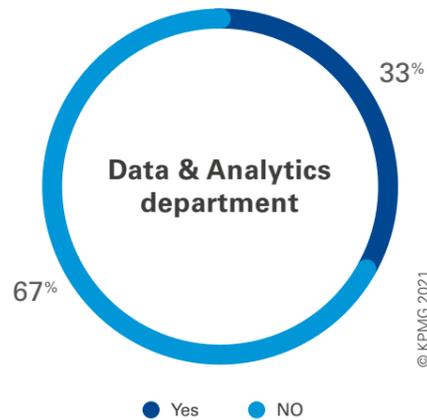
In terms of best practices, the optimal threshold of dedicated internal control personnel appears to be around 4% of all bank personnel.

The LOD1 dedicated permanent control personnel play a significant role in carrying out the internal control framework, since it carries out operational controls and is most familiar with the business and operations.

At the LOD2 and LOD3 levels, we found it optimal that LOD2 experts comprise of at least 1% of all bank personnel, LOD2 controllers of LOD1 comprise of at least 2% of all bank personnel, and LOD3 comprise of at least 1% of all bank personnel.

Data processing and incorporation of data & analytics into their Internal Control Framework is an ongoing issue for development for most banks. To facilitate the most efficient and effective use of data, the data & analytics department must be shared with the LOD1 to facilitate understanding of the business and allow for faster and more relevant analysis and remediation.

* N.B. : - Percentages are expressed based on the number of FTE in LOD2/LOD3 out of Bank total FTEs
 - For LOD2 figures, lowest range corresponds to count of Controls teams within LOD2, while highest range corresponds to counts of both controls and expert teams within LOD2



INSIGHTS

- Only 3 banks have more than 5% staff within LOD2
- For LOD3, the percentage of bank personnel is stable in all banks except one, between 0,6% to 1%
- 33% of our banks have a D&A department specializing in the processing and analysis of LOD 1 and LOD 2 control data
- The LOD2 nearshoring / offshoring main concerns relate to delegations and SLAs



BEST PRACTICES

- The percentage of Internal Control dedicated staff appears comprises of 4% of bank personnel:
 - 2% LOD2 controllers on LOD1
 - 1% LOD2 experts
 - 1% Internal Audit (LOD3)
- The "Data and Analytics" department must be present at LOD1 to facilitate the understanding of business and allow faster and more relevant analysis

2. GRC Approach

Is your ICF supported by an activity & process mapping ?

Did you integrate a holistic process mapping approach in your ICF?

This holistic process mapping approach binds together the different components of the Internal Control Framework (Activities – Process – Risks – Controls), including:

- Process mapping of the bank's principal activities;
- The identification of the risks associated to these processes;
- The controls mitigating these risks.

KPMG found that 50% of the panel banks performed a holistic mapping approach, while 50% of the panel banks had not.

For some of the banks which did not implement it, the focus was given on the activity and process mapping to a granular level, while the exhaustive cartography of these processes to risks and controls was not the priority. The European Central Bank, on the other hand, requires an integrated control framework that incorporates a holistic approach of mapping activities and processes to related risks and mitigating controls. Accordingly, EU banks have incorporated a holistic process mapping.

BANKS	Holistic process mapping approach ?	Comments
Bank A 	X	Exhaustive and holistic APRC approach
Bank B 	X	
Bank C 	X	
Bank D 	X	Process to risk to framework to control link
Bank F 	X	Controls are linked to a process taxonomy and are grouped in tasks
Bank G 		The GRC tool is linked to the Group's process repository
Bank E 	X	
Bank H 		
Bank I 		No activity & process mapping performed at the Bank
Bank J 		The risks are linked to the assessment units
Bank K 		The risks are linked to controls



INSIGHTS

- 50% of the responding banks out of our panel perform a holistic process mapping approach
- Two banks have identified the activities and related processes, risks, and controls in a single and accessible tool

3. Risk management - taxonomy and assessment

Did you implement a risk taxonomy ?

Is it an entity's specific taxonomy different than those of the regulator (i.e. risk taxonomy outlined in the Basel II Operational Risk Taxonomy) ?

How many levels (hierarchies) and categories per level are included in this taxonomy ?

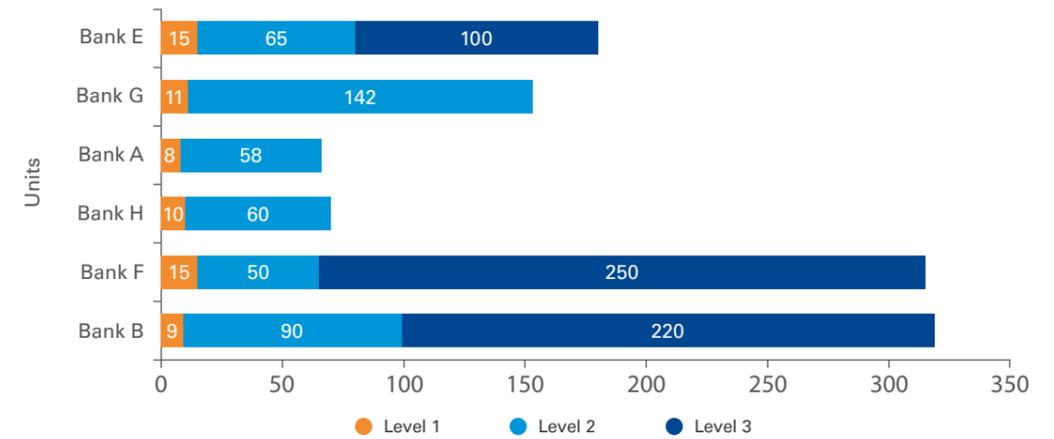
One-third of the banks that responded maintained a risk taxonomy in conformance with the Basel II Operational Risk taxonomy.

Two-thirds of banks stated that in addition to the incorporation of the Basel II Operational Risk taxonomy, they also implemented a specific risk taxonomy that captured up to four levels of risks in order to take into account the specific risks for business and service units and refine their risk assessment exercise.

BANKS	Risk levels	Risks
Bank A	2	<ul style="list-style-type: none"> Level 1 contains 8 major risks Level 2 contains 58 risks
Bank B	3	Level 1 contains 9 major risks / Level 2 contains 90 generic risks / Level 3 contains 220 risks
Bank C	2	The taxonomy includes 140 operational risks (including compliance one) at the finest level
Bank D	4	
Bank E	3	15 risks are level 1, 65 risks at level 2, >100 at level 3 (operational risks)
Bank F	3	The taxonomy contains 15 principles risks, declined to 50 at level 2, to 250 at level 3
Bank G	4	<ul style="list-style-type: none"> 11 risks types at level 1 142 risks types at level 3
Bank H	2	The taxonomy contains 10 principles risks, declined to 50 to 60 at level 2
Bank I	3	3 levels of risks
Bank J	4	
Bank K	4	

© KPMG 2021

Number of risks per level



© KPMG 2021

In terms of best practices, the risk taxonomy structure should be organized into three levels.

For regulatory purposes, the first level of risk incorporates the Basel II Operational Risk Taxonomy. We observe 9 to 15 risk categories.

The second level identifies specific risks based on the activities/functions of the banks and links them to the higher-level Basel II Operational Risk Taxonomy. This level is often used for the consolidation of more granular risks and reporting at Group management Level.

Importantly, banking groups should incorporate a

third level of risk linked to the second level of risk, which will provide for a more refined risk taxonomy that takes into account the specificities of the business line and support functions. Ideally, a banking organization should have no more than 150 level three risk categories, so that the categories are better homogenized and consolidated.

In terms of best practices, one single taxonomy should be implemented to take into account and manage operational, non-compliance, and IT risks.



INSIGHTS

- All panel banks have implemented a risk taxonomy linked to the Basel II Operational Risk Taxonomy
- 80% of the panel banks have implemented a single taxonomy, including operational, non-compliance, and IT risks
- All panel banks have developed an operational risk taxonomy with different granular levels :
 - L1 Basel,
 - L2 by topic,
 - L3 which include risks specific to Business & Service Units



BEST PRACTICES

The Risk Structure should be organized into three Levels :

- A First Level of risks linked to the Basel 2 Taxonomy
- A Second Level of risks to specify the Basel categories and to be used for consolidation
- A Third Level of risks used to take into account business/functions specificities and monitoring needs
- The Third Level of risks should be limited in order to preserve the homogeneity of the Risk structure

Adoption of a single Taxonomy for all operational Risks including non-compliance risks at a manageable level (no more than 150 Level 3 risks)

Is there a Risk & Control Self Assessment (RCSA) exercise ? What is its frequency and which department leads it ?

Is there a specific RCSA exercise for IT issues / Compliance exercise ? What is its frequency and which department leads it ?

The RCSA is carried out annually in all banks and quarterly for some units of the American and British banks. The Risk and Compliance functions are the frequent drivers of the RCSA exercise.

In terms of best practices, we recommend that one global RCSA exercise be implemented in a unique tool, coordinated by one single LOD2, with the involvement of each relevant business line/function at LOD1 to perform the exercise. This will further permit the LOD2 functions to analyze the results of the LOD1 controls in their risk area, based on drill-down capacities of the tool, so that they are readily linked in one exercise and tool.

BANKS	RCSA exercise	RCSA IT exercise	RCSA Compliance exercise
	Department	Department	Department
Bank A 	Risk	IT	CPLE
Bank B 	Group risk (ORC - LOD1) Check & challenge by LOD2	Done by IT & mapped to ORC RCSA	Group Risk (ORC) for a part & CPLE for the rest
Bank C 		Group Operational risk (applicable to the 3 exercises)	
Bank E 	Yes – driven by LOD1	Yes – driven by LOD1	Specific RCSA Compliance
Bank G 		NFR (LOD1/LOD2) (applicable to the 3 exercises)	
Bank H 	Compliance (LOD2)	Does not exist	Does not exist
Bank I 	NFR (LOD2)	Chief Information Security Officer (LOD1) /Tech & Cyber Department / NFR (LOD2)	Compliance function (LOD2)
Bank J 	1 exercise & tool Risk (LOD2)	1 exercise & tool Risk (LOD2)	1 exercise & tool Compliance (LOD2)
Bank K 	Risk (LOD2)	Risk (LOD2)	Compliance (LOD2)
Bank L 	Risk (LOD2)		Compliance (LOD2)

© KPMG 2021



INSIGHTS

- The frequency of the RCSA is at least annual in all the banks and quarterly in some units of the American Banks and the UK Bank. There is an on-going RCSA for a few banks
- Risk & Compliance departments are the frequent leaders of the RCSA exercise

N.B. There is a difference between compliance RCSA and compliance certification:

- Compliance RCSA assesses the compliance operational risks
- Compliance certification focuses laws and regulations that apply to activities and products per location that must be respected by the banks. Compliance officers certify this on a regular basis



BEST PRACTICES

- One global RCSA exercise implemented in one unique tool with the drill-down option and the involvement of LOD 2 from each business line (holistic approach)
- An on-going RCSA updated to take into consideration new losses & incidents

4. Tools

Is there a single tool within the Group for Internal Control and Risk Management ?

Do you use in-house developed tools or market software ?

Very few banks reported having a unique ICF tool that includes processes, LOD1 and LOD2 controls taxonomy and execution formalization, reporting for control anomalies, action plans, internal losses and incidents, the RCSA, quality assurance indicators, and Key Risk Indicators.

Most tools are external solutions but are further refined in-house.

When external solutions are reported, 40% of the respondents indicate using SAP or IBM Open Pages, as well as Archer and MetricStream among US and UK banks. Evolan is used by two French banks.

In terms of best practices, one single tool within the Group should be deployed that takes into account all components of the internal control framework: processes, control results, action plans, internal losses and incidents, the RCSA (operational risk, non-compliance risk, IT), and other Key Risk Indicators.



INSIGHTS

- Very few banks have a unique ICF tool that includes processes, control environment (both LOD1 and LOD2 controls), control anomalies, action plans, internal losses and incidents (including IT incidents), RCSA, quality assurance indicators, KRI, etc...
- The tools are mainly based on external solutions, which are further refined in-house
- The providers are SAP or Open pages (40%) but also Archer and Metric Stream
- Evolan is used by two French banks



BEST PRACTICES

- One unique and holistic tool including all the components of the internal control framework : processes, control results, action plans, internal losses and incidents, RCSA, indicators etc.

5. Regulatory & Challenges

What immediate or future challenges do you face in terms of internal control framework and operational risk ?

Was your Internal Control framework reviewed by the regulators ?

Methodology: one of the main challenges is to implement a holistic approach with one RCSA global exercise and that better integrates IT and fraud risks relating to cybersecurity. The link between operational risk and internal control needs to be improved, and the controls inventory across business divisions need to be rationalized. The establishment of a front to back mapping of processes remains a challenge for some banks, including a mapping to resources. A key controls heatmap may also permit the rationalization of controls and help adjust the control systems by making them more agile.

Tools: better automatization and effectiveness is needed to reduce the workload of controls, improve the quality of the reporting and enhance data quality. This will also help accelerate the resolution of anomalies in all phases of permanent control.

People and resources: banking institutions found that there needs to be a better acknowledgment of a "control culture" within the Bank, and that this is shared at the business level and not just compliance and general management functions. Better data sharing is also needed across organizations. Outsourcing/ offshoring continues to be a trend in most banks of our panel, with efforts given on digitalization, with the same ambition to reduce fixed costs.

Regulatory review: all banks had their internal control framework reviewed by the ECB, sometimes leading to the launch of a permanent control transformation program. KPMG observed that one of the paneled banks limited the number and impact of ECB recommendations received, by providing the ECB access to its single internal control tool.



CHALLENGES

Methodology

- Implement a holistic approach with one RCSA global exercise, with better integration of IT Risks (cyber-security,...)
- Improve the link between operational risk information and the internal control model
- Refine the key controls inventory (rationalization and harmonization across business divisions)
- Establish a front-to-back view of bank processes including mapping of resources (operational resilience)
- Produce a key controls heatmap
Adjust the control system by making it more agile

Tools

- Control efficiency (automatization)
- Reporting improvement (quality and upstream)
- Enhance the data quality

People & resources

- Better acknowledgement of the control culture around the group
- More effective data sharing within the group with a better risk analysis and data structuration
- Adaptability of the organization to new ways of working (remote, efficiency, change management)
- Efficiency & cost : further outsourcing, digitalization, remove controls redundancies, and adjust / optimize the number of staff in LOD1 & LOD2

Regulatory

- The new operational risk calculation method will be a challenge in calculating operational risk, which will affect the level of capital required.



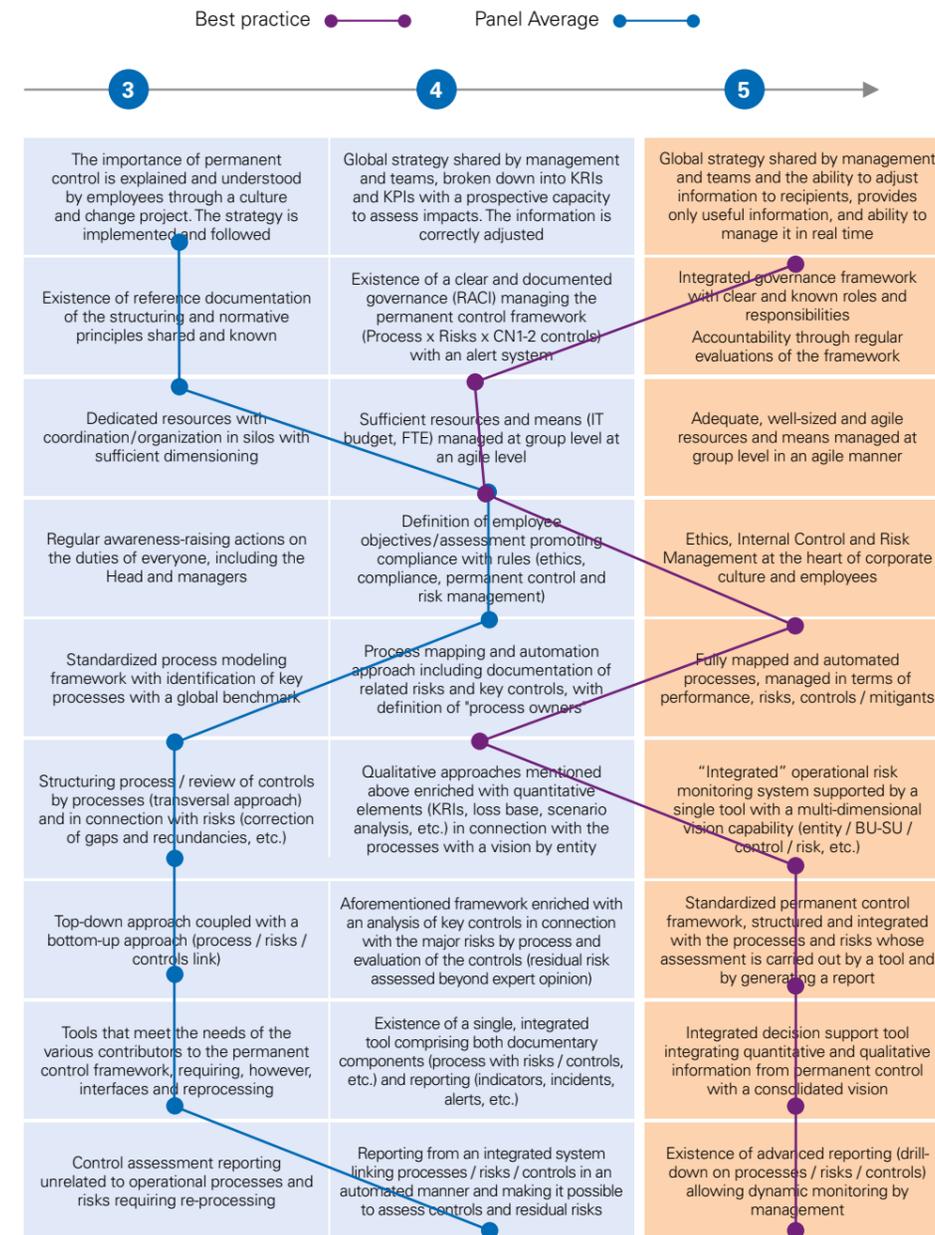
INSIGHTS

- Almost all panel banks had a regulatory review. In many cases the ICF was reviewed and recommendations received concerned its maintenance for completeness and continuous monitoring. One European bank provided the regulator with complete access to its ICF tool which facilitated the review process

6. Permanent Control Maturity Matrix

Permanent Control Maturity Matrix showing best practices and the panel average among banks interviewed

	0	1	2
1. Strategy & Vision	Lack of clarity, formalization and integrated monitoring of the strategy (Business, HR, Risks & Controls)	Strategy by activity supported by a risk appetite definition and monitoring system and decision support reporting. No independence of LOD1 and LOD2	Extended global strategy (Business, Risks & Controls, HR) broken down by business with an allocation of capital by activity and a dedicated risk monitoring system
2. Organization / Governance	Lack of organizational clarity (governance framework, roles and responsibilities, etc.) "Patchwork" without overall consistency	Unclear definition of operating principles with multiple uncoordinated actors and unaligned missions	Clear definition of operating principles (roles and responsibilities, hierarchical and functional links, etc.) covering LoD1 and LoD2
3. Resources & Means	Inadequate or insufficient resources and means	No dedicated resources performing operational tasks and controls without coordination or organization	Dedicated resources without coordination or organization with insufficient sizing
4. Company Culture & Values	No definition of company values	Definition but no formalization and communication of the values of the company and not shared by Management	Existence of a code of conduct and a code of ethics signed by all employees
5. Processes	Absence of documented processes	Unmapped and poorly automated processes, partially documented	Partially mapped and documented processes, without a transversal vision and without a global framework
6. Risks	Heterogeneous and undocumented operational risk maps	Existence of a charter and a framework of common operational risks	Identification and evaluation (frequency / impact) of operational risks to be "expert opinion" ("top-down") Existence of rating scales (standardized quality and quantity)
7. Controls	Lack of organizational clarity/Patchwork of control areas without overall consistency and without a normative framework	Non-standardized controls with flaws in design / implementation	Normative framework for the design and implementation of controls not linked to processes and risks
8. Integrated tools	Historical multiplication of systems as and when required	Multiple applications and tools, information not readily available. No common repositories	Multiple applications and tools, non-globalized databases requiring manual reporting by silo / activity
9. Monitoring & Reporting	Lack of monitoring and reporting on operational risks and controls	Basic reporting of control activities unrelated to processes and risks and which do not allow for monitoring	Basic reporting of control activities requiring re-processing to obtain a consolidated vision for management



7. ECB recommendations on internal control - lessons learned

Based on a review of the ECB recommendations issued for several global systemically important banks G-SIBs, KPMG identified the below lessons learned, which include:

- strengthening the governance and organization of the permanent control framework,
- maintaining an exhaustive yet efficient methodological framework that covers all operational risks but reduces control redundancy,
- improved quality and completeness of reporting,
- reinforcement of resources, and
- integrated IT tools common to the Group and its activities / functions worldwide.

Organization & governance	Methodological Framework <small>Process, Risks And Controls</small>	Reporting	Resources	IT Framework Tools
1. Refine / streamline the organization & governance	1. Harmonize / Reduce / Simplify the risk taxonomy and the number of controls focusing on key risks (especially for institutions with > 100 key risks) and key controls adequately designed and fully performed	1. Incidents – report exhaustively historical incidents & near-missed in a reliable information set	1. Reinforce the recruitment and training policies	1. Development & implementation of an integrated IT tool common to the Group and the activities / functions worldwide, in order to provide a full picture of the permanent control integrating Ops Risks & RCSA results together with the related Heatmaps
2. Define the operational control role, and communicate roles and responsibilities (mission statement)	2. Exhaustive coverage of the operational risk framework including compliance: financial security (fraud, sanctions...)	2. Improvement of quality, completeness & reliability of operational risk data & reporting	2. Ensure alignment of skills of resources with their scope of controls (business / Function)	
3. Strengthen management framework regarding outsourcing	3. Strengthen the LOD1 / LOD2 for effectiveness, coherency and comprehensiveness	3. Model incident - Enhanced management & monitoring of PIs at Group level, as major input for Advanced Measurement Approach	3. Strengthen the Permanent Control teams size	
4. Ensure proper segregation of duties and delegation	4. Consider all dimensions of Op. Risk when defining risk appetite metrics, including forward looking controls		4. Foster a risk culture across the Permanent Control teams	
5. Reinforce the definition / update of strategic approaches	5. Consistent & effective RCSAs across the businesses/functions at process level 6. Enhanced Op. Risk Management especially in terms of action plans			



4



The main drivers
of action

The main drivers of action

KPMG proposes main drivers of action to be implemented according to the degree of maturity in the permanent control framework

The areas of progress include strategy and vision, organization, and governance.

In order to build upon the existing permanent control framework, the main drivers of action to strengthen the Internal Control Framework include:

- Improving the operational risk identification framework and improving the system to report losses and incidents;
- Ensuring the completeness of the covered scope, including taking into account cases of outsourcing;
- Align and optimize the risk assessment frameworks (RCSA) with the permanent control framework;
- Integrate operational resilience into operational risk management;
- Rationalize IT tools and improve on the use of new technologies;
- Optimize resources of the risk department and clarify roles and responsibilities of different lines of defense.



Identification of operational risk and management

- Improve the operational risk identification framework (deploy an APRC method, set up a risk database, etc)
- Improve the system for reporting losses and incidents, capturing and exploiting weak signals



Ensure the completeness of the covered scope

- Take into account changes in scope, including cases of outsourcing (offshoring / outsourcing of processes or controls in repositories or tools)
- Improve risk management related to remote work and use of data management by third parties



Alignment and optimization of evaluation frameworks (RCSA) and risk control (CP)

- Rationalize use of activity/process mapping of the bank between different risk management frameworks
- Improve the link between the evaluation of non-compliance risks and those of operational risks.



Operational resilience

- Rely on a repository of activities and common processes to identify resources and means (people, tools, etc)
- Take into account the guidance of the Basel Committee relating to operational resilience with a view to integrate operational resilience into operational risk management
- Improve cyber-resilience in the face of sophistication of attacks



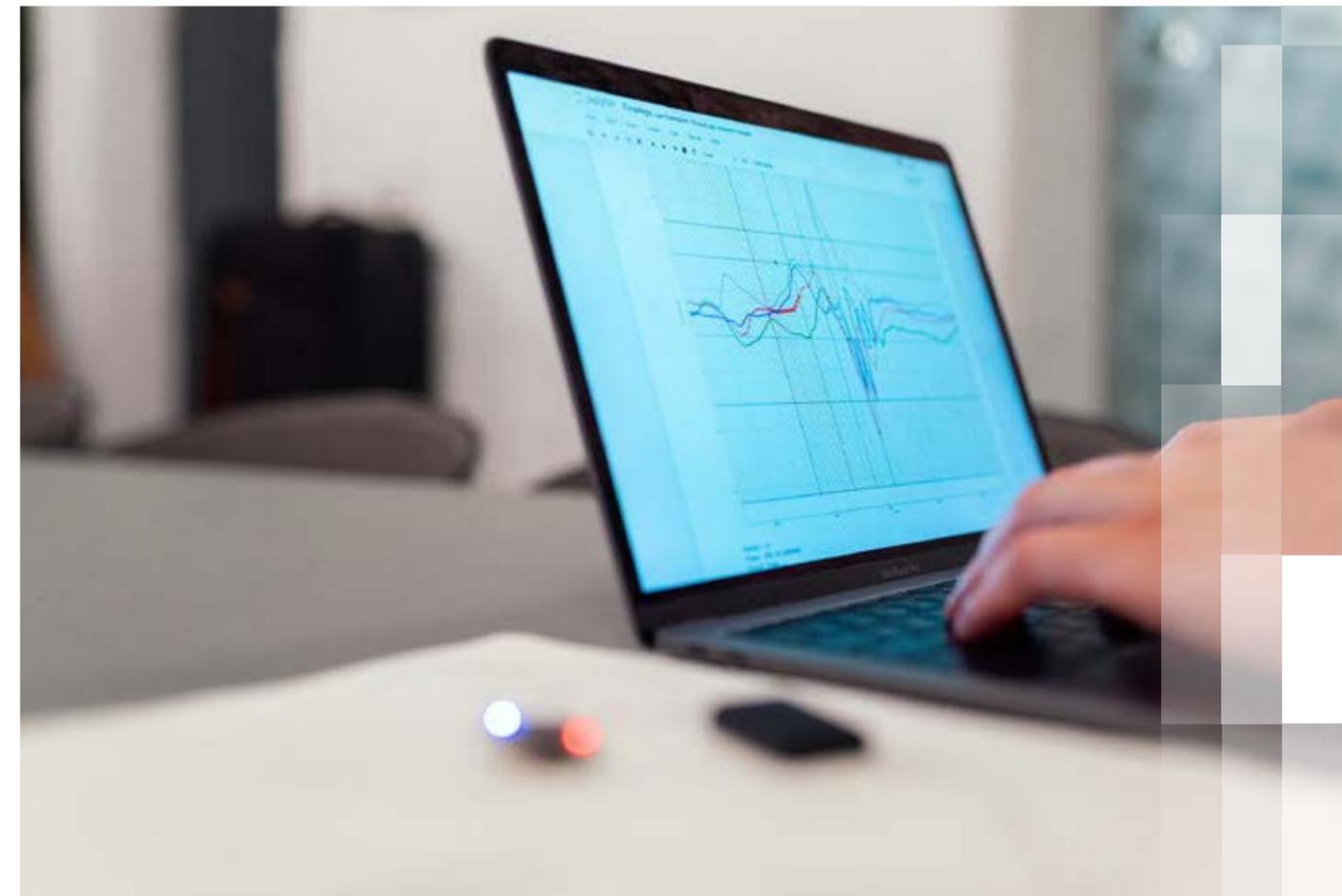
Tools

- Rationalize the application base and IS
- Improve the use of new technologies (D&A, Intelligent Automation, Blockchain, etc)
- Improve remote access



Governance and Reports

- Model the target organization / Creation of new positions
- Optimize resources of the risk department (e.g. expert functions / control functions, local / central, etc.)
- Clarify the roles and responsibilities of different lines of defense
- Improve comitology effectiveness
- Raise awareness of train operational staff and managers
- Improve the quality of reports (data quality, inter-report consistency, appropriate adaptation to recipients)



5.



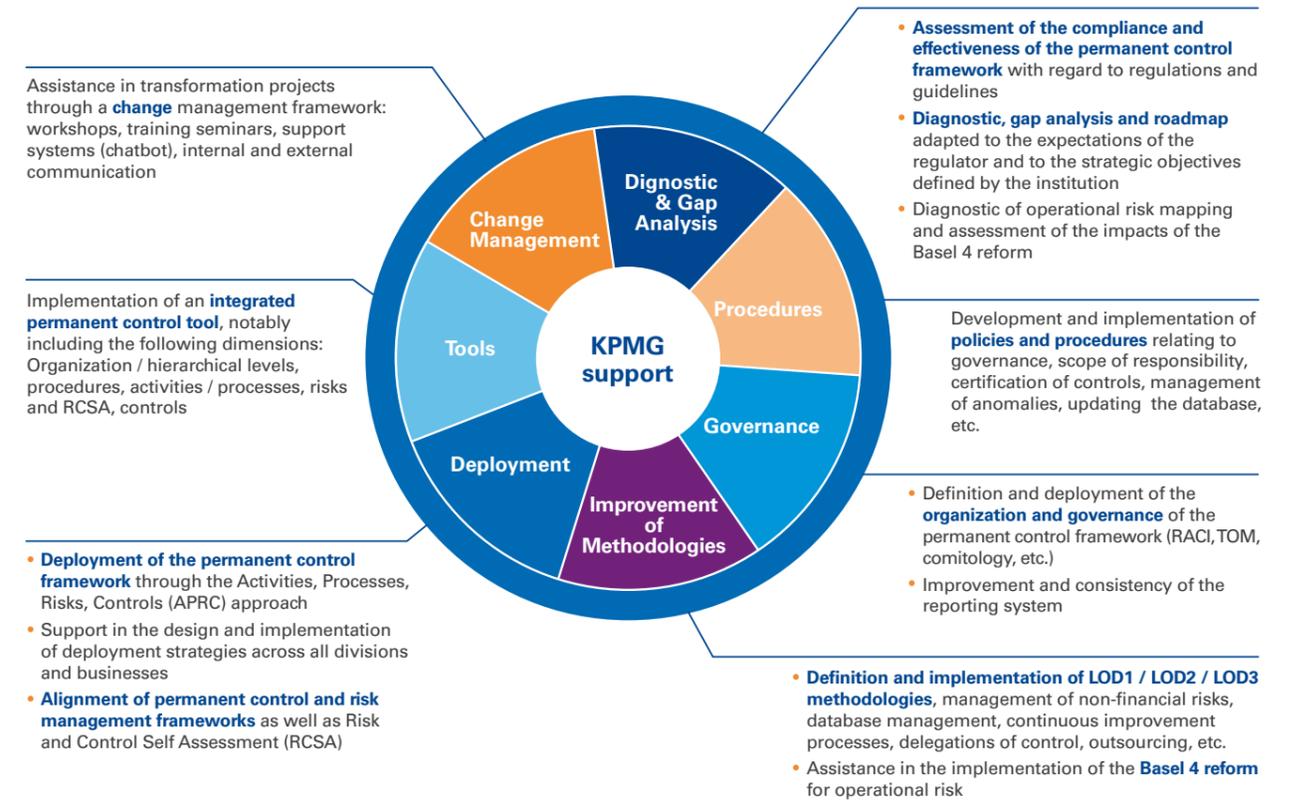
How KPMG
can assist you

How KPMG can assist you

Permanent Control and Operational Risk continue to be a heightened area of focus for financial institutions as the industry wrestles with challenges arising from Covid-19 Crisis, cyber threats, third-party concerns (clients, investors, partners, regulators...), trading, conduct and culture issues, stress testing requirements, and technological innovations driving greater incentives for process automation and digitization.

Regulators maintain a keen focus on ensuring firms develop and maintain effective risk management structures to enable them to identify, assess, monitor and manage risk with ever-increasing speed and accuracy.

The AxPxRxC approach is a "Top-down" approach defined by KPMG in order to ensure a comprehensive permanent control framework, and assist our banking clients to map and improve their existing control setups. KPMG's approach focuses on a risk-based approach that ensures that all risks of the existing RCSA and losses mapped to processes are addressed.



6.



Benchmark methodology

Benchmark Methodology

Internal Control Framework benchmark Questionnaire

The internal control questionnaire contained 55 questions as presented below on the following topics in regard to the ICF:

- Governance & Organization
- Governance & Risk Control (GRC) Approach
- Risk Management
- Tools Used
- Regulatory Review

#	Question
Governance & Organization	
Global overview	
1	• Could you please describe the Governance and Organization implemented with respect to Internal Control Framework (ICF), on the below axis:
Review of the ICF	
2	• What are the departments involved in the management and update of the ICF ?
3	• What is the frequency of the review of the ICF ?
4	• Is there a governance in place to update the internal control framework?
LoD 1	
5	• How is LoD 1 organized (dedicated or non dedicated staff, who are the interlocutors involved) ?
6	• Do the LoD1 assess the control execution (e.g. control result as satisfactory, globally satisfactory, marginally satisfactory, unsatisfactory) / the risks related to the anomalies or is it only the role of the LoD2 ?
7	• How are anomalies on LoD1 controls escalated ? Is there an escalation process to LoD2 ?
8	• How do the processes for reporting anomalies on LoD1 controls and operational risk incidents interact ?
LoD 2	
9	• Which departments contribute to LoD2 (e.g. Risk, Finance, Compliance, Tax, Legal, etc.) ?
10	• What are the assignments of the LoD2 departments in the internal control framework ? Could you clarify their role ?
11	• How many people are dedicated to LoD2 in number compared to the total staff of the bank, or preferably what is the percentage of LoD2 dedicated staff ?
12	• Is part of the LoD2 function near/offshored or outsourced ? If yes, which are these departments and is there a delegation process formalized ?
13	• Data and Analytics: Is there a department specialising in the processing and analysis of LoD 1 and LoD 2 control data ?
LoD 3	
14	• How many people are dedicated to LoD3 (General Inspection and Internal Audit) in number compared to the total staff of the bank, or preferably what is the percentage of LoD3 dedicated staff ?
GRC approach	
Did you implement an holistic and integrated approach (Governance Risk Compliance type) for Internal Control Framework ?	
Such approach binds together the different components of the ICF, which are :	
15	• The processes mapping of the main activities • The identification of the risks associated to these processes • The controls mitigating these risks • The data (BCBS239 principles) in the scope of the controls
16	• Is this approach materialized in data repositories (activity repository, process repository, controls library etc.) ?
17	• If yes, could you please indicate which department(s) is/are in charge of managing and updating these repositories ?
18	• What is the scope of deployment of this approach, particularly in the case of deployment at group level ? All entities, only significant entities according to criteria etc.
Process mapping	
Is your ICF supported by an activity process mapping ?	
If yes :	
19	• Could you please indicate the number of processes identified ? <100, 100-500 or >500
20	• Are these processes detailed by Business Units and Service Units ?
21	• Are the processes linked to risks and controls ?
22	• Are the processes linked to the financial statements ?
Monitoring & reporting	
24	• How is the whole framework monitored and reported ? Could you please describe the elements included in the reporting ?
25	• What levels of reporting are available ? Legal entity, by LoD2, organizational unit, department, service, etc.
26	• Does this reporting have drill down/up capacities (by family of processes, risks, etc.) ?
27	• Is there a specific department dealing with Internal control framework monitoring and reporting ?
28	• Is there a certification process for control results or a risk attestation process at entity or group level ? If yes, which members of senior management are involved ?

#	Question
Risk Management (RM)	
Risk taxonomy	
29	Did you implement a risk taxonomy ? If yes :
Review of the ICF	
30	• Is it an entity's specific taxonomy different than the regulators' ones ?
31	• Is it a single taxonomy for all risks ? For instance, you could manage separate taxonomies for risk root causes and risk events/consequences, or, he could have an operational risk dedicated taxonomy (targeted at operational departments) and a compliance risk dedicated taxonomy (targeted at compliance departments)
32	• How many levels (hierarchies) and categories per level are included in this taxonomy ?
Risk assessment	
Could you please describe your risk assessment ?	
34	• Is there a Risk & Control Self Assessment (RCSA) exercise ? What is its frequency and which department leads it ?
35	• Is there a specific RCSA exercise for IT issues ? What is its frequency and which department leads it ?
36	• Is there a specific a RCSA exercise for Compliance issues ? What is its frequency and which department leads it ?
37	• Is the residual risk outcome measured by the RCSA exercise treated differently depending on whether it is very low / low (e.g. risk acceptance) or high, very high (e.g. control review with higher frequency or redesign) ?
Tools	
Global overview	
38	• Is there a single tool within the Group for Internal Control and Risk Management ?
39	• If no, do the differents tools of Control and Risk Management feed a single datawarehouse which permits to generate consolidated views ?
40	• Do you use in house developed tools or market softwares, and in this last case, could you please state them ?
Internal Control tools	
41	Is there a single tool within the Group for Internal Control ? If no :
42	• Is there a single tool within the Group for LoD 1 ? For LoD 2 (Compliance, Risk, Finance etc.) ? For LoD 3 ? Cross LoD ?
43	• Do the differents tools of Internal Control feed a single datawarehouse which permits to generate consolidated views ?
44	• Is there a tool to centralize all anomalies on LoD 1 controls ? LoD 2 controls ?
45	• Is there a single value scale for control results (e.g. satisfactory, acceptable, etc.) and anomalies (e.g. very high, high etc.) at local or group level? What are the values of these scales ?
46	• Are the controls results and anomalies included in the tools ?
47	• Generally speaking, what is the level of data quality related to LoD1 and LoD2 controls ? Very Low, Low, Medium, High, Very High
Risk Management tools	
48	• Is there a single tool within the Group for collecting operational risk events ? If not, what are the differences between the differents tools (activity covered, financial impact, etc.) ?
49	• Is there a single tool within the Group for risk assessment ?
50	• Do the differents tools feed a single datawarehouse which permits to generate risk consolidated views ?
51	• Do you have a risk register to centralize all control results and operational risk events ? If yes, how is managed the link between both ?
52	• Generally speaking, what is the level of data quality related to operational risk events? Very Low, Low, Medium, High, Very High
Other topics	
Regulatory Review	
53	• Was your Internal Control framework reviewed by the regulators and what were the main outcomes/issues highlighted ?
Emerging challenges	
54	• What immediate or future challenges do you face in terms of internal control framework ?
55	• What immediate or future challenges do you face in terms of operational risk ?



KPMG global network contacts

KPMG global network contacts

KPMG IN FRANCE

Vicky Papaevangelou

T: +33 1 55 68 71 14
E: vpapaevangelou@kpmg.fr

Nicolas Coudrieau

T: +33 1 55 68 62 33
E: ncoudrieau@kpmg.fr

Carine Demonio

T: +33 1 55 68 72 95
E: cdemonio@kpmg.fr

KPMG IN SPAIN

Alberto Esteban Henche

T: +34 648029923
E: albertoesteban@kpmg.es

Luis Alberto Martin Riaño

T: +34 914563495
E: lamartin@kpmg.es

Jose Maria Mayor Bastida

T: +34 914568207
E: josemayor@kpmg.es

John Paul Depman

T: +34 914566029
E: johnpauldepman_extcolab@kpmg.es

KPMG IN SWITZERLAND

Thomas Wilson

T: +41 58 249 54 73
E: thomaswilson1@kpmg.com

Reto Ulrich Gareus

T: +41 58 249 42 51
E: rgareus@kpmg.com

Rafael Kaufmann

T: +41 58 249 58 97
E: rafaelkaufmann@kpmg.com

KPMG IN THE UK

Karim Haji

T: +44 207 3111718
E: karim.haji@kpmg.co.uk

Shanti Tharan

T: +44 7740 894517
E: Shanti.Tharan@KPMG.co.uk

Suvro Dutta

T: +44 7785 393901
E: Suvro.Dutta@KPMG.co.uk

Dawson, Libby

T: +44 7867 462923
E: Libby.Dawson@KPMG.co.uk

Richard Rawstron

T: +44 7789 202427
E: Richard.Rawstron@KPMG.co.uk

KPMG IN THE NETHERLANDS

Johannes Pastor

T: +31 6 82125727
E: Pastor.Johannes@kpmg.nl

Erwin Mol

T: +31 206 567498
E: Mol.Erwin@kpmg.nl

KPMG EMA HUB

Francisco Uria Fernandez

T: +34 914513067
E: furia@kpmg.es

Henning Dankenbring

T: +49 69 9587-3535
E: hdankenbring@kpmg.com

KPMG IN THE US

Judd A Caplain

T: +1 212 872 6802
E: jcaplain@kpmg.com

Brian J Hart

T: +1 212 954 3093
E: bhart@kpmg.com

Cameron W Burke

T: +1 404 222 3139
E: cburke@kpmg.com

KPMG IN GERMANY

Daniel Sommer

T: +49 69 9587-2498
E: DSommer@kpmg.com

Markus Quick

T: +49 69 9587-4687
E: markusquick@kpmg.com

Joerg Haupt

T: +49 69 9587-3438
E: JHaupt@kpmg.com

Peter Heidkamp

T: +49 221 2073-5224
E: PHeidkamp@kpmg.com



Contacts

KPMG in France

Vicky Papaevangelou

Tel. : +33 (0)1 55 68 71 14

E-mail : vpapaevangelou@kpmg.fr

Nicolas Coudrieau

Tel. : +33 (0)1 55 68 62 33

E-mail : ncoudrieau@kpmg.fr

Carine Demonio

Tel. : +33 (0)1 55 68 72 95

E-mail : cdemonio@kpmg.fr

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. KPMG S.A. is the member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a Private English company limited by guarantee. KPMG International and its related entities provide no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

© 2021 KPMG S.A., a French limited liability entity and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a Private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. Printed in France. Realisation: Advisory service - OLIVER - June 2021.

Pictures credits : iStock, Unsplash.