KPMG

Meet the new requirements for permanent control and operational risks management

Our service offering for operational risks and permanent control management for financial institutions

KPMG. Make the Difference.

SUMMARY

1. Current non-financial risks and permanent control issues

Regulatory supervision of financial industry actors (bank institutions, asset managers, insurance bodies) relating to non-financial risks, out of which operational risks, internal control, data and IT risks require the implementation of a holistic permanent control framework applying to all the bank's businesses and functions.

As a major player in this framework, the Risk & Internal Control functions must not only meet the expectations of the regulators, customers and investors, but also structure and organize themselves to become strategic and sustainable functions, while maintaining their cost structure.

KPMG supports the Risk & Internal Control functions of the financial industry and has developed a dedicated service offering.

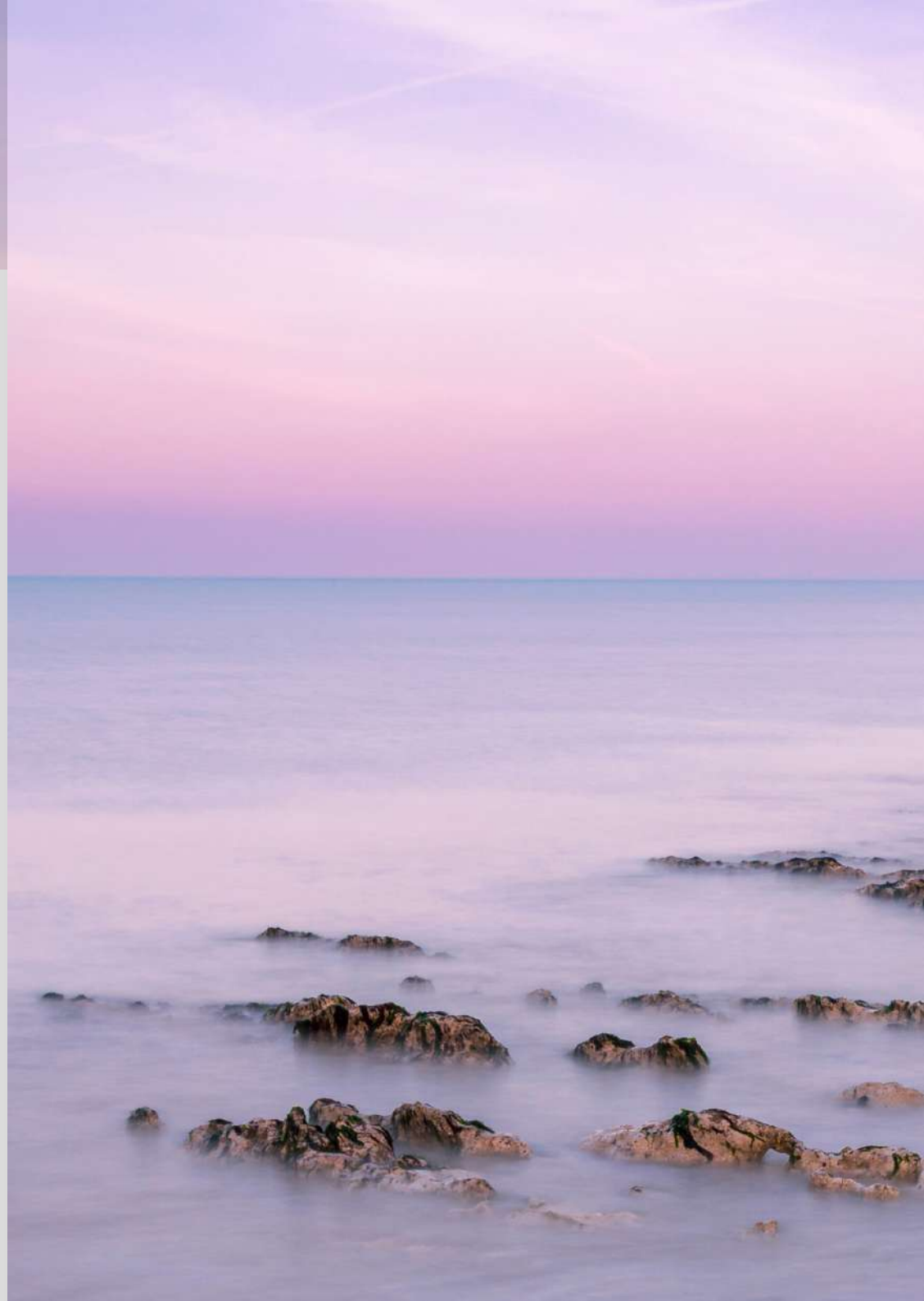
Regulators' expectations for an integrated permanent control and operational risk framework

The regulators recommend that banking and financial institutions establish an ecosystem of operational risks management and integrated permanent control, including:

- Strategy and Risk Appetite related to activities.
- Description of the processes associated with these activities, risks, and key controls to mitigate these risks.
- Key data related to these processes.
- The definition of roles and responsibilities at all levels of hierarchy, in particular LOD1, LOD2 and LOD3*.
- An integrated tool to enable the execution of an RCSA at the processes' level and specific reporting: risk cartography, key risks indicators on internal control, results of the controls execution and residual risks assessment.
- A description of the company's risk management framework.

This framework should cover the Group and its entities and be subject to governance with clear roles and responsibilities, reporting through an integrated tool, monitoring, and continuous improvement plans.

* LOD: three lines model - LOD1: 1st line of defense, LOD2: 2nd line, LOD3: 3rd line - audit/inspection



INTEGRATED INTERNAL CONTROL FRAMEWORK

Strategy & Vision
Capital allocation by activity

Risk appetite

Identification of activities

Processes

Cartography of banking activities processes at group and entity level

Description of key process tasks

Risks

Identification of risks by process

Risks Taxonomy
9 risk categories (B2), including operational risk (7 categories including subcategories)

Controls

Identification of controls that mitigate risks

LoD1 – First Level Controls: Operational/ Hierarchical controls

LoD2 – Second level controls: carried out by the independent and dedicated teams

LoD3 – Third level controls: internal audit/ inspection

Data

Data quality for a resilient permanent control framework

Confidentiality / Security

Integrity

Availability

Traceability

Holistic Information System for Risk and Control Management

RCSA at the Process level

Adequate resources with defined roles and responsibilities

Comprehensive normative framework

GOVERNANCE, MONITORING, REPORTING & CONTINUOUS IMPROVEMENT

ACTORS : BUSINESS UNITS /SERVICE UNITS OF WHICH LOD2 FUNCTIONS RISK, FINANCE, COMPLIANCE

2. Our solutions

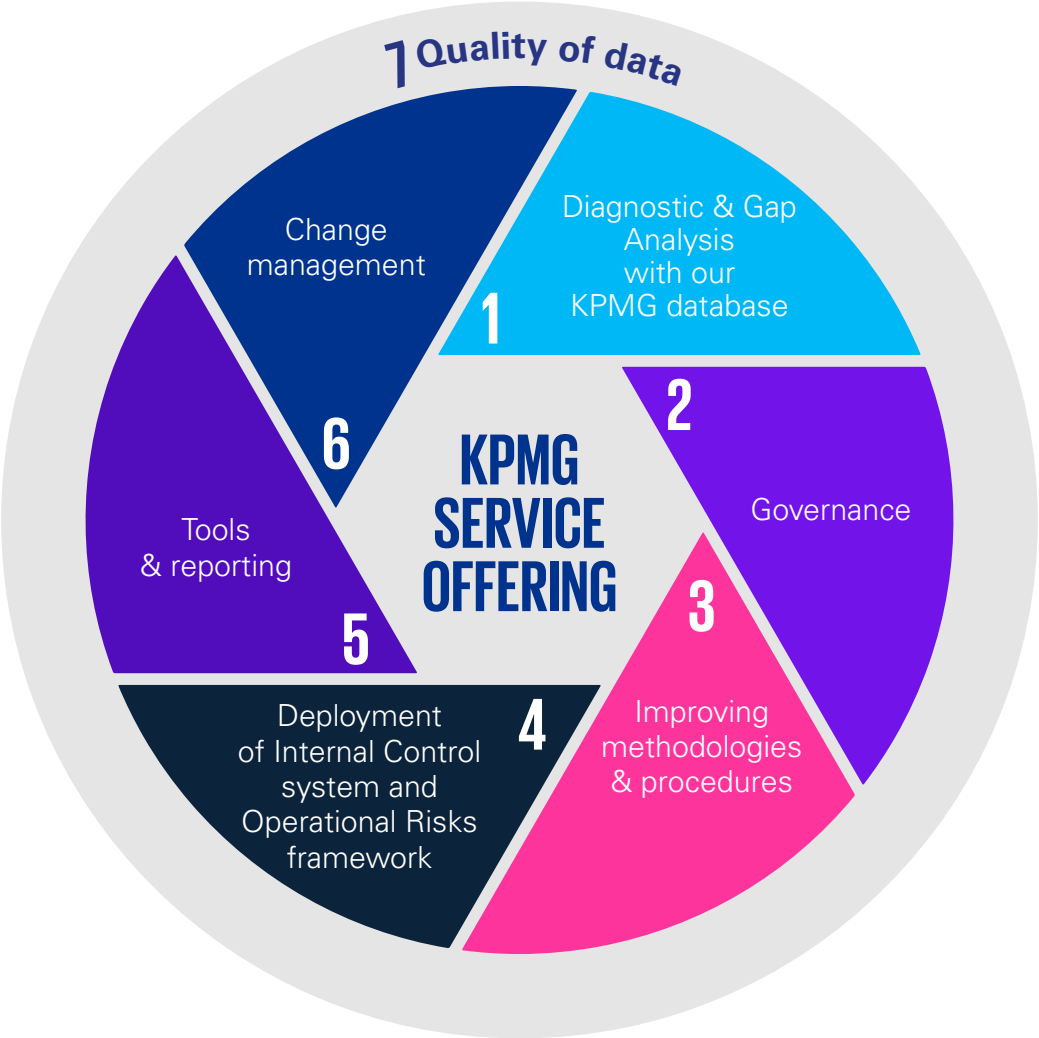
KPMG experienced teams can support you in all aspects of permanent control and operational risks management. KPMG is the choice of a major player to accompany your internal & permanent control programs.

KPMG is involved with the entire financial industry in France and internationally in a pragmatic and operational approach. KPMG has developed a **database** of activities, processes, their main tasks, operational risks and controls covering all businesses and functions of a universal bank.

This database contains **200 Activities**, over **500 Processes**, a risk taxonomy and over **2000 controls** to mitigate these risks.

KPMG through its regulatory watch centers of international network continuously update its practices and database.

KPMG is recognized by the largest and middle-sized players in the financial services sector and brings you its expertise on all of your internal control themes. We adapt our intervention to your unique needs and challenges, with a view of continuous quality.



1. Permanent control diagnosis and gap analysis

- Workshops with you to review your institution's **regulated/non-regulated activities/processes.**
- **Diagnosis:** comparison of your risk and control framework covering your activities with our KPMG database (Activities, Processes, Risks, Controls) in order to identify areas for improvement.

- Diagnosis of operational risk mapping and assessment of the impact of the Basel IV reform.

Examples of missions carried out

- For a medium-sized French corporate and investment bank, diagnostic of the operational risks cartography and the risks to controls mapping by activity using our KPMG database.

- For a major French bank, review of the permanent control and operational risk management framework and support of its improvement.

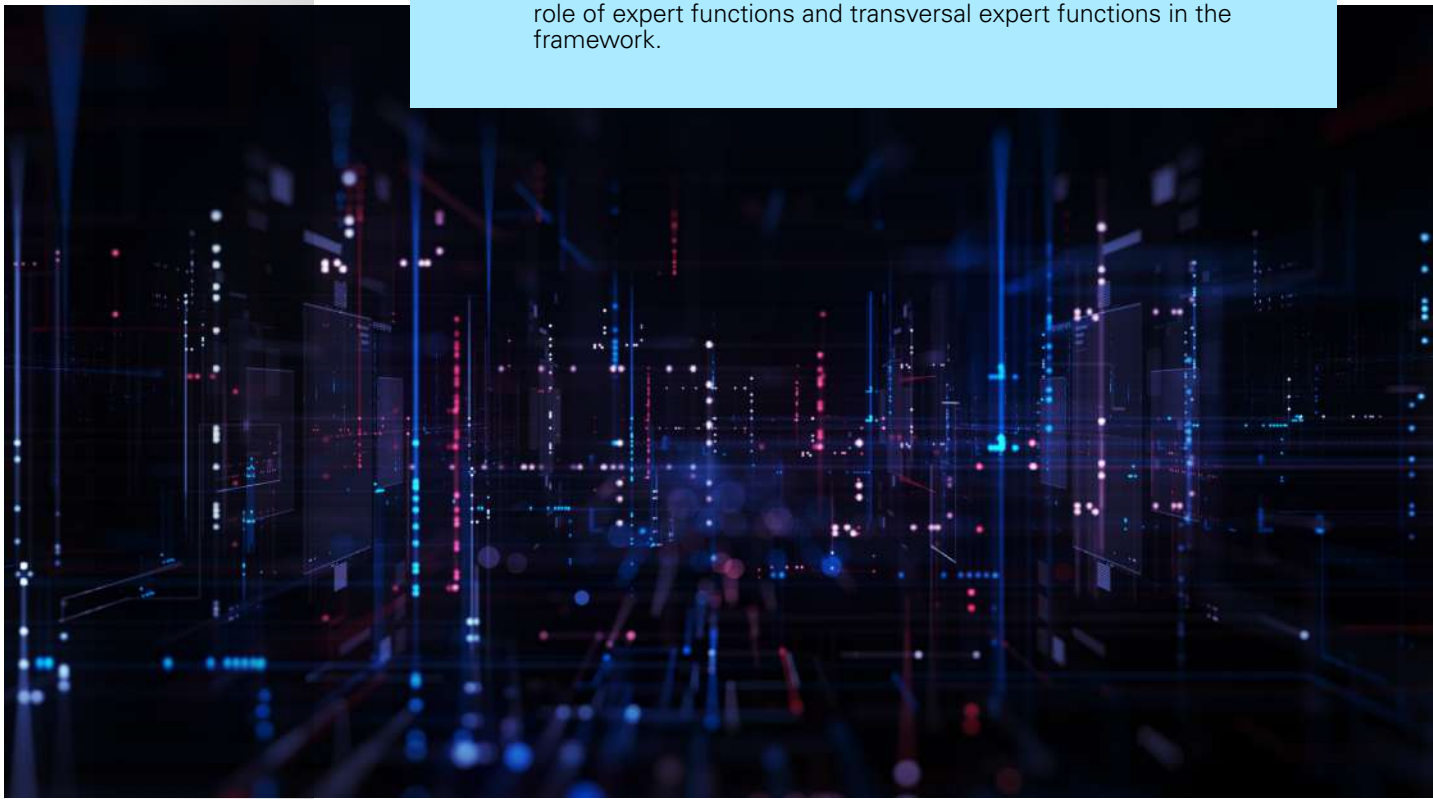
- Gap analysis of the governance and permanent control framework of a major French bank with SREP expectations.

2. Governance of permanent control

- Definition and deployment of **the organisation and governance** of the permanent control framework (RACI, TOM, comitology, etc.).

Examples of missions carried out

- For a major French bank, definition of the target operating model for permanent control and deployment within the bank's business lines and functions. Definition of the roles and responsibilities of the first / second lines of defence, as well as the role of expert functions and transversal expert functions in the framework.



3. Improving permanent control methodologies

- Definition and implementation of LOD1/LOD2/LOD3 control methodologies, non-financial risks management, repository management, continuous improvement process, control delegations, outsourcing.
- Support in reviewing and updating procedures (incident management, RCSA/risk mapping, operational resilience, etc.).

Examples of missions carried out

- Definition of a systematic methodology for building a multi-year 2nd level control plan for a major French banking group, and backtesting of the methodology with available resources.
- Documenting normative procedures on 1st/2nd level controls, and upgrading of existing procedures.

4. Deployment of the internal control framework

- Deployment of the **permanent control framework to the business lines and functions** using the Activities, Processes, Risks and Controls (APRC) approach.
- Support for the design and implementation of **deployment strategies** across all functions and business lines.
- Aligning **the permanent control and risk management frameworks,** as well as the Risk and Control Self Assessment (RCSA).

Examples of missions carried out

- Support a major French banking group in remediating its permanent control and operational risk management framework following an ECB inspection, and deployment across all its business lines and functions.
- Assisted a major French banking group in defining and rolling out its permanent control transformation program.
- Assisted the General Management office of a major French banking group in rolling out its permanent control framework to the General Management office and the heads of business lines and functions.

5. Tools, automation & reporting

- Implementation of an integrated **permanent control tool** covering the following dimensions in particular: organisation/hierarchical levels, procedures, activities/processes, risks and controls, with granular and consolidated Business Intelligence reporting capabilities.
- Integration of the various modules to build a **holistic GRC** tool (external incidents, recommendations, action plans, etc.),Third Party Risk Management TPRM, operational resilience, RCSA, etc.).
- Implementation of a **control automation solution** for the first and second lines of defense.

Our control automation solution (KAS tool)

KPMG's control automation solution delivers significant benefits in terms of agility, reusability and standardisation. Based on a manual, dispersed and heterogeneous control environment, KPMG has identified, ordered, designed and automated more than 300 independent logics, which, combined, address and improve the effectiveness of individual control objectives, as well as achieving a global, unified, interlocked and homogeneous internal control environment.

Examples of missions carried out

- For a major French bank, digitisation of the Level 2 Permanent Control Risk function to optimise the workload and automate certain tasks.
- For a medium-size bank, construction of a tool for consolidating risk cartography and automated reporting, in conjunction with the RAS/RAF.

6. Change management

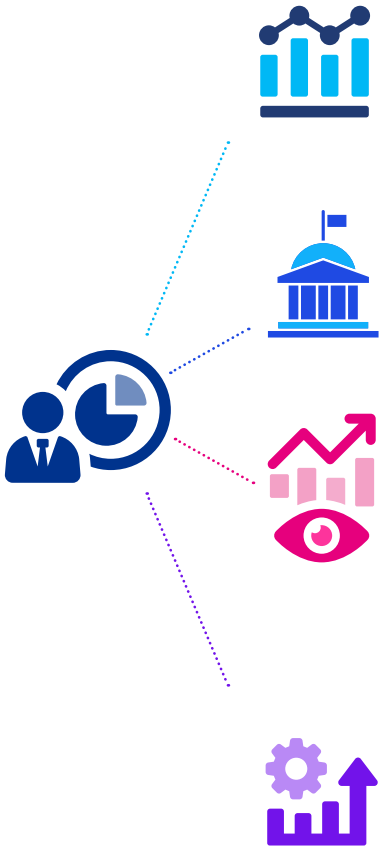
- Strengthen and spread the risk culture within financial institutions by setting up an exchange and sharing framework at every level of the organisation, as well as a measurable and pragmatic operational model.
- Conduct investigations in case of **realized operational/IT risks incidents**, before or in addition to missions carried out by the supervisory authorities.
- Support with a change management framework : training seminars, e-learning, knowledge chatbots, internal and external communications.

Examples of missions carried out

- For a medium-size bank, creation and delivery of training materials on risk assessment, internal/external fraud awareness and IT security.
- Assisted a major banking group with its permanent control remediation plan.
- Change management and support in the deployment of recommendations.

7. Our offer on GRC tools and D&A

The digitisation of controls is based on a continuum of technological solutions addressing different automation needs.



- **Data preparation**
- **Integration of no/low code and AI components**
- **Generation of dynamic reports (via power BI)**

- **Integration of BCBS239 principles: data governance, data architecture, data lineage, reporting**

- **Process analysis and automation via Robotic Process Automation**
- **KPMG control automation tool**
- **Ongoing supervision via KPIs**

- **Integration of the various modules to build a holistic GRC tool**
  1. **Formalisation of activities, processes, execution of the RCSA and assessing controls,**
  2. **Identification of losses and incidents,**
  3. **Assessment of residual risks,**
  4. **Recommendations and action plans.**

Taking account of ESG risks and their impact on non-financial risks management and internal control frameworks

Business

- Track record / evaluation of customers and suppliers against ESG criteria
- Credibility of transition plan for customers
- Development of sustainable finance products
- Mitigation of 'greenwashing' / Implementation of a sustainable development strategy
- ESG consulting in supply chain networks
- ESG regulatory due diligence for clients and transactions

ESG RIsks

- Integrating ESG risks into an ESG policy and governance involving the appropriate functions
- Integrating ESG into existing risk management frameworks and processes
- Training on ESG risks & control of 'greenwashing' risk
- 'Net Zero» strategy and supervision of carbon emissions planning

Compliance

- Integration of ESG into existing control procedures
- Product governance - review and validation
- Mitigation, control and monitoring of greenhouse gas emissions
- Support ESG transformation throughout the company
- Supporting the implementation of ESG workstreams
- Internal ESG policy assessments and governance reviews
- Support regulatory watch on ESG regulations

Finance

- ESG reporting and declarations
- Pilar 3 reporting - Green asset ratio
- Taxonomy
- ESG report by the Board of Directors and management
- Carbon emissions planning (financed emissions)
- Companies stress tests and scenario analysis

Group Sustainability

- Definition of a sustainable development strategy / Industry commitment
- Policy guidance and initiatives across the business
- Coordination and monitoring of ESG initiatives across the bank
- Panorama analysis for new ESG initiatives
- ESG ratings and controversies/transition arrangements
- Support for external reporting

NOTES

Contacts

Operational risks & permanent control

Vicky Papaevangelou
Partner
Governance, Risk & Compliance
vpapaevangelou@kpmg.fr

Nicolas Coudrieau
Director
Governance, Risk & Compliance
ncoudrieau@kpmg.fr

BCBS239 - Data

Bertrand Aubry
Partner
Connected Tech
bertrandaubry@kpmg.fr

GRC tools

Pauline Eckert
Partner
Connected Tech
peckert@kpmg.fr

IT Risks

Grégoire Levis
Partner
Connected Tech
glevis@kpmg.fr

ESG regulations

Sylvie Miet
Partner
FSPB
smiet@kpmg.fr

kpmg.fr