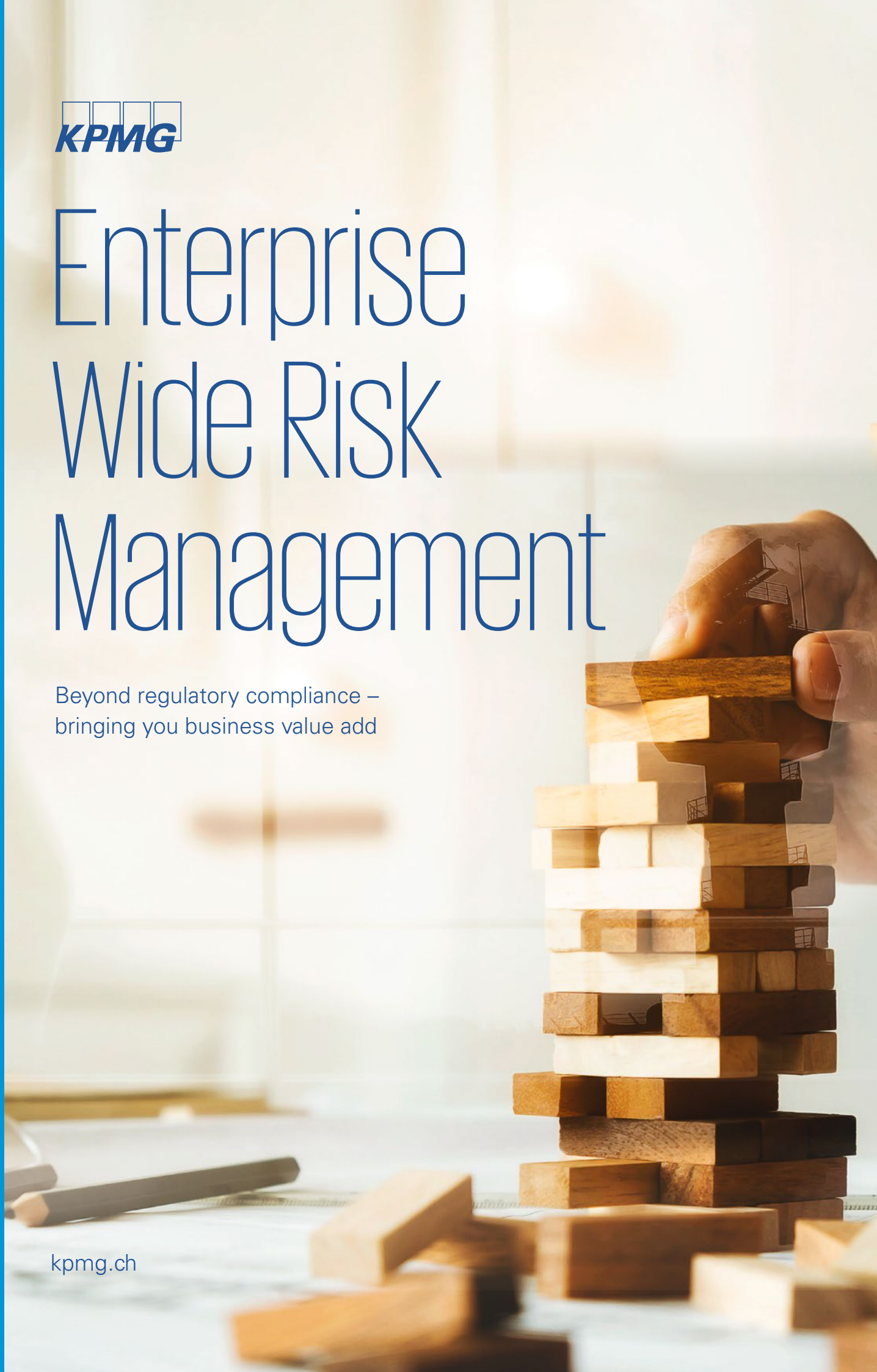
KPMG

Enterprise Wide Risk Management

Beyond regulatory compliance – bringing you business value add



kpmg.ch

Regulatory Background

Following the global financial crisis there has been heightened regulatory attention on corporate governance and enterprise wide risk management, including incorporating a risk appetite framework. Regulators have raised strong concerns on the standards of corporate governance in the banking industry and the FSB, BCBS and the ECB have all issued papers setting out regulatory expectations.

In Switzerland, the FINMA Corporate Governance Circular 2017/1, comes into force on 1 July 2017, and has far reaching requirements for corporate governance, risk management and the internal control system. In particular, the Executive Board must develop an **Enterprise Wide Risk Management ("ERM") Framework** which must be approved by the Board of Directors. The Framework should:

- Establish the risk tolerance and risk limits, ensuring they are embedded in the business strategy and BaU processes;
- Define the organizational structures and tools that will be applied to identify, analyse, evaluate, manage and monitor the key risk categories; and
- Include provisions on risk data aggregation and reporting.

There is much to do to meet these requirements and regulatory expectations.

So what's the impact?

Most banks will already have certain aspects of an ERM Framework in place. However, in order to allow the Board to fully discharge its new regulatory responsibilities, a step change in comprehensive structured, enterprise wide risk management is necessary. Below we set out three examples of ERM Framework components which banks are finding challenging.

	Example Best Practice Indicators	Key Challenges
Risk Appetite statement	• Well defined triangulation process between the risk appetite statement (RAS), strategic, capital and funding planning • RAS is integral to the bank's strategic objectives and foundation of the ERM Framework, so that the bank operates within this appetite	• RAS is "standalone", not reflective of business, nor embedded • Lack of quantitative metrics or qualitative expectations/ behaviours • Risk limits determined "bottom up", lack of "top down" guiding principles and/or set at wrong level • Lack of calibration to stressed conditions
Three Lines of Defence model	• Clear & consistent understanding and demarcation of roles & responsibilities between and within 1LOD and 2LOD across regions/businesses • Ability to demonstrate and evidence 1LOD risk ownership and proactivity in identifying issues, and 2LOD challenge • Consistent approach to control ownership and testing • Transparency of key processes and controls, front to back, resulting in no duplication	• Lack of clarity/duplication of responsibilities across LODs • Inappropriate balance of activities between 1LOD (accountability & ownership), and 2LOD (challenge) • 1LOD process or skill gaps leads to 2LOD discharging 1LOD role. • 2LOD too far removed from business to give sufficient challenge • Lack of front-to-back understanding of process and controls
Risk Data Aggregation	• Based on BCBS 239 • Comprehensive data governance for risk data including data owners from business and IT • Risk data models unified or automatically reconcilable across banking divisions with unified naming conventions • Risk and accounting data is reconciled • Effective data quality management including automated measurement methods and escalation procedures • Comprehensive, timely, reliable and adaptable risk reporting capability across all units and all material risks, with drill down capability • Risk reporting and aggregation mapped into IT strategy	• Lack of uniform naming convention (e.g for legal entities, customers & accounts) • Conflicting legal entity v management views • Risk data in reporting is not flexible or capable of being analysed bank-wide in all "relevant" dimensions • Difficult to speed up reporting without impacting accuracy • Inability to increase frequency of analysis in times of crisis • Lack of metrics or KPIs on data quality • High amount of manual steps in processing and reporting processes. Numerous uncontrolled manual interventions. • No defined approach to automatic and manual adjustments and quality controls in the reporting process • Lack of simulations or scenarios for the most important markets and risk parameters.

What does a good ERM Framework look like?

1 Risk Governance

Committee Structure and Authority
- Board and Board Risk Committee
- Mandate + delegated authorities

Holistic approach
- Risk Management philosophy and key principles
- Link to strategic planning capital + funding frameworks

Risk Culture, Values and Behaviours
- "Tone at the top"
- Reward and Remuneration
- Transparency and disclosure

Risk Appetite Statement
- Key Risks
- Risk Bearing capacity
- Risk Tolerance and Limits

Risk Framework + Key Risk Policies
- Approve ERM Framework
- Risk Policy Framework & Hierarchy

2 Risk Oversight and Control Function

- CRO mandate and organisation
- Stress testing and resilience
- Review, challenge, reporting & escalation
- Framework & policy oversight and maintenance
- Model Validation and Approval
- Enterprise wide view and aggregation

3 Risk Operating Model
- 3 lines of defence
- Demarcation of roles and responsibilities
- Independence and objectivity

4 Risk Management
- Identification
- Assessment
- Measurement
- Response & Mitigation
- Control & Monitor

5 Portfolio Review Optimisation and Pricing
- Risk approval & underwriting
- Risk return & optimisation

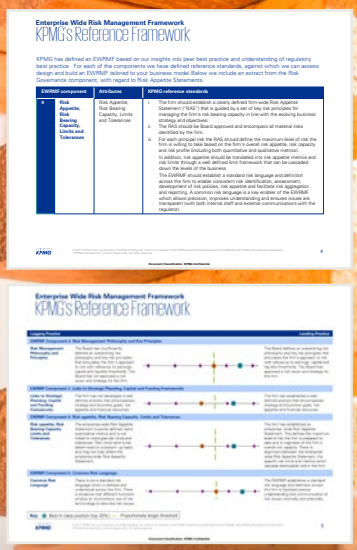
6 Contingency Planning and Resilience
- Contingency Planning
- Resilience testing
- Franchise protection

7 Risk Data Aggregation, Infrastructure and Reporting

- Board and management reporting
- Enterprise wide view & aggregation
- Common risk language/risk taxonomy
- BaU and stressed

How can we help?

- KPMG has designed **a best practice comprehensive ERM Framework** comprising of 7 key components based on our in depth market understanding and risk management knowledge.
- For each of the components we **have detailed expectations of what is required** and **a clear view of leading and lagging practice.**
- Our **deep risk management understanding** and knowledge of regulatory expectations, coupled with **practical, hands on advice** means we can support you in designing an ERM Framework, **tailored to your business operating model** – this is not a one-size-fits all approach.
- Working together to implement and **embed the framework sustainably** in BaU, we will support you to close skill and capability gaps, upgrade technology enablers, and evaluate right sizing options.
- We go beyond regulatory compliance, bringing you **real business value add.**



Engage & Understand → **Gap Assessment** → **Design** → **Implement & Embed** → **Continuous Improvement**

Our Team:

Highly experienced dedicated risk management professionals

- Risk management is what we do – it's in our DNA
- We know what good looks like, what works and what doesn't
- Leveraging from our deep experience means we can help you avoid pitfalls and challenges
- We will understand your business model and tailor our approach accordingly

Access to industry expertise and benchmark information

Ready to go tools to identify impacts and solutions

Deep experience to accelerate progress

Innovative ideas to bring new perspectives

Contacts

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch

Helen Campbell
Partner
Head Financial Risk Management
Financial Services
+41 58 249 35 01
hcampbell@kpmg.com

Reto Gareus
Director
Financial Services

+41 58 249 42 51
rgareus@kpmg.com

Matthias Degen
Director
Financial Services

+41 58 249 40 36
mdegen@kpmg.com