# *Redefining the risk management and internal control system requirements* – the new FINMA circular on corporate governance

The Swiss Financial Market Supervisory Authority FINMA published on 1 November 2016 its new circular 2017/1 'Corporate governance – banks', consolidating the FINMA's requirements relating to corporate governance, risk management and internal control systems.

## The new requirements should not be underestimated

The new FINMA circular 2017/1 consolidates the provisions of circular 2008/24 ('Supervision and internal control – banks') along with the related FAQs and the requirements defined in other circulars. In the process, FINMA has also revised circulars 2008/21 ('Operational risks – banks') and 2010/1 ('Remuneration schemes').

These new and modified circulars incorporate the most recent findings from the financial crisis and developments in international standards. The revised circulars were published on 1 November 2016, taking into account comments raised by the industry during the consultation period, and will enter into force on 1 July 2017.

### Principles-based regulation

FINMA is streamlining its regulatory framework by defining the revised requirements in terms of underlying principles. The principle of proportionality is embedded in the revised requirements, allowing institutions to implement the requirements in a way that takes into account their specific business models and risk profile.

### Modern corporate governance requirements

The new 'Corporate governance – banks' circular underlines the importance of modern corporate governance and sets minimum requirements relating to the composition of the Board of Directors and the qualifications of its members, corporate governance disclosures and, more extensively, the development and implementation of a comprehensive risk management framework and internal control system.

We believe that the enhanced requirements in the area of risk management and the internal control system will require changes to existing organisations. They will be challenging to implement but, at the same time, will allow institutions to enhance risk culture and the awareness of controls throughout the organisation.

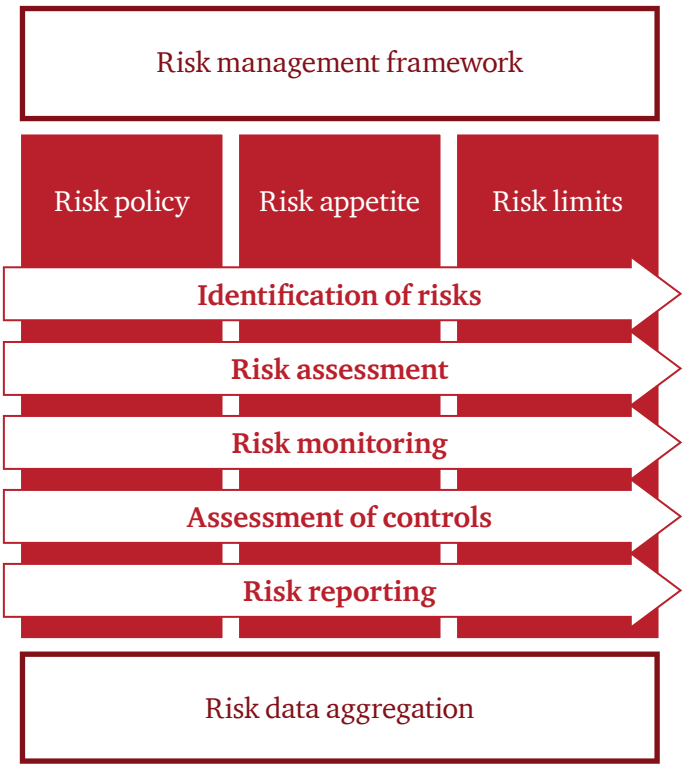
pwc

# 1 Risk management framework and Board of Director oversight

According to the FINMA circular, all banks must implement a comprehensive *risk management framework*.

The framework is an overarching document that covers a bank's risk policy, *risk appetite and risk limits*. Furthermore, banks must describe the tools and the organisation they have implemented to identify, assess, monitor and report the defined risks within each risk category.

The Board of Directors needs to evaluate and approve the risk management framework annually. Approval by the Board of Directors goes further than merely confirming adherence to the purely formal aspects. The key to an effective risk management framework is the ability to assess whether the framework is *effective*.




## Key questions…

- Have you identified and documented all the risks relating to the activities undertaken by the institution?
- Have you set and documented your risk appetite with regard to the activities?
- Has the risk appetite been defined through a set of limits and key indicators?
- Do your existing processes, policies and procedures constitute a comprehensive risk management framework? Are they documented?
- Does your organisation have adequate controls in place to manage those risks?
- Are the controls documented? Do you assess their effectiveness on a regular basis?
- Does your Board of Directors receive timely, concise and complete risk and internal controls reports to ensure the risks undertaken are in line with the appetite and to enable challenges and decision making?
- Does your risk identification and assessment process ensure the timely identification of new risks?

# 2 Implementation of the controlling bodies

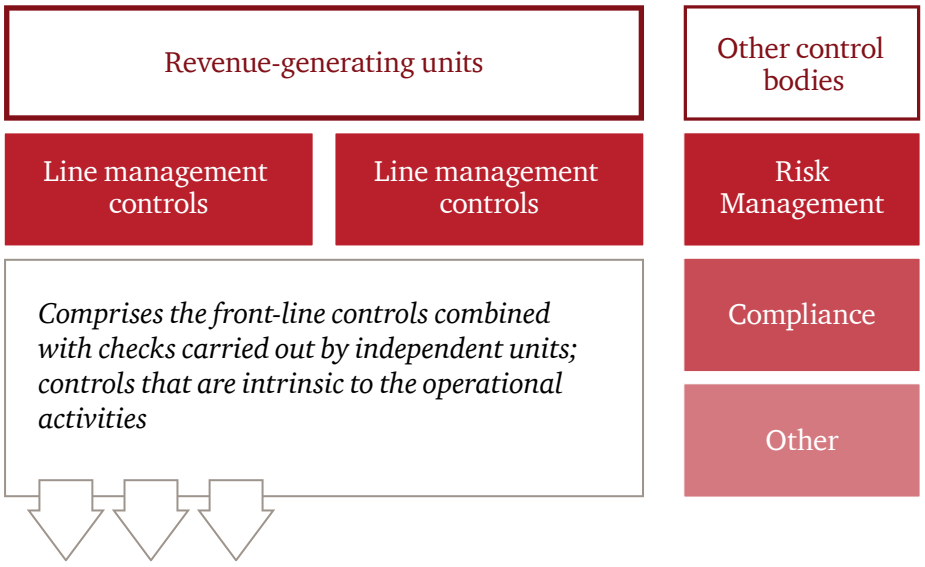
Within the internal control system, banks will need a minimum of two lines of control: the *revenue-generating units* and the *independent control bodies*. Banks, in fact, are expected to implement the 'three lines of defence' model –based on front-office controls, support functions/back-office controls and internal audit – which is an internationally recognised standard.

## Revenue-generating unit controls

The objective of controls in the revenue-generating units is to ensure that the front office takes ownership for the risks it undertakes. This requires controls to be in place that ensure adherence to the bank's internal guidelines and regulations, including responsibility for being in line with the bank's risk strategy. The banks' incentive schemes should encourage the revenue-generating units to manage risks effectively and within the set rules. A consequence-management process should be defined to properly deal with exceptions.

## Independent control bodies

The independent control bodies monitor risks as well as compliance with the internal guidelines and the legal and regulatory requirements. Typically, the independent control bodies are defined as the 'Risk Management' function and the 'Compliance' function.




### Key questions …

- How do you differentiate between the revenue-generating unit controls and the independent control bodies?
- Have you defined and documented controls in the revenue-generating units (1st line of defense)?
- Who owns the controls in the revenue-generating units?
- How do you monitor and report on the controls in the various control bodies?
- Is the incentive scheme aligned with the risk appetite?
- Is there a formal process to deal with exceptions (consequence management)?

# Contacts

PwC
Birchstrasse 160
Postfach, 8050 Zurich

**Andrin Bernet**
Partner
andrin.bernet@ch.pwc.com
+41 58 792 24 44

**Yousuf Khan**
Senior Manager
yousuf.khan@ch.pwc.com
+41 58 792 15 62

**Alena Nicolai**
Senior Manager
alena.nicolai@ch.pwc.com
+41 58 792 27 28

**Alexandra Burns**
Senior Manager
alexandra.burns@ch.pwc.com
+41 58 792 46 28