Enterprise Risk Management Framework: What does good look like?

Swiss Risk Dinner

Helen Campbell

12 June 2017

Agenda

Regulatory Context

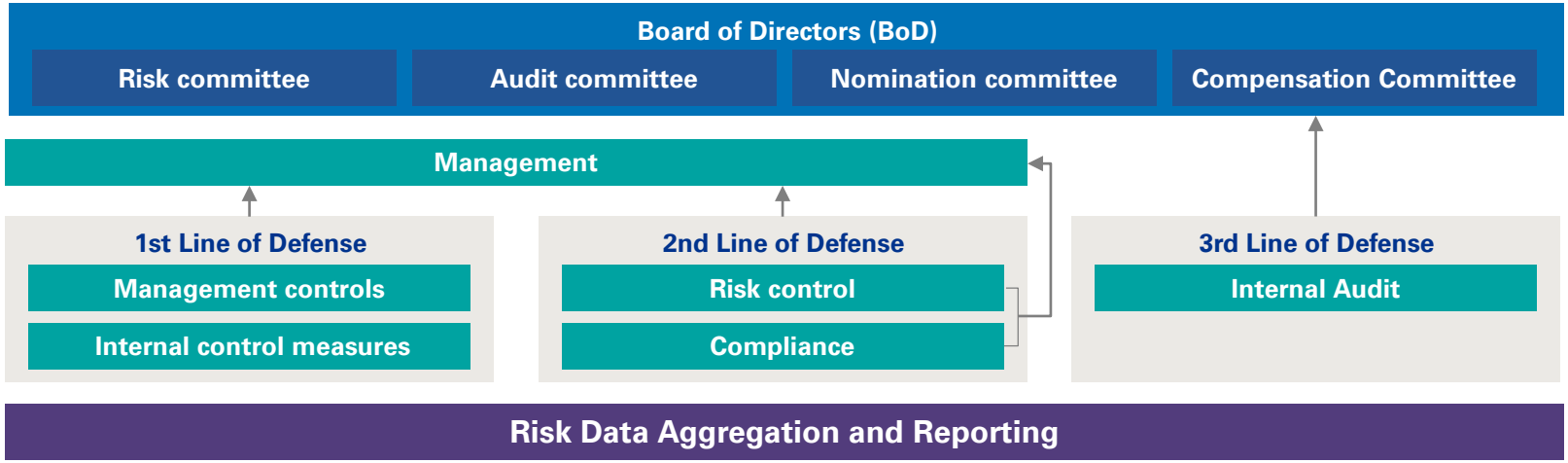
The FINMA Corporate Governance Circular 2017/1 (the "Circular"), comes into force on 1 July 2017, and has far reaching requirements for corporate governance, risk management and the internal control system of banks.

The requirements and expectations of the regulator have significantly increased in this regard for all banks, with a focus on:

- Specific Board responsibilities on business strategy and risk policy, and ensuring there is an effective internal control system and appropriate risk and control environment;
- Applying a comprehensive structural concept to risk management through the mandatory establishment of an enterprise wide risk management framework; and
- Establishing an effective and comprehensive 3 lines of defence system, with specific responsibilities of the risk, compliance and internal audit functions.

In addition there are specific additional requirements for Tier 1-3 Banks, such as

- Establishing a Risk and Audit Committee, comprising of a majority of members who are independent, having an independent risk control function headed by a CRO, and risk data aggregation and reporting considerations.



Regulatory Context

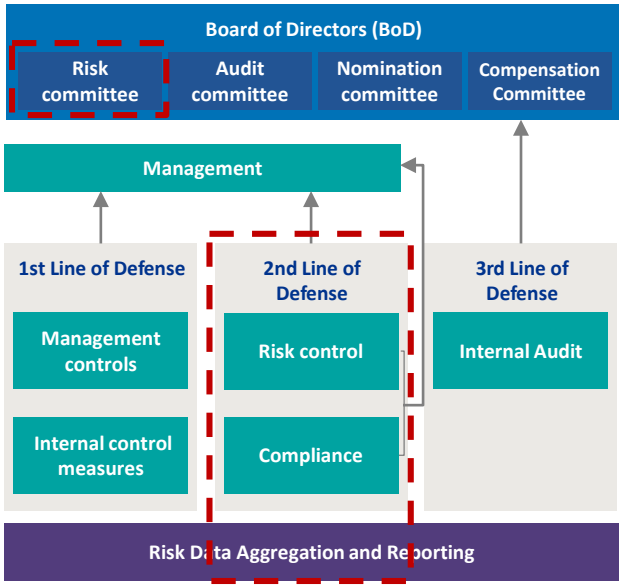
Some of the most far reaching requirements are focused on risk management and can be summarised in 3 areas:

1) Specific Board Responsibilities

2) Enterprise Wide Risk Management Framework

- Identifies key risks and potential losses
- Establishes the risk tolerance and risk limits, and documentation to verify this;
- Defines the organisational structures and tools that will be applied to identify, analysis, evaluate, manage and monitor the key risk categories; and
- Includes provisions on risk data aggregation and reporting. `

3) Independent Risk Control function



So what does this mean in practice?

What does good look like?

Key implementation challenges

1 Risk Governance

Committee Structure and Authority
- Board, Board Risk and Exec 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 & disclosure

Risk Appetite Statement
- Key Risk identification
- Risk Bearing capacity,
- Risk Tolerance and Limits
- Qualitative & Quantitave Metrics

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

2 Risk Oversight and Control Function

- CRO 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

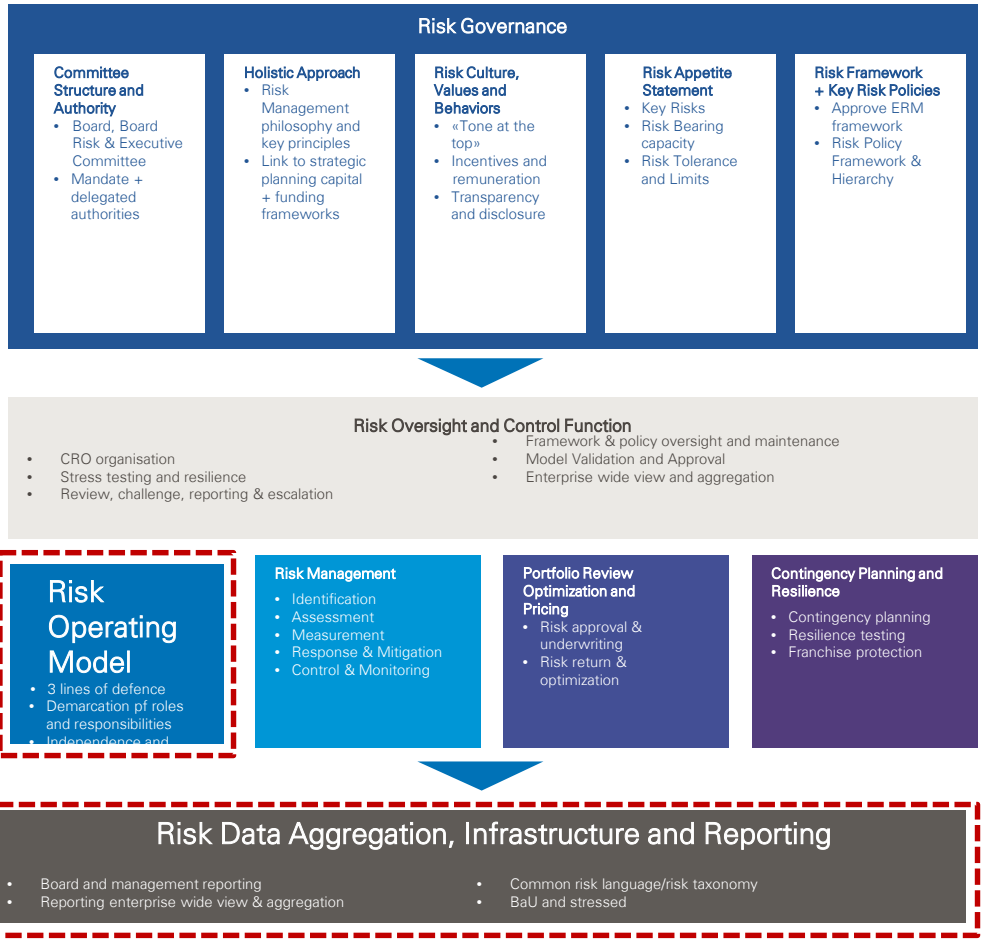
5 Portfolio Review, Optimisation and Pricing
- Risk Approval & Underwriting
- Risk Return & Optimisation

6 Contingency Planning and Resilience
- Contingency Planning
- Resilience Testing
- Franchise Protection

7 Risk Data Aggregation, Infrastructure and Reporting

- Board and Management Reporting
- BaU and Stressed
- Common Risk Language/Risk Taxonomy
- Reporting Enterprise Wide View & Aggregation

Implementation Challenges



Key Challenges – Risk Operating Model

- **Balance of activities between 1st v 2nd LOD**
  - Lack of clarity /duplication of responsibilities and front-to-back process & control transparency
  - Inappropriate balance of activities between the 1st (ownership) and 2nd line (challenge)
  - 1st line process or skills gaps lead to 2nd line discharging 1st line role;
  - 2nd line to far removed from the business to give sufficient challenge
- **The trend towards Line 1.5**
  - Roles & tasks
  - Impact on 2nd line

Key Challenges – Risk Data Aggregation & Reporting

- **Global regulatory context (BCBS 239)**
  - Data governance and data quality framework
  - Data ownership
  - Data aggregation – common data dictionary
- **Board and management reporting**
  - Holistic view – financial & non financial
  - Getting the balance right – quantitative v qualitative
  - Speed v Quality

Business value add

Drive disciplined risk taking

Ensuring new business, product development, and pricing reflect risk capacity and appetite

- Meaningful definition of the risk strategy, risk appetite and risk tolerance translated into enforceable operating limits
- Appropriate use of risk measures to steer key business critical decisions

Achieve more with less

Optimizing use of resources and talent

- Efficient implementation of the 3 lines of defence concept, clarification of respective roles, and elimination of functional silos
- Focus resources on highest residual risks

Turn data into insights

Gaining a competitive edge through a superior understanding of risks and opportunities

- Effective governance of data, improving data quality underpinning business critical decisions
- Transparent and complete Management Information on risk levels, including forward looking indicators and ability to slice and dice

Q&A

Questions ?