Chapter 15

Governance and Organisation

The aim of this chapter is to show one possible governance form for an effective risk management. It is to be noted that there are many different forms of organisational principles and that the concrete implementation needs to reflect the needs of the company.

15.1 Governance

In this section the aim is to define a segregation of duties needed to provide effective risk management.
15.1.1 Definitions

In order that everybody speaks a common language and to avoid misunderstandings with the aim to anchor an adequate governance within the company it is necessary to define some roles and functions as follows:

**Risk owner:** Executive committee, through setting limits and appetite for risks and approving risk policies & governance, owns the risks, through the delegation of authority and responsibility for these risks through the company’s management processes.

**Risk taker / Line Management (1st line of defence):** The business functions (Products / Operation / Distribution), through writing business and implementing the risk policies and governance framework as well as management controls, take risks. In addition, corporate functions take risks, eg. finance through its balance sheet and control management activities.

**Risk controlling & reporting (2nd line of defence):** The risk specialist functions, through identification of emerging issues, creation of risk policies, review of the risk taking activities of the business functions, provision of management information and consolidated risk committee / executive committee reporting, perform core controls in the risk management process. The Chief Risk Officer, through periodical review of any part of the risk assurance matrix as he deems appropriate, performs additional controls.

**Independent assurance (3rd line of defence):** Internal audit, through their audits of process and policy compliance by both business functions and risk specialists, provide independent (from management / risk committee) assurance that framework is complied with.

**Risk Policy:** The risk policies are governance documents with the aim to ensure that an adequate risk framework is in place for a certain type of risk. These documents are prepared by the risk Management function (second line of defence) and they are adopted by the Risk Owners. risk policies are published by the Chief Risk Officer. The company sets the risk appetite for the business. For most of the policies the implementation is the responsibility of the Line Management.

**Policy Owner:** The policy owner is the manager within the first line of defence who is responsible for the corresponding policy.

**Policy Coordinator:** The policy coordinators act on behalf of the policy owner and ensure the implementation of the corresponding policy in the business.