

6.1 Definition

Operational risk is the risk of losses owing to

- deficient or erroneous internal procedures and processes
- human or system errors
- external events, including legal events

Operational risk is thus often associated with specific and one-off events, such as failure to observe business or working procedures, defects or breakdowns of the technical infrastructure, criminal acts, fire and storm damage or litigation. Operational risks are thus non-financial risks.

6.2 Basis of operational risk management

The Executive Board has appointed an Operational Risk Committee. This Committee assists the Executive Board in its functions and processes in relation to operational risk management. The Committee is chaired by a member of the Executive Board.

The primary tasks of the Operational Risk Committee are described in detail in the committee charter, which must be seen in conjunction with the operational risk policy. The tasks include the following:

- Identifying, monitoring and managing the Group's current and potential operational risk exposures.
- Handling "critical exposures" which the managements of business areas or the Committee itself considers to be of a nature that requires further follow-up and reporting.
- Following up on reviews by and reports from financial supervisory authorities, and informing the Executive Board of the current situation in areas affecting the Group's operational risks.
- Following up on reports prepared by Internal Audit, and informing the Executive Board of unusual circumstances.
- Preparing management information on issues such as IT security, physical security, business continuity and compliance.

In addition to the operational risk policy, the following policies have been defined for the business and support areas:

Security policy	Specifies the Group's procedures within the areas of IT, information and staff safety. Defines the security framework for the Group's IT systems to maintain the desired security level for customer-sensitive information. Determines requirements for third-party suppliers working for the Group within these areas.
Control policy	Ensures that the Group has a strong control organisation where good management can be demonstrated through compliance with internal control standards.
Compliance policy	Ensures that all the Group's activities always meet internal and external requirements, including legal and ethical standards. Compliance officers are placed in the local business areas. They are independent of the areas and report to Group Compliance.

The Group also has policies regulating other operational risk areas, such as an insurance policy, an outsourcing policy and an auditing policy. Each business area is in charge of the day-to-day monitoring of operational risks and is responsible for mitigating losses resulting from such risks. Resource area staff provides support to business areas as part of the Danske Banking Concept.

6.2.1 Measurement and control

The measurement and control framework comprises four qualitative elements:

- Risk identification and assessment that ensure that all key risks are effectively highlighted for group-wide transparency and management. This enables the Group to focus on fewer but more fundamental risks.
- Monitoring of key risks. This is an ongoing process that ensures that an unfavourable development in such risks is consistently highlighted on a group-wide basis.
- Risk mitigation strategies and implementation processes that ensure that key risks are reduced and establish transparency in these strategies and processes.
- Follow-up on loss data and events.

All material operational losses are commented on and registered. Since 2001, the Group has captured data on about 4,400 events involving losses in excess of DKr25,000.

For several years, the Group has also collected loss data directly from the Group accounting system to calculate the total sum of losses below the limit. Such losses are recorded as “expected losses”.

The Group participates in the international Operational Riskdata eXchange Association (ORX) founded to allow the participating banks to exchange observations on operational losses. Data on losses exceeding €20,000 are exchanged quarterly, and ORX has collected data on more than 30,000 events since 2003. Finally, the Group subscribes to Fitch Ratings’ public loss database.

6.2.2 Calculation of capital requirements

The calculation of capital requirements in accordance with the standardised approach under the CRD is based on one indicator: core income. The Group calculates its capital requirements by multiplying the core income of the individual business activities by the weights determined by the CRD. The aggregate capital requirement for the Group is the sum of the capital requirements for the various business activities.

The Group’s business areas have therefore been divided into the eight business activities specified by the CRD:

- corporate finance
- trading and sales
- retail brokerage
- commercial banking
- retail banking
- payment and settlement
- agency services
- asset management

As of 2008, the Group uses the standardised approach under the CRD rules for calculating risk-weighted assets. The Group intends to apply to the Danish FSA for approval for using the Advanced Measurement Approach (AMA) within the next few years.