



# Application for Standardised Approach, operational risk

February  
2008

## General information concerning the notification process

This document contains Finansinspektionen's requirements regarding the format of a notification to use the Standardised Approach for operational risk.

An institution that intends to use the Standardised Approach for operational risk shall file a notification with Finansinspektionen before the institution begins using the method.

In the Capital Adequacy and Large Exposures Act (2006:1371), Chapter 6, section 4, it states that an institution which uses the Standardised Approach shall:

1. based on written guidelines and instructions which are reviewed regularly, divide the operating income or the calculation basis which corresponds to the operating income into different business areas in an appropriate manner; and
2. possess an appropriately structured risk management system for operational risks which fulfils the requirements set forth in Chapter 6, sections 2 and 5 of the Banking and Financing Business Act (2004:297) and Chapter 8, sections 4 and 8 of the Securities Market Act (2007:528).

Which further measures an institution shall take in order to fulfil these requirements are outlined in Finansinspektionen's regulations.

A financial group shall submit an application which covers the institutions constituting the group on both a consolidated basis and an individual basis. Below, we refer to the institution as "notifier", but for those institutions which are included in a financial group, the application is accordingly submitted on a consolidated basis.

Those undertakings wishing more information concerning operational risks and the control and management thereof are referred to the following documents:

- The Financial Supervisory Authority's general guidelines (FFFS 2005:1) regarding governance and control of financial undertakings, [www.fi.se](http://www.fi.se), which contain general recommendations concerning risk management.
- The Basel Committee on Banking Supervision's "Sound practices for the management and supervision of operational risk" (February 2003), [www.bis.org](http://www.bis.org), which contains recommendations regarding the manner in which management, control, and monitoring of operational risks should take place.

## Formulation of the notification

### *Format*

It would be appreciated if the completed application and attached documents were submitted, as far as possible, in an agreed electronic format.

The responses should be formulated such that they, together with references and attached documents, can be used by the Financial Supervisory Authority to process the application.

### *Language*

The institution can respond to questions in either Swedish or English. The regulations and the notification form will be translated into English. This is done to facilitate the notification of foreign branches and subsidiaries and to make possible efficient cooperation with foreign supervisory authorities.

### *Attached documents*

At several points in the notification, the institution is asked to attach documents that prove compliance with the section. The institution need, of course, attach a document only once. Where the institution is asked to attach a document which has already been attached under another section, simply refer to the relevant portion of the already attached document. When the response is to be found in an attached document, it is important that the institution refer to the exact section of the document.

### *Information about the institution/group*

As previously described, a financial group need submit only one application encompassing the entire group, both on a consolidated basis and on an individual basis. The notification must set forth those legal entities which constitute the financial group. Moreover, the Managing Director of each legal entity and, where applicable, the Managing Director for the group, must sign the application. This must be set forth in the enclosed table or other appropriate manner. Copy or expand the table if the number of lines provided is insufficient.



## NOTIFICATION

The structure of the institution's notification should conform to the format set forth below. References are to sections circulated for comment concerning Finansinspektionen's regulations and general guidelines regarding capital adequacy and large exposures, Section F Operational risk, dated 17 November 2006.

### **Business line mapping**

*Chapter 3, section 2, subsection 7*

*The institution shall have policies and instructions and documented criteria for mapping the activities and relevant indicator to the relevant business lines. These policies, instructions and criteria shall be continually reviewed by an independent audit function. The criteria shall be updated regularly and adjusted for new and changed business activities, products, and risks. The policies and instructions shall be approved by the Managing Director of the institution.*

### Questions

1. Describe the process by which the institution has determined the mapping of the activities and the relevant indicator.
2. Who has decided on this mapping?
3. How is this mapping reviewed?
4. How often and when does review occur?
5. How well does the mapping accord with the opportunity to capture the relevant indicator in the activities which are mapped into the respective business lines?
6. Which activities are of a common nature or support several activities?
7. How are these activities mapped?
8. Are there instructions in place regarding approval of new or changed activities, products, and risks?
9. How has the mapping been handled in respect of new or changed activities, products, and risks?
10. Is the financial reporting adjusted such that it is possible to capture the relevant indicator when calculating capital adequacy?

### Request for materials

Attach the relevant policies and instructions.

**Policies and instructions**

*Chapter 3, section 2, subsection 1*

*The institution shall have policies and instructions which have been approved by the board of directors for the handling and evaluation of the institution's exposure to operational risks, and which also include low-frequency, high-severity events that have a major impact on the institution's operations. In addition to the definition of operational risk employed by the undertaking, the policies and instructions shall set forth the types of operational risk that are relevant to the operations.*

**Questions**

1. Are there policies and instructions which set forth the way in which the operational risks exposure shall be evaluated and handled?
2. Who approves the policies and instructions?
3. Are there procedures for revision of the policies and instructions?
4. Do the policies and instructions set forth the way in which the institution has categorised and defined its operational risks?
5. Do the policies and instructions set forth which methods and/or approaches shall be used for evaluation of operational risks?
6. Do the policies and instructions contain information about the institution's tolerance level for operational risks?
7. Are there quantitative measures for the evaluation of the exposures?
8. Do the policies and instructions set forth the organisational structure and allocation of responsibility?
9. Do the policies and instructions also cover evaluation and handling of high-severity events that can have a major impact on the institution's operations?
10. Are there principles for handling, i.e. identification, assessment, monitoring, and control/transfer, of operational risks?
11. Do the policies and instructions set forth the way in which outsourcing of the operations may take place?
12. Has a reporting procedure been adopted?
13. Have divisions and business lines produced their own policies and instructions regarding operational risk?

**Request for materials**

Attach relevant policies and instructions for operational risk as well as excerpts of minutes showing when the policies and instructions were approved.

**Processes**

*Chapter 3, section 2, subsection 2*

*The institution shall have processes for handling its exposure to operational risks.*

**Questions**

1. Are there processes for handling exposure to operational risks?
2. Briefly describe these processes.
3. Are these processes documented?
4. Do these processes also include handling of high-severity events which can have a major impact on the operation?
5. Have persons with responsibility for these processes been designated?
6. Have rules been adopted regarding the way in which the exposure to operational risks shall be handled within these processes?

**Request for materials**

Attach process descriptions.

**Contingency and business continuity plans**

*Chapter 3, section 2, subsection 3*

*The institution shall have contingency and business continuity plans in place to ensure an institution's ability to operate on an ongoing basis and limit losses in the event of severe business disruption.*

**Questions**

1. Are there general policies and instructions regarding contingency planning?
2. Have the operation's business-critical processes and systems been identified?
3. Are plans in place for all of these processes and systems?
4. Provide a general description of these plans.
5. Have contingency and business continuity plans been tested?
6. Are the plans documented and well-known within the organisation?
7. Does every subsidiary/division/business line produce its own contingency plans which are better suited to its own operations?
8. Are these individual plans well-integrated into the common plan?
9. Who has approved the contingency and business continuity plans?
10. When were these plans last revised?
11. How often and on what bases are these plans revised?

**Request for materials**

Attach central level contingency and business continuity plans.

**Risk management system**

*Chapter 3, section 2, subsection 4)*

*The institution shall have a documented management system for operational risks with clear responsibilities assigned for this system. The institution shall identify and assess its exposures to operational risks and, in an organised and structured manner, track relevant data. The risk management system shall be subject to regular audit by an independent audit function.*

Questions

1. Briefly describe the structure of the institution's risk management system.
2. Is the risk management system documented?
3. Does the documented risk management system set forth how responsibility for handling of the institution's operational risks is assigned?
4. Does the institution identify its operational risks?
5. Is identification carried out in all of the institution's business lines, business units, control units, and processes?
6. Does the identification render possible an assessment of the institution's exposure to operational risks?
7. Does the institution assess the identified risks, e.g. based on likelihood and impact?
8. What parts are excluded from such identification and why?
9. Does the institution track the relevant data for operational risks in a systematic and organised manner?
10. Has the institution decided upon and documented risk mitigation measures?
11. Is the way in which operational risks are to be managed and prioritised for divisions'/business lines' products, activities, processes, and systems set forth?
12. Does the institution have an independent audit function? If so, describe the function's structure and the methods it uses.
13. On what level in the institution are audit plans approved?
14. Is an independent audit of the risk management system conducted?
15. How often is this audit conducted?

Request for materials

Attach documentation concerning the structure of the institution's risk management system (including instructions and tools, etc.).

Attach documentation which shows the assignment of responsibility. The documentation shall show on which level the decision concerning assignment of responsibility has been taken.

Attach documentation showing the way in which risk identification occurs.

Attach documentation showing the way in which assessment of risk exposure takes place.

Attach the most recent years' audit programmes (e.g. two years or otherwise demonstrate that an independent audit has been conducted).

Attach the independent auditor's instructions.

**Monitoring and control**

*Chapter 3, section 2, subsection 5)*

*The institution's operational risk management system must be closely integrated into the risk management processes of the institution. Its output must be an integral part of the process of monitoring and controlling the institution's operational risk profile.*

**Questions**

1. Is the operational risk management system closely integrated into the risk management processes of the institution?
2. Describe the institution's monitoring and control of exposure to operational risks.
3. Is the output of the risk management system used in monitoring and control of the exposure?

**Request for materials**

Attach the instructions and processes for the way in which monitoring and control occur on central level.

**Reporting structure**

*Chapter 3, section 2, subsection 6*

*The institution shall implement a system of reporting, with a reporting line ultimately to the board of directors, that provides operational risk reports to relevant functions within the institution. Institutions shall have procedures for taking appropriate action according to the information within the management reports.*

**Questions**

1. Does the institution have a system for reporting of operational risks?
2. On what level has this structure been approved?
3. Describe the structure, content, frequency, sender, and recipient.
4. To whom/what function does the audit function report concerning its completed independent audits?
5. Are there procedures to manage the operational risks and take measures based on the information in the risk reports?
6. Are the results of the institution's monitoring and control activities included in the centrally compiled reports?
7. Is there analysis and feedback concerning the contents of the received risk reports?

If so, between what levels does such feedback occur?

**Request for materials**

Attach documents showing the reporting system.

Attach the most recent years' centrally compiled operational risk reports (e.g. two years or demonstrate through other reports that the operational risks have been reported).

Attach the most recent years' internal audit reports (e.g. two years or otherwise show that an independent audit has occurred).