FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Risk-based supervision

Operational Risk Module

Evaluation of:
– Management and control
– Exposure

DATE:
JANUARY 2016

NUMBER:
1.1

LATEST REVISION:
FEBRUARY 2016

AUTHOR:
IRENE STØBACK JOHANSEN

SECTION/DEPARTMENT:
BANKING SUPERVISION

Contents

Introduction

The operational risk module is a guidance for Finanstilsynet's assessment of institutions' operational risk. The document is used by Finanstilsynet at on-site inspections and in connection with assessments of institutions' overall risk profile and capital needs (Supervisory Review Evaluation Process – SREP).

Finanstilsynet defines operational risk as "*the risk of loss resulting from inadequate or failed internal processes or systems, human error or external events*". The definition includes legal risk, but not strategic risk and reputational risk, which must be assessed separately.

Operational risk (OpRisk) is a wide field that affects overall management and control and other risk areas, which can make it challenging to restrict the risk area. The OpRisk module differs from the other modules as it does not target a specific area of operations, but includes different categories of events that may affect several units. The starting point for the OpRisk module is that it as far as possible should function on a stand-alone basis, which means that there will be overlaps with the other models for risk management and control in some areas.

The guidance has been drawn up primarily with a view to the assessment of large institutions. Where smaller institutions are concerned, the guidance must be tailored to the complexity and scale of the particular business (proportionality principle).

The document is divided into two main chapters – *A. Management and control* and *B. Exposure*. A. *Management and control* is divided into six sub-chapters: *1. Strategy and overarching policies, 2. Organisation, responsibilities, outsourcing etc., 3. Measurement – including loss event categories, 4. Monitoring, reporting and disclosure of information, 5. Preparedness and continuity and 6. Independent control.* Each chapter contains sections covering risk in sub-areas, as well as examples of sources of information – documentation (the lists are not exhaustive). Relevant assessment factors are given in each section. *B. Exposure* gives a brief description of elements associated with measurement of the operational risk profile.

The assessment factors in this document are based on provisions of relevant laws and regulations for financial institutions. See appendix I for further details on relevant regulations. In addition, account has been taken of the Basel Committee's[1] "Principles for the Sound Management of Operational Risk"[2] from June 2011 and the EBA's[3] "Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)"[4], dated 19 December 2014, as well as other relevant international guidelines in this area. Beyond the above, the assessments are based on experience gained from the work of supervision.

As part of Finanstilsynet's assessment, each sub-chapter under *A. Management and control* in this document ends with a table to assist classification of the quality of management and control. Classification is four-tiered: *Good control, Satisfactory control, Less than satisfactory control* and *Unsatisfactory control.* The basis for classification will be the conclusions reached regarding deficiencies and flaws in management and control. Furthermore, the risk level is classified under *B. Exposure* as *Low, Moderate, Substantial* or *High.* The classification of individual institutions will not be published.

[1] Basel Committee on Banking Supervision – www.bis.org
[2] www.bis.org/publ/bcbs195.pdf
[3] European Banking Authority – www.eba.europa.eu
[4] www.eba.europa.eu/documents/10180/935249/EBA-GL-2014-13+(Guidelines+on+SREP+methodologies+and+processes).pdf

A. Management and control

1. STRATEGY AND OVERARCHING POLICIES

The purpose of this chapter is to assess the institution's strategy/policy and strategy process for operational risk.

1.1. Strategy and overarching policies – documentation and process

Relevant assessment factors:

- The institution should maintain a framework that includes a strategy for operational risk management and covers its entire operations, cf. the Financial Institutions Act, Section 13-5 (1) and the Basel Committee's principle 2.
- In addition to the strategy, the framework should include limits and guidelines for operational risk management and a system of controls, registration, follow-up and reporting, and should further take the institution's business model, areas of operation and competitive situation into consideration, as well as its risk culture.
- The framework should be adopted by the board of directors and be regularly reviewed by the board in light of changes in the regulatory framework, the macroeconomic outlook, developments in strategic priority areas and the institution's financial soundness and financial performance, cf. Section 47-1 of the Capital Requirements Regulations and the Basel Committee's principle 3.

Some factors may result in elevated operational risk. For example, the following factors should be addressed when assessing the framework

– Have acquisitions, mergers, demergers or other significant changes to the institution's business model and/or strategy taken place?
– Has the institution implemented staff reductions, reorganisations or other major organisational change processes?
– Has the institution implemented major changes in its ICT system and/or in other production processes?
– Is the level of ambition outlined in the institution's strategy and/or business plan likely to affect operational risk in the period ahead?

1.2. Strategy and overarching policies – content

Relevant assessment factors:

- In the strategy, the board of directors should clearly define its operational risk tolerance, i.e. the level of operational risk the institution is willing to accept, cf. the Basel Committee's principle 4.
- The risk level must be commensurate with the institution's financial soundness and profitability.
- The strategy and policy should include quantified limits for exposure in different areas and for different types of operational risk.
- The institution should have a systematic approach to its definition and assessment of risk tolerance. Scenario analyses are one methodology that can be used for this.

The institution should give special attention to events that occur infrequently and have severe consequences, i.e. extreme, but not unlikely events that could lead to heavy losses for the institution. Both actual and potential events (near events) should be considered.

1.3. *Target figures and limits for operational risk*

Relevant assessment factors:

- The board of directors should via the established limit structure ensure that the institution has sufficient control of operational risk.
- The risk limit structure should be adapted to the institution's activity and risk levels and apply across the entire business.

For example, the operational risk level and exposure can be quantified on the basis of the maximum acceptable level of losses stemming from operational risk factors, the number of operational events (overall, in different areas and by type), customer complaints, sickness absence, etc.

Finanstilsynet expects the institutions, when setting limits and target figures for operational risk management, to take their loss and event database into consideration. See section *3 Measurement – including loss event categories* and *B. Exposure* below for more information on operational risk levels.

1.4. *Sources of information – relevant documentation:*

- Strategy and/or policy for operational risk, as well as any overarching policies/principles.
- Documentation showing target figures/limit structure for the institution's operational risk management.

Finanstilsynet's assessments are assigned to one of the categories in the table below.

Good control	**Satisfactory**	**Less than satisfactory**	**Unsatisfactory**
The institution has good processes for establishing a framework and strategy.	The institution has satisfactory processes for establishing a framework and strategy.	There are flaws in the institution's processes for establishing a framework and strategy.	There are serious flaws in the institution's processes for establishing a framework and strategy.
The strategy includes a clear definition of operational risk tolerance.	The strategy includes a satisfactory definition of operational risk tolerance.	The strategy includes an unclear definition of operational risk tolerance.	The board of directors has not defined its risk tolerance.
The limit structure ensures good management and control of operational risk.	The limit structure ensures satisfactory management and control of operational risk.	There are some flaws in the limit structure for management and control of operational risk.	The institution has no defined risk limits, or there are serious flaws in the limit structure for management and control of operational risk.

2. ORGANISATION, RESPONSIBILITIES, OUTSOURCING ETC.

The purpose of this chapter is to assess whether the institution's organisational set-up, and lines of responsibility relating to operational risk are clear, documented and tailored to the size of the operation. For more information on corporate governance in general, see Finanstilsynet's Module for overall management and control.

2.1. *Organisation and responsibilities*

Relevant assessment factors:

- The board has overall responsibility and should establish a strong risk management culture throughout the organisation, cf. Section 13-5 of the Financial Institutions Act and underlying regulations and the Basel Committee's principle 1. "The tone at the top" is crucial to an institution's risk management, and efforts to establish a sound organisational culture are believed to have a positive effect on operational risk management.
- The board of directors shall oversee the institution's senior management to ensure that policies, processes and systems for operational risk management are implemented effectively at all decision levels, cf. Section 8-6 of the Financial Institutions Act and the Basel Committee's principle 3.
- The board should ensure that the institution has a healthy organisational culture. The organisational culture (values, attitudes, ethics, etc.) of an institution may have an impact on operational events. An unhealthy organisational culture may increase the likelihood of operational losses, which in turn may have consequences for the institution.
- The institution's remuneration scheme, which shall be adopted by the board of directors, shall promote sound management and control of the institution's risk, counteract high risk-taking and help to avoid conflicts of interest, cf. Section 1 of the regulations on remuneration in financial institutions etc. Remuneration schemes that encourage aggressive behaviour may heighten the institution's operational risk in the form of an increase in rule violations, malpractice and human errors.
- The institution's senior management is responsible for developing a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility for approval by the board of directors, cf. Section 8-11 of the Financial Institutions Act.
- Senior management is responsible for implementing and maintaining policies, processes and systems for operational risk management throughout the institution consistent with the risk tolerance defined by the board, cf. Section 4 of the regulations on risk management and internal control and the Basel Committee's principle 5.
- The institution must ensure that there is appropriate independence and separation of duties between units and personnel with executive functions and units and personnel with responsibility for monitoring, reporting and controlling operational risk.
- A financial institutions shall have in place independent control functions with responsibility for internal audit, risk management and compliance, cf. the Financial Institutions Act, Section 13-5 (2).
- The risk control function, which is also responsible for management and control of operational risk, shall be independent of operative functions, report either directly or indirectly to the general manager, be able to report directly to the board of directors and not be possible to discharge without the board's approval, cf. Section 47-3 of the Capital Requirements Regulations.

For more information, see the Module for overall management and control.

2.2. *Resources and expertise*

Relevant assessment factors:

- The institution's board and senior management must ensure that the institution has personnel with sufficient expertise to manage and control relevant operational risks.
- The number of employees should reflect the complexity and scope of the business. Resources should be sufficient to cover temporary absence of key personnel.
- The board should define key functions, regularly assess the risk and initiate risk-mitigating measures if the risk becomes too high.
- The resources of the risk control function, the compliance function and the internal audit within operational risk management should be adapted to the complexity and scope of operations, and it is imperative that personnel with control responsibilities have sufficient expertise and authority.

Key-person dependency risk may be particularly high for small undertakings. Special risk factors include vulnerability to loss of expertise, lack of expertise to control specialists within the institution, dependence on individuals, weak division of work and insufficiently independent control.

2.3. *Outsourcing*

Outsourcing provides opportunities for better and/or less costly processes and services due to factors such as economies of scale and access to expertise, and is used by several institutions in the banking/financial industry. Outsourcing has a legal basis in Section 13-4 of the Financial Institutions Act. The outsourcing of tasks may elevate the institution’s operational risk. Outsourcing may also give rise to new types of risk that must be addressed by the institution’s board of directors and management.

Relevant assessment factors:

- Responsibility cannot be outsourced, and the institution is responsible for risk management and internal control of any outsourced parts of its business, cf. Section 13-4 (3) of the Financial Institutions Act, section 5 of the regulations on risk management and internal control and Section 12 of the ICT regulations.
- The board should establish internal guidelines for outsourcing. The guidelines should include procedures for notification to Finanstilsynet prior to the entry into force of outsourcing agreements, cf. Section 4c of the Financial Supervision Act.
- Outsourcing requires a written agreement that ensures the right to inspect, control and audit the outsourced activities, which also applies to Finanstilsynet.
- Outsourcing agreements should be approved by the board and ensure a reasonable right to terminate the agreement under satisfactory conditions until an alternative solution has been established. Agreements on the outsourcing of ICT systems that are of significance to the institution’s operations (and changes to such agreements) shall be approved by the board, cf. Section 2 of the ICT regulations. Outsourcing decisions shall be made on the basis of a risk assessment. The institution must possess the expertise required to consider whether the contractor carries out the assignment in a satisfactory manner. The principal must continuously have the opportunity to identify and control the risks associated with the outsourcing of tasks.

2.4. *Sources of information – relevant documentation:*

- Organisation chart showing actual reporting lines and responsibilities for operational risk, risk management, etc., stating the number of person-years worked and the names of persons with key functions.
- Job instructions for key functions in the risk management and compliance functions and the internal audit.
- Guidelines and limits for remuneration schemes.
- Internal guidelines/instructions for control functions etc.
- The institution’s values and code of ethics.
- Internal guidelines for outsourcing.

Finanstilsynet's assessments are assigned to one of the categories in the table below.

Good control	Satisfactory	Less than satisfactory	Unsatisfactory
The board has established a strong risk management culture based on a sound organisational set-up, clear lines of responsibility and a division of work tailored to the size of the business.	The board has established a satisfactory risk management culture based on an acceptable organisational set-up, lines of responsibility and division of work relative to the size of the business.	The board has less focus on risk management, and the organisational set-up, lines of responsibility and division of work are less than satisfactory relative to the size of the business.	The board has little focus on risk management, and the organisational set-up, lines of responsibility and division of work are unsatisfactory.
The risk control function is organised in accordance with regulations and manages and controls operational risk in a good manner.	The risk control function is generally organised in accordance with regulations and manages and controls operational risk in a satisfactory manner.	There are flaws in the organisation of the risk control function, which manages and controls operational risks in a less than satisfactory manner.	There are serious flaws in the organisation of the risk control function, which manages and controls operational risks in an unsatisfactory manner.
The institution has ample resources and expertise, and personnel with control responsibilities have the necessary authority.	The institution has adequate resources and expertise, and personnel with control responsibilities have acceptable authority.	The institution's resources and expertise are not adequately adapted to the business, and personnel with control responsibilities lack sufficient authority.	The institution’s resources and expertise are unsatisfactory, and personnel with control responsibilities have no authority.
The institution’s management and control of its outsourced business is sound, with good agreements, procedures, levels of expertise etc.	The institution’s management and control of its outsourced business is satisfactory, with acceptable agreements, procedures, levels of expertise etc.	The institution’s management and control of its outsourced business is less than satisfactory, and there are flaws in agreements, procedures, levels of expertise etc.	The institution’s management and control of its outsourced business is unsatisfactory, and there are serious flaws in agreements, procedures, levels of expertise etc.

3. MEASUREMENT – INCLUDING LOSS EVENT CATEGORIES

The purpose of this chapter is to assess whether the institution has in place relevant systems to identify, measure and assess operational risk. In this assessment the complexity and scope of operations must be kept in mind.

A financial institution shall at all times have an overview over the risks attending its activity, including operational risk. Assessments of operational risk shall be made at least once a year in connection with the institution's assessment of its overall need for capital relative to its risk profile (ICAAP[5]), cf. Section 13-6 of the Financial Institutions Act.

Operational risk events are normally divided into seven loss event categories, and according to section 44-2 of the Capital Requirements Regulations, institutions wishing to apply for approval to use the advanced measurement approach (AMA) to calculate minimum capital requirements for operational risk are required to allocate internal loss data to the following loss event categories:

1. Internal fraud
2. External fraud
3. Employment practices and workplace safety
4. Clients, products and business practices
5. Damage to physical assets
6. Business disruption and system failures
7. Execution, delivery and other transaction processing

3.1. *System for measuring operational risk in ongoing operations*

Relevant assessment factors:

- The institution should have in place a system and internal guidelines to identify and measure the operational risk inherent in all material products, activities, processes and systems, cf. the Basel Committee's principle 6.
- The institution's loss and event database should be designed to preserve as much information as possible. The information should be systematised in a way that enables learning and enhanced knowledge as well as the implementation of measures to prevent future undesirable events.
- The institution should have in place a system and internal guidelines which ensure that events leading to a material reduction in the functionality of ICT systems are reported to Finanstilsynet, cf. Section 9 of the ICT regulations and Circular 15/2009 (in Norwegian only).

Best practice for measuring operational risk includes a system for registering loss events in a loss and event database, where the events are distributed across the seven loss event categories and sub-categories and where both events that have resulted in losses and events that have not resulted in losses (near-events and potential losses) are recorded.

Deficiencies and deviations pointed out by independent control functions, such as risk control, compliance and the internal and external auditor, are important sources of information about the institution's operational risk (see point 6.1 below), and should be assessed and viewed in light of the institution's loss and event database.

[5] "Internal Capital Adequacy Assessment Process", cf. Circular 9/2015. Finanstilsynet's methodologies for assessing risk and capital needs (in Norwegian only).

3.2. Operational risk attending new products, activities, processes and systems

Relevant assessment factors:

- The institution's senior management must ensure that the institution has an approval process that includes internal guidelines for new products, activities, processes and systems, cf. the Basel Committee's principle 7.
- New products, activities, processes and systems of material significance and/or with a diverging risk profile should be approved by the board and/or a relevant body at the top management level.
- The institution shall, when changing or establishing material products and procedures, conduct a risk assessment before the activities commence that includes operational risk factors, cf. Section 6 of the regulations on risk management and internal control.
- The risk assessment should clarify risk-mitigating measures, both measures to be initiated prior to commencement and measures that may be implemented in the short and long term in the event of adverse risk developments.

3.3. Measurement of operational risk in assessments of capital needs

Under current regulations, financial institutions can use three different approaches to calculate the capital requirement for operational risk under Pillar 1: *the basic indicator approach, the standardised approach and the AMA approach.* The basic indicator approach and the standardised approach are based on standardised percentages of defined concepts of income. The capital requirement under the basic indicator approach is 15% of average income over the previous three years, while the standardised approach is based on different percentages (from 12% to 18%) depending on the business area. The standardised approach seeks to give a better reflection of differences in risk profiles across the institution and can only be used by institution that meet certain requirements for risk management, cf. Section 43-1 of the Capital Requirements Regulations.

Norwegian institutions use the basic indicator approach or the standardised approach. At end-December 2015, no Norwegian institutions used AMA approaches approved by the authorities. The institutions shall, as part of their internal capital assessment process (ICAAP), assess their capital need for operational risk at least once a year. In this regard, the institutions should assess whether the estimated regulatory capital is sufficient relative to the risk level, and whether there is a need for a pillar 2 add-on for operational risk.

Relevant assessment factors:

- The institution should have procedures in place that ensure proper measurement and calculation of regulatory capital for operational risk.
- The estimated regulatory capital should be considered against the institution's defined risk tolerance and actual historical losses related to operational errors.

For expanding institutions, the estimated regulatory capital will be too low – all else equal – in a forward-looking perspective. This also applies to institutions that have been through one or more years with extraordinarily low income. The operational risk will not necessarily be reduced even if income declines.

In October 2014, the Basel Committee published a consultation document[6] on a new approach for measuring the capital requirement for operational risk, proposing to replace the basic indicator approach with a revised standardised approach. It was proposed that the measurement methodology for the revised standardised approach should still be based on income for the previous three years. What is new is that the proposed methodology is to be based on the size of so-called business indicators, and that gross amounts should be used, with the consequence that size gains in significance compared with the current regulations, which are based on net figures.

[6] www.bis.org/press/p141006.htm

3.4. Some sub-categories of operational risk

There are a number of sub-categories of operational risk. The purpose of this chapter is to assess some of the risks that are normally of relevance to financial institutions and may have a strong influence on the institutions' operations.

3.4.1. Model risk

Model risk may relate to various factors:

1) The risk of underestimating capital needs due to errors in the development, implementation and use of internal models, normally IRB models for calculating capital for credit risk.
2) The risk of losses arising from the development, implementation and improper use of models used in the institution's decision-making processes, e.g. for pricing of products, evaluation of financial instruments, monitoring of risk limits and target figures, etc.

With respect to point 1), this risk is considered during special IRB inspections and is thus not part of the ordinary supervision of operational risk.

With respect to point 2), this risk falls in its entirety under operational risk and must be assessed during the inspection of the relevant risk area. Elements that may be of significance are the quality of the institution's processes for changes in and new products and services (cf. point 3.2 above), validation processes, etc.

3.4.2. Conduct risk and consumer protection

Internationally, there is increasing focus on the risk of losses resulting from rule violation or malpractice. Fines and compensation claims may have major negative consequences for both the finances and the reputation of individual institutions. Although there has been a limited number of these types of events in Norway thus far, recent years have seen events related to malpractice that have caused significant losses for some Norwegian institutions[7]. In general, consumer protection has gained in importance internationally in recent years. This is also the case in Norway, which was evidenced by the amendment to the objects clause of the Financial Supervision Act in 2012.

Conduct risk and consumer protection fall under loss event category 4 – Clients, products, and business practices – cf. point 3 above.

In addition to ensuring that financial institutions are financially sound and liquid, and thereby able to meet their obligations to consumers, the following factors are relevant and should be considered:

Consumer protection:

- The institution should have internal guidelines to ensure that consumers receive adequate and reliable information and good advice about the products sold by the institution and that the customers' interests are given priority. The guidelines should cover the development and quality assurance of documentation and marketing material, as well as training.
- Banks with securities licences shall have internal guidelines to ensure compliance with the requirements concerning investment advice in accordance with the provisions of Section 9-11 of the Securities Trading Act (the MiFID rules), cf. the Securities Trading Act, Section 9-11 and part 2, chapter 3 II of the Securities Regulations.
- The institution shall have a register of financial agents that is publicly available on the institution's website, cf. Circular 16/2009 (in Norwegian only).
- The institution shall have written procedures that ensure thorough processing of complaints, including the recording of all customer complaints in a separate register, and annual reporting of customer complaints to Finanstilsynet, cf. Circular 12/2014 (in Norwegian only).

The use of external distributors (dealers, agents, etc.) and the sales of sophisticated financial savings instruments etc. may increase conduct risk and the need for consumer protection.

[7] E.g. the so-called "Røeggen case" from 2013.

In low-interest regimes, the demand for alternative savings products with a potential for higher returns (and higher risk) may increase, which in turn may heighten the institution's conduct risk.

Bundled products are as a rule prohibited and can only be offered if a connection exists between the products such that the offer of one product presupposes the offer of another product, or if cost savings justify such bundling, cf. the regulations on bundled products, Section 2.

A number of new international EEA relevant provisions relating to consumer protection will be introduced and are expected to result in amendments to Norwegian regulations[8]. It is not yet clear which specific changes will be made and when they will enter into force in Norway.

Other customers/activities:

- With respect to large banks, there may be a risk that they will manipulate reference rates (e.g. NIBOR), exchange rates and indices to increase their profitability. As regards NIBOR, Finance Norway is currently responsible for establishing the rules, while Oslo Børs is the calculation agent. These factors are most relevant to follow up as part of the supervision of market risk.

3.4.3. ICT risk

ICT risk is an important sub-group in the "Business disruption and system failures" category – cf. the loss event categories in point 3 above. The financial sector in Norway bases its activities on ICT solutions. ICT risk is considered to be one of the biggest risks faced by the institutions, to which they are highly vulnerable. Moreover, there is rapid technological development within this sector.

See the Risk and Vulnerability Analysis (RVA)[9] on Finanstilsynet's website for examples of specific factors which may elevate ICT risk and which are of relevance to a number of Norwegian financial institutions.

As regards ICT risk, the provisions of the ICT regulations are essential. The institutions shall have an ICT strategy, conduct risk analyses, establish quality targets and develop procedures that secure the systems for development, procurement, operations, deviation and change management, as well as outsourcing agreements. In addition, business continuity and emergency plans are required. The institution shall have in place a system and internal guidelines which ensure that events leading to a material reduction in the functionality of ICT systems are reported to Finanstilsynet, cf. Section 9 of the ICT regulations and Circular 15/2009.

The OpRisk module is structured to include a limited assessment of ICT risk. If there is a need for a more thorough review, e.g. on the basis of findings from OpRisk inspections or inspections in other areas, this will be considered as part of special IT inspections where separate modules based on COBIT are used.

3.4.4. Money laundering and terrorist financing risk

Money laundering and terrorist financing risk includes elements of external fraud and execution, delivery and other transaction processing, cf. loss event categories 2 and 7 in point 3 above. Anti-money laundering and counter terrorist financing measures are essential to fight organised crime and terrorism and has gained increasing attention both in Norway and internationally of late. Banks and other financial institutions play a key role in the fight against money laundering and terrorist financing.

Relevant assessment factors:

- The institution's work in this area must be clearly organised, with a distinct division of responsibilities. The institution must have an anti-money laundering officer who is a member of the senior management team, and sufficient resources and expertise in the field, cf. Section 23 of the Anti-Money Laundering Act.

[8] E.g. MiFID II (http://ec.europa.eu/finance/securities/isd/mifid2/index_en.htm), PRIIPS (http://ec.europa.eu/finance/finservices-retail/investment_products/index_en.htm), POG (http://www.eba.europa.eu/documents/10180/888290/EBA-CP-2014-37+%28Draft+Guidelines+on+POG%29.pdf) etc.

[9] www.https://www.finanstilsynet.no/en/publications/risk-and-vulnerability-analysis-rav/

- The board of directors shall establish specific and adequate internal guidelines to ensure compliance with legislation in this field.
- The institution shall have an electronic transaction monitoring system covering the entire business, cf. Section 24 of the Anti-Money Laundering Act.
- The institution shall apply risk-based customer due diligence measures and ongoing monitoring, cf. chapter 2 of the Anti-Money Laundering Act, including:
    - Risk classification of customers (Section 5),
    - Customer due diligence measures (Sections 6 through 15), which includes verifying the customer's identity, identifying beneficial owners, obtaining information about the purpose and intended nature of the customer relationship and the origin of the funds, and determining whether the customer is a politically exposed person.
- The institution shall examine and report suspicious transactions to ØKOKRIM (the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime), cf. Chapter 3 of the Anti-Money Laundering Act.
- The institution shall store documentation and recorded information, cf. Section 22 of the Anti-Money Laundering Act. The institution must also ensure that documentation is erased after the time limit for the duty to retain information expires.

See the sub-module for management and control of money laundering and terrorist financing for more details.

3.5. *Sources of information – relevant documentation:*

- Internal guidelines for identifying, measuring, and recording events in institutions' loss and event databases.
- A list of loss events over the last 1-2 years (copy of the loss and event database).
- Events reported to Finanstilsynet, cf. the ICT regulations and Circular 15/2009.
- Internal guidelines for approval of changes in or the establishment of new products, activities, processes and systems.
- An example of a risk assessment concerning changes in or the establishment of material products and/or procedures.
- Any completed gap analysis if the institution has started using the standardised approach during the past year, cf. Section 43-1 of the Capital Requirements Regulations.
- The agent register on the institution’s website.
- Marketing materials for customer loyalty programmes and price lists.
- Internal guidelines to ensure compliance with requirements for investment advice.
- Internal guidelines for customer complaints and customer complaint registers.
- Organisation chart showing the organisation of the institution’s AML officers.
- Internal guidelines for the implementation of the Anti-Money Laundering Act.
- A selection of documents related to due diligence measures applied for new and existing customers.
- An overview of flagged and reported suspicious transactions over the last 1-2 years.

Finanstilsynet's assessments are assigned to one of the categories in the table below.

Good control	Satisfactory	Less than satisfactory	Unsatisfactory
The institution has established a good system for measuring operational risk which includes registering the events in one of the seven loss categories including sub-categories.	The institution has established an acceptable system for measuring operational risk which is primarily based on registration in accordance with the seven loss event categories.	The institution's system for measuring operational risk is inadequate. Loss events are not categorised.	The institution has an unsatisfactory system for measuring operational risk, as it does not register loss events.
The institution has good processes for approving changes in or new products etc., including clear guidelines and sound risk assessments.	The institution has satisfactory processes for approving changes in or new products etc., including guidelines and risk assessments.	The institution's processes for approving changes in or new products etc. are flawed, and guidelines and risk assessments are inadequate.	The institution's processes for approving changes in or new products etc. have serious flaws, and guidelines and risk assessments are unsatisfactory.
The institution has and follows good procedures for measuring regulatory capital for operational risk.	The institution has and follows satisfactory procedures for measuring regulatory capital for operational risk.	The institution has less than satisfactory procedures for measuring regulatory capital for operational risk.	The institution has unsatisfactory procedures for measuring regulatory capital for operational risk.
Regulatory capital is considered to cover the capital requirement by an ample margin.	Regulatory capital is considered to be adequate.	Regulatory capital is considered to be low.	Regulatory capital is considered to be inadequate to cover operational risk.
The institution has good control of its model risk.	The institution has satisfactory control of its model risk.	The institution has less than satisfactory control of its model risk.	The institution has unsatisfactory control of its model risk.
The institution has good control of its conduct risk and offers no bundled products that are in breach of legislation.	The institution has satisfactory control of its conduct risk and offers no bundled products that are in breach of legislation.	The institution has less than satisfactory control of its conduct risk and offers bundled products that seem to be in breach of legislation.	The institution has unsatisfactory control of its conduct risk and offers bundled products that are in breach of legislation.
The institution has good procedures for processing, recording and reporting customer complaints.	The institution has acceptable procedures for processing, recording and reporting customer complaints.	The institution's procedures for processing, recording and reporting customer complaints are inadequate.	There are serious flaws in the institution's processing, recording and reporting customer complaints.
The institution's investment advice is in line with legislation.	The institution's investment advice is essentially in line with legislation.	The institution's investment advice is inadequate and not in line with legislation.	There are serious flaws in the institution's investment advice, which is not in line with legislation.

The institution's AML work is well organised, with ample resources and expertise.	The institution's AML work is organised in an acceptable manner, with satisfactory resources and expertise.	The institution's AML work is organised in a less than satisfactory manner, with inadequate resources and expertise.	The institution's AML work is organised in an unsatisfactory manner, with an obvious lack of resources and expertise.
The institution has good internal AML guidelines approved by the board of directors.	The institution has satisfactory internal AML guidelines approved by the board of directors.	The institution has less than satisfactory internal AML guidelines that have not been approved by the board.	The institution has unsatisfactory internal AML guidelines that have not been approved by the board.
The institution has a good system for monitoring and reporting suspicious transactions.	The institution has a satisfactory system for monitoring and reporting suspicious transactions.	The institution has a less than satisfactory system for monitoring and reporting suspicious transactions.	The institution has an unsatisfactory system for monitoring and reporting suspicious transactions.

4. MONITORING, REPORTING AND DISCLOSURE OF INFORMATION

In this chapter the institution's systems for monitoring, reporting and acting on operational risk are mapped and their relevance assessed. The following should be mapped and assessed: what reporting lines are established, what levels of the organisation receive various types of reporting and whether the content of the reports is relevant and sufficient.

In this chapter it is important to map and evaluate concrete management reports that are produced in the institution and the relevance of their content. In addition to the actual reports, appurtenant memos with analyses will be assessed to identify what assessments, conclusions and decisions are made with a basis in the content of the reports.

4.1. *Monitoring*

Relevant assessment factors:

- The institution should have consistent procedures that ensure regular monitoring of operational risk developments and material exposures to losses throughout the business, cf. the Basel Committee's principle 8.
- The institution should also have procedures that ensure regular monitoring of compliance with the requirements of laws and regulations as well as internal policies and procedures. In the event of repeated rule breaches it must be ascertained whether this is due to a lack of respect for the rules and/or to unsatisfactory monitoring procedures.

4.2. *Reporting and follow-up*

Relevant assessment factors:

- The institution should report and follow up the strategic target figures and limits set out in the institution's strategy/policy for operational risk.
- The recipient of reports should be the organisational level that has adopted the strategy, policy, targets and exposure limits.
- The institution should ensure documentation of reports that are produced, how often they are produced, who is responsible for the content of the reports, who are the recipients of the respective reports and how the information is used and followed up.
- The institution should have in place established procedures for quality assurance of the reported data and the reporting systems, both for internal reports and for reporting to the authorities[10]. Resonableness tests and random checks of the data should be undertaken. The form, content and frequency of reporting should be reviewed on a regular basis.

4.3. *Internal control of operational risk*

Principles for internal control, what processes have been established to implement internal control, and the quality thereof make up the themes addressed by Finanstilsynet's Module for overall management and control. This section is designed to identify and assess how the institution, through its internal control function, has brought to light possible weaknesses in the operational risk area that require action to be taken.

Relevant assessment factors:

- The board should develop and maintain robust internal control systems with appropriate internal controls covering operational risk aspects throughout the business, cf. the Basel Committee's principle 9.

[10]External reporting of particular relevance to operational risk includes capital requirements reporting and reporting of ICT events to Finanstilsynet, as well as reporting of suspicious transactions to ØKOKRIM.

- The management reports should specify the operational risk factors that have been controlled and assessed, the control procedures undertaken, the results thereof and long-term developments, as well as the risk-mitigating measures initiated, cf. Section 7 of the regulations on risk management and internal control.

4.4. Disclosure of information on operational risk

Relevant assessment factors:

- The institution should disclose sufficient information to allow stakeholders to assess its approach to operational risk management, cf. the Basel Committee's principle 11.
- The institution shall have internal policies and procedures to fulfil the disclosure requirement within operational risk (Pillar 3), cf. Section 3 of the Capital Requirements Regulations.
- With respect to operational risk, the institution shall as a minimum disclose information on strategy and processes, organisation of the risk management function, risk reporting and measurement systems and guidelines and procedures for the monitoring and use of collateral, cf. Section 45-7 of the Capital Requirements Regulations.

4.5. Sources of information – relevant documentation:

- Internal guidelines for compliance with legislation, procedures, etc
- Experience with external reporting to Finanstilsynet.
- An overview of reports to the board and senior management regarding operational risk aspects and the latest version of each report.
- The most recent management reports concerning internal control.
- Internal guidelines for external reporting and disclosure of financial information.

Finanstilsynet's assessments are assigned to one of the categories in the table below.

Good control	**Satisfactory**	**Less than satisfactory**	**Unsatisfactory**
There is sound internal control of the institution's operational risk, and management reports are good.	There is satisfactory internal control of the institution's operational risk, and management reports are acceptable.	There are flaws in the institution's internal control of operational risk and in its management reports.	There are serious flaws in the institution's internal control of operational risk and in its management reports.
The institution undertakes relevant and regular monitoring and reporting of operational risk to the board and senior management and has and follows good procedures for quality assurance of data.	The institution's reporting of operational risk to the board and senior management is satisfactory, and it has and follows acceptable procedures for quality assurance of data.	The institution undertakes less relevant and irregular reporting of operational risk to the board and senior management, and quality assurance is flawed.	There are serious flaws in the reporting of operational risk to the board and senior management, and the reporting frequency and quality assurance are unsatisfactory.
The institution has good processes for disclosing information and provides good information on operational risk management.	The institution has satisfactory processes for disclosing information and provides acceptable information on operational risk management.	The institution has less than satisfactory processes for disclosing information and provides inadequate information on operational risk management.	The institution's processes for the disclosure of information are unsatisfactory, and the information on operational risk management has serious flaws.

5. PREPAREDNESS AND CONTINUITY

This section is designed to assess the institution's plans to ensure ongoing operations and limit losses in the event of business disruptions. In this assessment the complexity and scope of operations must be kept in mind.

The institution shall have contingency plans that ensure ongoing operations and limit losses in the event of severe business disruptions, cf. the Basel Committee's principle 10 and Section 47-2 (5) of the Capital Requirements Regulations. In Finanstilsynet's view, all institutions need to have a clear opinion of what might happen, how events may affect the institution's operations and how the institution will face such challenges. All these elements should be included in a contingency plan.

Norwegian legislation sets explicit requirements for continuity/contingency plans in the following areas:

- *ICT systems:* The operational solutions of Norwegian banks and finance companies are based on information and communication technology. A detailed assessment of the institution's ICT solutions and relevant emergency plans is made at special IT inspections, cf. Sections 8 and 11 of the ICT regulations.
- *Liquidity/funding:* A detailed assessment of the institution's contingency plan for liquidity crises, cf. Section 6 of the regulations on sound liquidity management, is made in connection with liquidity inspections, cf. the Module for liquidity risk – evaluation of management and control.
- *Financial soundness:* A capital plan to assess how the institution's capital needs can be met in the short and longer term, cf. Section 13-6 (3) of the Financial Institutions Act.

Relevant assessment factors:

- The institution's contingency plans, both at the overarching level and for key areas of operation, should apply to the entire business, be viewed together and be based on an updated risk assessment. The institution's contingency plans should be approved by the board.
- Contingency plans shall be updated regularly and on the basis of changes in the regulatory framework, developments in strategic focus areas, etc.
- The contingency plans must be available in all situations.
- The institution should arrange training and test the contingency plans on a regular basis.
- Plans should include different types of scenarios that could have a profound impact on the institution's operations, both physical events such as fire, robbery and flooding, and events related to ICT systems, such as hacking, Trojan attacks and DDoS attacks.
- The plans should include internal policies and procedures plus measures, an overview of roles and responsibilities (contingency organisation), and requirements for internal and external information and communication.
- Emergency plans for the institution's ICT systems must satisfy the requirements of Section 11 of the ICT regulations.
- Contingency plans for liquidity crises must also satisfy the requirements of the regulations on sound liquidity management.

In 2014, the EU's "Bank Recovery & Resolution Directive" (BRRD) was adopted. The purpose of the directive is to establish a European recovery and resolution system that ensures financial stability by providing banks and other credit institutions, as well as the authorities, with the necessary tools to prevent and handle crises at an early stage. The factors behind the requirement for recovery plans are relevant to Norwegian banks. One of the key issues in the directive is the requirement that all banks must draw up recovery plans setting out specific, implementable measures for dealing with financial crisis situations. The plans must be evaluated by the supervisory authorities.

5.1. *Sources of information – relevant documentation:*

- Contingency and continuity plans.
- Internal guidelines for updating, training, and testing of contingency and continuity plans.
- Reports after conducted emergency drills.

Finanstilsynet's assessments are assigned to one of the categories in the table below.

Good control	**Satisfactory**	**Less than satisfactory**	**Unsatisfactory**
The institution has good processes and guidelines for updating, approving and testing contingency plans.	The institution has satisfactory processes and guidelines for updating, approving and testing contingency plans.	There are flaws in the institution's processes and/or guidelines for updating, approving and testing contingency plans.	There are serious flaws in the institution's processes and/or guidelines for updating, approving and testing contingency plans.
The contingency plans cover the entire business and include relevant scenarios and measures.	The contingency plans cover the greater part of the business and include relevant scenarios and measures.	The contingency plans do not cover the entire business, and the scenarios and measures are inadequate.	The contingency plans do not adequately cover the business and there are serious flaws in the scenarios and measures.

6. INDEPENDENT CONTROL

The purpose of this chapter is to assess the quality and use of the work performed by the line-independent control functions within operational risk. In this context, line-independent control functions mean the risk management function, the compliance function (second line of control) and the internal and external audit (third line of control).

Relevant assessment factors:

- The line-independent control functions should perform relevant, documentable controls of operational risk of a high professional standard.
- The independent control functions must have sufficient expertise and resources within operational risk.
- Reports from the independent control functions concerning operational risk.should be addressed to and considered at the relevant level of the organisation.
- The institution should have procedures for how critical comments from independent control functions concerning operational risk should be treated and followed up.
- The institution's system for management and control of operational risk should be regularly evaluated by independent control functions~~,~~. With respect to institutions using the standardised approach, the system should regularly be reviewed and confirmed by an independent function, cf. Section 43-1 (1) of the Capital Requirements Regulations.

6.1. *Sources of information – relevant documentation:*

- Risk reports.
- Compliance reports.
- Reports from and correspondence with the internal and external auditor.
- If the institutions use the standardised approach: the most recent confirmation from an independent function.

Finanstilsynet's assessments are assigned to one of the categories in the table below.

Good control	**Satisfactory**	**Less than satisfactory**	**Unsatisfactory**
Independent control functions have good expertise and sufficient resources and regularly perform sound controls of operational risk.	Independent control functions have satisfactory expertise and acceptable resources and perform satisfactory controls at an acceptable frequency.	Independent control functions have less than satisfactory expertise and inadequate resources and perform less than satisfactory controls too infrequently.	Independent control functions have inadequate expertise and resources and perform unsatisfactory controls.
Reports concerning operational risk are handled by the appropriate body, and critical comments are followed up in a proper manner.	Reports concerning operational risk are generally handled by the appropriate body, and critical comments are followed up in a satisfactory manner.	The institution’s handling of reports concerning operational risk is less than satisfactory and there are some flaws in the follow-up of critical comments.	The institution’s handling of reports concerning operational risk is unsatisfactory, and there are serious flaws in the follow-up of critical comments.
The institution’s system for operational risk management and control is evaluated by independent functions	The institution’s system for operational risk management and control is evaluated by independent functions	The institution’s system for operational risk management and control is not evaluated by independent	The institution’s system for operational risk management and control is not evaluated by independent

on a regular basis, and the most recent assessment confirms that the system is satisfactory.	on a regular basis, and the most recent assessment confirms that the system is acceptable.	functions on a regular basis, and the most recent assessment confirms that the system is less than satisfactory.	functions on a regular basis, and the most recent assessment confirms that the system is unsatisfactory.

B. Exposure

It can be challenging to measure the actual operational risk level as no uniform quantitative indicators have been established, as is the case in other risk areas, and there is limited access to external data for comparative analyses. Measurement and modelling of economic losses resulting from operational risk is also problematic, especially for rare events with serious consequences. However, there are alternative modelling tools for operational risk analysis, such as Bayesian networks, which have become increasingly popular in some circles, such as the OpRisk project at the University of Stavanger[11]. In this assessment the complexity and scope of operations must be kept in mind.

Even though it may be difficult to establish whether the risk exposure is high or low, this does not mean that it is inexpedient to assess the risk level. Such an assessment may provide valuable information in itself regarding the current development/trend, why the risk exposure is the way it is, which factors/components are important, how different measures affect the risk situation etc.

Examples of factors that may give an indication of the institution's level of operational risk:

- The number of loss events, overall and distributed across the various loss categories. For various reasons, it is logical to register some types of events under sub-categories of the seven main categories, such as customer complaints and events related to money laundering (e.g. suspicious transactions).
- The types of loss events that have occurred in the various areas of operation.
- Losses resulting from operational events, both actual and potential losses, overall and distributed on sub-categories.
- The number of issues/critical comments from independent control functions.

Below are examples of loss events, cf. point 3 above, distributed on the loss event categories with indicators. The list of examples and indicators is not exhaustive, and some types of events may be categorised under more than one category, while some indicators may point to more than one type of event.

Type of event	Definition	Examples	Indicators
Internal fraud	Losses due to acts involving at least one internal party that are intended to misappropriate funds or circumvent the law or the institution's policy, excluding diversity/ discrimination events.	- Corruption - Embezzlement - Insider trading - Rogue trading	- An overview of cases reported to the police/insurance undertaking - Unauthorised activity - Holiday statistics (failure to take holiday) - An overview of working hours (odd working time, weekend/night work) - The number of whistleblowing cases
External fraud	Losses due to acts intended to defraud, misappropriate funds or circumvent the law, by a third party	- Fraud, incl. card fraud and identity theft - Document forgery - Robbery and other violent crime - Threats to employees - Money laundering - Terrorist financing - Hacking, phishing, ransomware	- An overview of cases reported to the police/insurance undertaking - Statistics of suspicious transactions; flagged cases and notifications to ØKOKRIM - Card fraud statistics - Statistics of attempts to break firewalls etc.
Employment practices and workplace safety	Losses due to acts that are non-compliant with laws, regulations and working environment agreements, payment of personal injury	- Occupational injuries - Violations of HS&E rules - Discrimination - Reorganisation	- Sickness absence - Personnel statistics (turnover, overtime, gender distribution,

[11] A research project under the auspices of the University of Stavanger, with participants from six Norwegian banks, the Research Council of Norway and Finanstilsynet, concluded in 2014. For more information see: www.oprisk.no.

	claims or other circumstances.	- Downsizing	distribution on ethnic groups etc.) - Employee satisfaction surveys - Whistleblowing cases - Statistics of processing times/unprocessed cases/missed calls etc.
Clients, products and business practices	Losses due to unintentional or negligent failure to meet obligations to specific customers (including fiduciary and suitability requirements), or due to the nature or design of a product.	- Unauthorised activity - Absence of processes for the approval of new products - Sale of unauthorised products, bundled products - Aggressive sales and sales of high-risk products to the wrong customers - Unauthorised insight into and misuse of confidential customer data - Manipulation of reference rates etc.	- Statistics of customer complaints, incl. complaints handled by a complaints board - Statistics of unauthorised activity - Sales statistics and portfolio analyses, broken down on distribution channels - Customer satisfaction surveys - Reports/results, bonus/incentive schemes
Damage to physical assets	Losses due to damage to, or loss of, physical assets from natural disasters or other events.	- Damage caused by fire, flooding, snow - Robbery and vandalism - Terrorist acts (11 September / 22 July)	- Number of reported insurance claims
Business disruption and system failures	Losses due to business disruptions or system failures.	- IT events, both software and hardware - Power outage/utility disruptions - Disruption of telecommunications services	- Registered system downtime - The stability of power supply, telecommunications and web access - Statistics of attempts to break firewalls etc. - Statistics of IT events reported to Finanstilsynet
Execution, delivery and other transaction processing	Losses due to insufficient or failed transaction processing or systems for transaction processing with trading counterparts and suppliers.	- Errors in recorded data (typing error) and systems - Misunderstandings and miscommunication - Incorrect system accesses - Errors in collateral documentation and lack of legal documentation - Disputes with other counterparts (not customers) and suppliers - Losses related to outsourcing agreements	- Transaction statistics and error logs - Reports from internal control, compliance, auditor, inspection - Access lists

A good analysis of the institution's operational risk level based on an analysis of recorded loss events and near-events requires that the system is considered to cover the entire business and that all events in all risk areas are recorded. Underreporting of loss events is not an unknown issue.

Long-term trends are equally important as the status at a given point in time. It must be considered whether the changes are due to changes in the reporting system and compliance with internal reporting guidelines or whether developments are due to changes in the actual underlying risk level. Developments in loss events and losses should also be viewed in light of other factors that may result in increased operational risk over time, such as changes in strategy and business model, organisational changes, system conversions and changes in production processes etc.

Finanstilsynet's assessments are assigned to one of the categories in the table below.

Low operational risk	Moderate operational risk	Substantial operational risk	High operational risk
The institution’s total operational losses are low.	The institution’s total operational losses are moderate.	The institution’s total operational losses are substantial.	The institution’s total operational losses are high.
The institution has few loss events.	The institution has a moderate number of loss events.	The institution has a substantial number of loss events.	The institution has a high number of loss events.
The institution's other indicators point to a low risk level.	The institution's other indicators point to a moderate risk level.	The institution's other indicators point to a substantial risk level.	The institution's other indicators point to a high risk level.

Appendices:

I. Relevant laws and regulations

- LOV-2015-04-10-17: Act on financial institutions and financial groups (Financial Institutions Act)
- LOV-1956-12-07-1: Act on the supervision of financial institutions etc. (Financial Supervision Act)
- LOV-2007-06-29-75: Act on securities trading (Securities Trading Act)
- LOV-2009-03-06-11: Act relating to measures to combat money laundering and terrorist financing (Anti-Money Laundering Act)
- FOR-2006-12-14-1506: Regulations on capital requirements for commercial banks, savings banks, finance companies, financial holding companies, investment firms and fund management companies for securities funds etc. (Capital Requirements Regulations) (available in Norwegian only).
- FOR-2008-09-22-1080: Regulations on risk management and internal control
- FOR-2014-08-22-1094: Regulations on remuneration schemes in financial institutions, investment firms and fund management companies (available in Norwegian only).
- FOR-2003-05-21-630: Regulations on use of information and communication technology (ICT) in banks etc. (ICT regulations).
- FOR-2007-06-29-876: Regulations to the Securities Trading Act (Securities Trading Regulations).
- FOR-1990-06-01-429: Regulations on bundled products, etc. (available in Norwegian only)
- FOR-2009-03-13-302: Regulations relating to measures to combat money laundering and terrorist financing (Anti-Money Laundering Regulations)
- Circular 3/2009: Guide to the regulations on risk management and internal control (available in Norwegian only).
- Circular 15/2009: Reporting of ICT events to Kredittilsynet (available in Norwegian only).
- Circular 12/2014: Guidelines for complaint processing in banking, financial, insurance and securities activities (available in Norwegian only).
- Circular 16/2009: Financial agents (available in Norwegian only).
- Circular 15/2014: Remuneration schemes in financial institutions, investment firms and fund management companies (available in Norwegian only).
- Circular 9/2015: Finanstilsynet's methodologies for assessing risk and capital needs (available in Norwegian only).

II. The Basel Committee's principles for operational risk

See: www.bis.org/publ/bcbs195.pdf.

Fundamental principles of operational risk management

Principle 1: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.

Principle 2: Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

Governance

The board of directors

Principle 3: The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

Principle 4: The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

Senior management

Principle 5: Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for operational risk management in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

Risk management environment

Identification and assessment

Principle 6: Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

Monitoring and reporting

Principle 8: Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

Control and mitigation

Principle 9: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

Business resiliency and continuity

Principle 10: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Role of disclosure

Principle 11: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.