ASISA GUIDELINE ON OPERATIONAL RISK FOR LIFE INSURERS

Date of first publication: 22 July 2022

Last updated: 30 July 2025

1. PURPOSE

1.1. Insurers are being progressively exposed to more complex risks, and as a result are compelled to take more controlled and measured risks in line with defined tolerance and risk appetite levels, which subsequently leads to operational risk becoming increasingly important in the management and corporate governance of insurers because of its implications and interactions with the other risks faced, such as market, credit and insurance risks.

1.2. Operational risk management plays a critical role within financial institutions due to the inherent complexities and vulnerabilities of their operations. It is essential for these institutions to identify, assess, and mitigate operational risks to protect their financial stability, reputation, and regulatory compliance. By effectively managing operational risks, financial institutions can minimize the likelihood and impact of operational failures.

1.3. The purpose of this ASISA Guideline on Operational Risk ("**Guideline**") is therefore to provide guidance to ASISA members on the following aspects of operational risk, specifically as they relate to insurers.

1.3.1. definition of operational risk;

1.3.2. operational risk taxonomy;

1.3.3. reporting of operational risk events (including boundary events);

1.3.4. outsourcing.

1.4. Operational risk can have different applications for different members. Each member should accordingly assess the appropriateness of this Guideline in light of the scale, nature and complexity of its own activities and understand the types of operational risk that are relevant to its particular circumstances, including the potential sources of operational risks addressed in this Guideline.

1.5. This Guideline is being shared with ASISA members and the public at large for their consideration and voluntary implementation and is non-binding on ASISA members.

1.6. This Guideline should be reviewed as practices mature.

2. DEFINITION OF OPERATIONAL RISK

2.1. "Operational risk" is defined by the Basel Committee on Banking Supervision as "*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events*". This definition includes legal risk but excludes strategic and reputational risk. In essence, this definition indicates that operational risk stems from the influence and interaction of internal and external events in people, processes and technology applied to business processes.

2.2. It is recommended that insurers follow the aforementioned definition of "operational risk". Guidance on the inclusions and exclusions are provided below for further clarification (as adapted from the ORX Reference Taxonomy Guidelines):

2.2.1. **Legal Risk** (included) – The risk of execution errors in the legal procedures and processes. This would include, amongst others, mishandling of legal process, contractual rights or obligation failures and non-contractual rights/obligation failures.

2.2.2. **Strategic Risk** (excluded) - The risk that the current initiative is not consistent with the overall strategic objectives of the insurer and that the insurer may not have the **expertise to oversee, manage and monitor such risks.**

2.2.3. **Reputational Risk** (excluded) - The risk that the third party's conduct may not be consistent with the overall standards of the insurer or the stated practices (ethical or otherwise) of the insurer. This should not be confused with the potential for reputational impact of materialised operational risks.

2.3. In addition to the above, consideration should also be given to including the following risk types in the definition of operational risk as these risk types are primarily operational in nature, and its

management is key to the effective operations of Insurers. It should, however, be noted that while these are considered to be included in the definition of operational risk, this Guideline does not indicate in any way the operating model to be employed in ensuring management and oversight of these risks.

2.3.1. **Compliance Risk** - The risk of legal or regulatory sanctions, financial loss or reputational damage as a result of the failure of an insurer to comply with the applicable statutory, supervisory and regulatory requirements.

2.3.2. **Conduct Risk** - Failure to act in accordance with customers' best interests, fair market practices, and codes of conduct. Broadly defined as the risk that stems from the actions or inactions of an insurer and/or its employees or representatives that may lead to the lack of market integrity (such as anti-competitive behaviour), inappropriate behaviour towards customers, improper products and services and improper business practices..

3. OPERATIONAL RISK TAXONOMY

3.1. The nature, structure and interpretation of operational risk means that the taxonomy will vary from insurer to insurer. In order to drive some level of consistency across the financial services industry, it is recommended that the following sub risk types (as set out in the ORX Reference Taxonomy Guidelines) be considered,

Primary Risk Type	Sub Risk Type
	People
	Transaction Processing and Execution
	Technology
	Information Security (including cyber risk)
	Legal
	Regulatory Compliance

Operational Risk	Conduct
	Third Party
	External Fraud
	Internal Fraud
	Physical Security and Safety
	Business Continuity
	Financial Crime
	Statutory Reporting and Tax
	Data Management
	Model

3.2. It is also recommended that insurers align to the following operational risk loss event types defined at the category level 1 taxonomy as set out in the consultative paper, "*Sound Practices for the Management and Supervision of Operational Risk*," issued by the Basel Committee for the reporting of all operational risk loss events.

OR Event (Category level 1)	**Description with examples of insurance exposure**
Internal fraud	Acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involve at least one internal party. Examples: Employee theft, claim falsification
External fraud	Acts by a third party of a type intended to defraud, misappropriate property or circumvent the law. Examples: Claims fraud, falsifying application details.
Employment	Acts inconsistent with employment, health or safety laws or agreements,

practices and workplace safety	or which result in payment of personal injury claims, or claims relating to diversity/discrimination issues. Examples: Workers' compensation claims, violation of employee health and safety rules, organised labour activities, discrimination claims and general liability (for example, a customer slipping and falling at a branch office).
Clients, products and business practices	Unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product. Examples include fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering and sale of unauthorised products.
Damage to physical assets	Loss or damage to physical assets from natural disaster or other events. Examples: Vandalism, physical damage as a result of building renovations.
Business disruption and system failures.	Disruption of business or system failures. Examples include hardware and software failures, telecommunication problems and utility outages.
Execution, delivery and process management	Failed transaction processing or process management, and relations with trade counterparties and vendors. Examples include data entry errors, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty mis-performance and vendor disputes, poor change management failures leading to the product not being built as designed.

4. OPERATIONAL RISK EVENTS

4.1. Definition of an operational risk event

An "operational risk event" is an event leading to the actual outcome(s) of a business process

to differ from the expected outcome(s), due to inadequate or failed processes, people, and systems, or due to external factors. (See Reference 5 listed below).

4.2. **Losses and near misses**

4.2.1. There can be many types of events. Some events lead to a direct and/or indirect financial loss or a gain, other events do not lead to a direct financial impact (the Bank of International Settlements gives the example of an IT disruption in the trading system outside trading hours). While indirect losses are included in the definition of an operational risk event, an operational risk loss is a direct, negative and quantifiable impact on the profit and loss of the company due to an operational risk event. Operational risk events that do not lead to a direct loss or gain are defined as "near misses". The full definition of a near miss, is:

"*A risk event where inadequate or failed internal processes, people, systems or external events materialised but did not result in a direct loss to the organization. Typically, near misses includes incidents where the impact was prevented or avoided*."

Refer to no. 4 in the ToR: CRO Forum.

4.2.2. It is recommended that operational risk events that result in a financial gain also be considered as near misses and the loss be considered as zero. The financial gain should not be netted off against other operational risk losses.

4.3. **Reporting threshold**

It is recommended that all operational risk losses above an internally agreed threshold (in line with the size and complexity of the organisation) be recorded individually. In line with regulatory reporting requirements, it is recommended that this loss threshold be set at a maximum of R10 000 per event. It is recommended that all similar losses less than the internally agreed threshold be recorded on an aggregated basis. While losses could be aggregated, consideration should be given to the nature of the operational risk event. If the event may have resulted in material non-financial impact, it is recommended that it be recorded and managed individually. Where Insurers take the decision of not setting any internal threshold, consideration

should be given to the quantum and administrative impact of reporting all losses.

4.4. Data fields required for capturing, monitoring, and reporting operational losses

Organisations are constantly refining their internal processes for recording operational risk losses/events. The minimum data fields recommended should be those required to meet the relevant regulatory requirements for reporting. In addition, it is recommended that to enhance the ability to perform analysis and internal reporting of losses and events additional fields be considered. Below are some examples of additional fields.

Data field	Descriptor
Discovery date	Refers to the date that the event was discovered.
Recognition date	Refers to the date of the booking in the profit and loss statement of the loss associated with the event.
Root cause	Describes the root cause of the event. This is attained by conducting a root cause analysis.
Related business areas	Represents the business related to the event, excluding the business area where the event was suffered.
Insurable event	Was the event insurable?
Insurance recovery	How much was recovered from insurance if relevant.
Boundary event	Was this an event that was related to other risk types, e.g. Insurance risk suffered due to an operational failure; Credit risk loss suffered due to failure in the credit approval process.
Boundary event type	Type of Boundary event, e.g. Credit, Insurance, Market, etc.
Control enhancement	Were controls found to be deficient and what has been done to improve controls?

4.5. Boundary Events

4.5.1. The following is recommended regarding the reporting of boundary events:

4.5.1.1. An 'operational risk boundary event' be defined as an operational risk event (i.e. due to inadequate or failed internal processes, people, systems or from an external event) which triggers a consequence (e.g. financial loss) in another risk category (e.g. insurance, market, credit). Refer to no. 4 in the ToR: CRO Forum.

4.5.1.2. **Principle**: Where the boundary relates to a risk category that also attracts regulatory capital, the overriding principle be that an organisation only provides capital for the loss once, to avoid an instance of double counting.

4.5.1.3. **Reporting requirement**: The reporting of boundary events is only required when the operational risk contribution to that loss event can be calculated. Only the operational risk related amount of the loss should be reported. If this part cannot be identified due to the nature of the event, the event should not be reported to the loss database.

4.5.2. Operational risk is one of the several risk types that an insurance company faces and may be related to other risk types. Boundary events are events of which the cause is wholly or partially attributable to an operational failure, but for which the effects (economic or otherwise) are already explicitly or implicitly captured by another risk type, for which typically a separate model exists. The definition that is used to determine whether an event is a boundary event is based on the definition of the Bank of International Settlements (BIS):

"*Boundary events are partial or full operational risk contributions to credit risk, market risk, or insurance risk related losses*."

4.5.3. It is recommended that the reporting of boundary events is only required when the operational risk contribution to that loss event can be calculated. Boundary events should be 'flagged' in the loss database by indicating the associated risk type:

4.5.3.1. credit risk;

4.5.3.2. market risk;

4.5.3.3. insurance risk.

4.5.4. It is recommended that any boundary event be flagged, even if the operational risk contribution of the boundary loss is 100% of the total loss amount. Only the operational risk related amount of the loss should be reported. If this part cannot be identified due to the nature of the event, the event should not be reported to the loss database.

4.5.5. Banking definitions, as per the South African Reserve Bank. have created additional consistency in dealing with boundary events. It is recommended that for the insurance industry, agreement be reached on how insurance boundary events are treated. It is recommended that the guidelines for credit and market risk applied to the banking industry be adopted by the insurance industry to ensure consistency across the financial services industry.

5. OUTSOURCING

5.1. Requirements regarding outsourcing by an insurer are comprehensively set out in regulation. Activities are outsourced to providers for various reasons such as: it provides an opportunity for insurers to have access to expert skills without having to employ such a person on a full-time basis or in certain instances, the outsourced party offers various skills to the insurer that do not reside in one person, or such skills are needed on a temporary basis only and would not justify employing a person.

5.2. An insurer must maintain an appropriate level of contact with and implement processes for ensuring that the level and standard of service to the insurer and, where relevant, its policyholders, under an outsourcing arrangement for a material business activity or a binder function are appropriately monitored, managed, and reviewed. To achieve this an insurer must regularly assess the service provider's:

5.2.1. governance

5.2.2. risk management, and internal controls

5.2.3. ability to comply with applicable laws

5.2.4. operational and financial capability

5.2.5. level of performance.

References

1. Operational risk management: Practical implications for the South African insurance industry (M Martin and M Hayes, 2013)

2. Operational Risk Management for Insurers (Maria Isabel Martínez Torre-Enciso1 and Rafael Hernandez Barros, 2012)

3. Maria Isabel Martínez Torre-Enciso1 & Rafael Hernandez Barros (Deloitte, 2007)

4. CRO Forum. (2014, December). Minimum standards for reporting incidents to an insurance operational risk loss data consortium. The Netherlands.

5. Operational Risk data exchanged Association (ORX). (2020, April). Insurance Operational Risk Reporting Standards (I-ORRS). Switzerland.

DOCUMENT HISTORY

Date	Publication/amendment
22 July 2022	Approved by the Life & Risk Board Committee
30 July 2025	Competition law review changes

RESPONSIBLE SPA AND COMMITTEES

Responsible Board Committee	Life and Risk Board Committee
Responsible Standing Committee	
Responsible Senior Policy Advisor	ASISA Point Person to the Life and Risk Board Committee