Minimum standards for reporting incidents to an insurance operational risk loss data consortium

December 2014

CRO FORUM

Table of Contents

1 Introduction

This document describes the CRO Forum recommendation for minimum data standards for reporting loss events to an operational risk (OpRisk) loss data consortium for (re)insurance companies[1]. The standards have been developed by the OpRisk working group of the CRO Forum in 2014 to create common ground for multiple loss data consortiums (LDC) with different database providers, and to ensure compatibility between the different databases. In the development of these standards, the working group has built on existing materials from loss data consortiums ORIC and ORX, as well as existing Basel II standards.

It is important to note that the data standards described here are minimum standards only. This document does not aim to provide risk management principles or best practices for the loss data collection process in an insurance company. This document only provides minimum standards for reporting events to ensure compatibility between different databases, and to ensure a minimum level of quantification and qualitative risk management. Different providers can create additional standards and guidelines. However, when all data consortiums adhere to the standards described here, it is ensured that data is mutually exchangeable and easy to be merged.

The set of data standards comprises two types of fields. The first type are the fields that are essential for using the data for quantitative analysis ("*quantitative data fields*"), e.g. backtesting of OpRisk capital, benchmarking. The second type are elements that allow the data to be used for qualitative risk management purposes ("*qualitative data fields*"), e.g. internal control system effectiveness. Both types are described in this document.

In case of comments or questions regarding this set of standards, please contact the CRO Forum office at *croforum.office@kpmg.nl*.

[1] Whenever the term "insurance companies" is used in this document, it applies to both insurance and reinsurance companies. The losses to be registered in the consortium loss database include asset management losses as well.

2 Type of events

2.1 Losses and near misses

There can be many types of events. Some events lead to a financial loss or a gain, other events do not lead to a financial impact (the Bank of International Settlements gives the example of an IT disruption in the trading system outside trading hours[2]). Operational risk events that do not lead to a loss or gain are called "near misses". The full definition of a near miss, as used in this document, is:

Near miss is a risk event where inadequate or failed internal processes, people, systems or external events occurred but did not result in a direct or indirect impact to the organization. Typically, near misses are described as incidents that were prevented by circumstances not within the organisation's established control environment.

Only financial loss events are recorded. It is recognised that near misses can contain important information for risk management purposes. It is recommended that internal records for near gains and misses within the own organisation are maintained. In case an LDC wants to go beyond the minimum standards, and wants to include near misses in the collection process, the use of the abovementioned definition is encouraged.

2.2 Open and closed events

The general principle is to report both closed events and open events. In some case, there may be legal or compliance issues with reporting open events. Therefore, members can deviate from the principle if they have a good reason to do so.

2.3 Reporting threshold

There is no standard for the threshold to be used in reporting incidents to a loss data consortium. Any loss data consortium should apply a meaningful reporting threshold to eliminate the noise of small losses, while maintaining the benefits of the database.

[2] Bank of International Settlements, *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches*, June 2011.

3 List of data fields

There are fifteen data fields defined for quantitative purposes, and four data fields for qualitative purposes (to be used for events above the threshold of EUR 500k). The list below mentions each field with a short description. In sections 4 and 5, more detailed guidelines are provided for each data field.

3.1 Quantitative data fields

- *Event type level I*: Represents the 7 Basel II level 1 event type categories set by the Bank for International Settlements. The event type provides a classification for the event that caused the loss.
- *Event type level II:* Represents the Basel II level 2 event type categories, adjusted to the insurance business.
- *Occurrence date:* Refers to the date that the event occurred.
- *Discovery date:* Refers to the date that the event was discovered.
- *Booking date:* Refers to the date of the booking in the profit and loss statement (P&L) of the loss associated with the event.
- *Business line:* Indicates the part of the insurance company that is suffering the loss.
- *Gross loss amount*: Gives the total amount for the loss including all impact types.
- *Recovery amount*: Gives any amount recovered from third parties related to the event.
- *Recovery date*: Refers to the date that the recovery amount was booked (if any).
- *Currency:* Refers to the currency in which the loss is reported.
- *Location Level I:* The region in which the event occurred.
- *Location Level II:* The country in which the event occurred.
- *Type of boundary risk*: Indicates whether the loss is related to other risk types, for which usually separate models exist.
- *Status of loss event*: Indicates whether the loss is related to an open event, or whether the event is closed.
- *Reinsurance flag (yes/no)*: Indicates whether the loss originated in a reinsurance business unit.

3.2 Qualitative data fields

- *Root cause*: Describes the root cause of the event.
- *Function*: Represents the company function in which the loss originated.
- *Description*: Provides a free text description of the event of what happened, including the aspects relevant for risk management.
- *Benchmarking data:* Provides a basis for companies who want to apply scaling to the data in their models.

4 Quantitative data fields

4.1 Event type level I & Event type level II

Seven different event types are defined on Level I, in line with the Basel II definitions[3]. For each Level I event type, Level II event types are developed to provide more detail on the type of the event to answer the question "what has happened?". The Level II event types are closely related to the Basel event types, but some adjustments were made for the application to the insurance industry. The event types on both levels are listed below:

- **1: Internal Fraud**
  - *1.1: Unauthorised Activity*
  - *1.2: Internal Theft & Fraud*
  - *1.3: System Security Internal – Wilful Damage*
- **2: External Fraud**
  - *2.1: External Theft & Fraud*
  - *2.2: System Security External – Wilful Damage*
- **3: Employment Practices & Workplace Safety**
  - *3.1: Employee Relations and Employment Practices*
  - *3.2: Safe Workplace Environment*
  - *3.3: Diversity & Discrimination*
- **4: Clients, Products & Business Practices**
  - *4.1: Suitability, Disclosure & Fiduciary Duties*
  - *4.2: Improper Business or Market Practices*
  - *4.3: Product Flaws*
  - *4.4: Selection, Sponsorship & Exposure*
  - *4.5: Advisory Activities*
- **5: Damage to Physical Assets**
  - *5.1: Natural Disasters*
  - *5.2: Accidents & Public Safety*
  - *5.3: Wilful Damage & Terrorism*
- **6: Business Disruption and System Failure**
  - *6.1: Internal Business Disruptions and Internal System Failure*
  - *6.2: External Business Disruptions and External System Failure*
- **7: Execution, Delivery & Process Management**
  - *7.1: Transaction Capture, Execution & Maintenance*
  - *7.2: Monitoring & Reporting*
  - *7.3: Customer Intake & Documentation*
  - *7.4: Customer / Client Account Management*

[3] Bank of International Settlements, *Working Paper on the Regulatory Treatment of Operational Risk*, September 2011.

Details for the different event types (with examples) are provided in Appendix I.

4.2 Occurrence date

The occurrence date is defined as the date on which the event occurred. In case of a series of events, it is the first time that it occurred. If the exact date is not known, the first day of the month is used (even if it is not a working day).

4.3 Discovery date

The discovery date is defined as the date on which the event is discovered or identified.

4.4 Booking date (last)

The booking date is defined as the day on which the event is booked in the P&L (the final booking of a loss). The recovery date does not impact the booking date.

4.5 Business Line

Business lines represent cost- or profit centres where the loss is suffered. In reporting the business lines, there are the following options:

- *Non-life*
- *Life*
- *Health*
- *Asset Management/Investment Management*
- *Corporate*

If an event impacts more than one business line, the event needs to be reported in the business line which was impacted most by the event.

The category "Corporate" is to be used only for those events that cannot be linked to any of the other business lines. It is not meant to be an alternative for events that are difficult to allocate.

Reinsurance is not included as a separate business line, as reinsurance events may be related to "life", "non-life", etc. as well. This information would be lost if all reinsurance events would be reported in one business line. Therefore, a flag is included to indicate losses within reinsurance companies or reinsurance companies within an insurance group.

4.6 Gross loss amount

The gross loss amount equals the sum of all P&L impacts related to an operational risk event before potential recoveries. Net gains following from an operational loss event are not to be reported.

Elements to include in the gross loss are: fines, compensation payments, write-offs, restitutions, costs for external experts, replacement costs, stolen amounts, legal costs, communication expenses, investigation costs, severance payments or compensation), interest, additional costs for evoking recovery plans or business continuity plans, out-of-court agreements, and ex-gratia payments.

Not included are costs made even if the event did not occur, costs for improvements compared to the original situation, or overtime paid out. Opportunity costs and lost profit are also excluded.

As a result of a loss event, a timing loss can occur. Timing losses can be defined as the negative economic impacts booked in a fiscal period, due to events impacting the cash flows (lower cash in / higher cash out) of previous fiscal periods. In the loss database, timing losses should not be recorded. Potential fines, legal costs or costs resulting from the misstatement or late payment (based on a cost-of-capital basis) are seen as OpRisk events and should be included in the gross loss amount.

4.7 Recovery amount

The recovery amount is defined as any amount received back from third parties related to the particular event.

If the amount is (partially) recovered within five days after the booking date, the event is defined as a rapid recovery. In this case, the event should not be reported as a separate loss amount with a separate recovery amount, but rather as a loss with an adjusted loss amount. Rapid recoveries covering the total amount of the loss are considered as near misses, which should not be reported to the database.

The recovery amount does include recoveries from insurance. Reinsurance recoveries are not included in order to avoid making the data collection process too complicated. The number of events involving reinsurance recoveries is expected to be small, as reinsurance is only involved in boundary events.

4.8 Recovery date

The date of recovery is defined as the date that the recovery amount is booked (final booking) in the general ledger (if existing). In case of multiple recoveries, the date of the last recovery is used.

4.9 Currency

There are no standards on how to report the currency of loss events. However, losses will be displayed by a loss data consortium in a single currency to avoid identification of the company that submitted the event. In case of FX conversion, the date for the FX conversion is the booking date.

4.10 Location Level I and Location Level II

The location is reported using a Level I indicator for the region, and a level II field for the country. The regions and countries that can be used for reporting are shown in the table below. Submission should be on country level. Loss database consortiums may only provide regional information on a level that does not compromise the anonymity of the companies reporting the data.

Level I options	**Level II options**
Asia & Oceania	Afghanistan, Australia, Bangladesh, Bhutan, Brunei, Burma, Cambodia, China, Christmas Island (Australia), Cocos (Keeling) Islands (Australia), Cook Islands (NZ), Federated States of Micronesia, Fiji, Guinea, Hong Kong (China), India, Indonesia, Japan, Kazakhstan, Kiribati, Kyrgyzstan, Laos, Macau(China), Malaysia, Maldives, Marshall Islands, Mongolia, Nauru, Nepal, New Zealand, Niue (NZ), Norfolk Island (Australia), North Korea, Pakistan, Palau, Papua New Guinea, Philippines, Samoa, Singapore, Solomon Islands, South Korea, Sri Lanka, Taiwan, Tajikistan, Thailand, Timor-Leste, Tokelau (NZ), Tonga, Turkmenistan, Tuvalu, Uzbekistan, Vanuatu, Vietnam
Eastern Europe	Albania, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Georgia, Hungary, Kosovo, Latvia, Lithuania, Macedonia, Moldov, Montenegro, Poland, Romania, Russia, Serbia, Slovakia, Slovenia, Ukraine

Latin & South America	Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Sao Tom and Principe, Suriname, Trinidad and Tobago, Uruguay, Venezuela
Middle East & Africa	Algeria, Angola, Bahrain, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guinea-Bissau, Iran, Iraq, Israel, Ivory Coast, Jordan, Kenya, Kuwait, Lebanon, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Oman, Palestine, Qatar, Republic of the Congo, Rwanda, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Swaziland, Syria, Tanzania, Togo, Tunisia, Turkey, Uganda, United Arab Emirates, Western Sahara, Yemen, Zambia, Zimbabwe
North America	American Samoa (USA), Canada, Guam (USA), Puerto Rico, United States, United States Virgin Islands (USA)
Western Europe	Aland Islands (Finland), Andorra, Anguilla (UK), Aruba (Netherlands), Austria, Belgium, Bermuda (UK), British Virgin Islands (UK), Caribbean Netherlands (Netherlands), Cayman Islands (UK), Curacao (Netherlands), Cyprus, Denmark, Falkland Islands (UK), Faroe Islands (Denmark), Finland, France, French Guiana (France), French Polynesia (France), Germany, Gibraltar (UK), Greece, Greenland (Denmark), Guadeloupe (France), Guernsey (UK), Iceland, Ireland, Isle of Man (UK), Italy, Jersey (UK), Liechtenstein, Luxembourg, Malta, Martinique (France), Mayotte (France), Monaco, Montserrat (UK), Netherlands, New Caledonia (France), Northern Mariana Islands (USA), Norway, Pitcairn Islands (UK), Portugal, Reunion (France), Saint Barthelemy (France), Saint Helena, Ascension and Tristan da Cunha (UK), Saint Martin (France), Saint Pierre and Miquelon (France), San Marino, Sint Maarten (Netherlands), Spain, Svalbard and Jan Mayen (Norway), Sweden, Switzerland, Turks and Caicos Islands (UK), United Kingdom, Vatican City, Wallis and Futuna (France)

4.11 Type of Boundary risk

Operational risk is one of the several risk types that an insurance company faces, and is often 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 exist. 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)[4]:

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

The reporting of boundary events is only required when the OpRisk contribution to that loss event can be calculated. Boundary events should be "flagged" in the loss database by indicating the associated risk type:

- *Credit risk*
- *Market risk*
- *Insurance risk*

[4] Bank of International Settlements, Principles for the Sound Management of Operational Risk, June 2011.

Any boundary event should 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.

Strategic risk events, business risk events and reputational risk events with a boundary OpRisk contribution are not recorded as an operational risk event. Although a strategic financial loss (for example caused by an improper due diligence process) can be considered as boundary operational risk, it is unlikely that it is possible to determine the loss amount.

Because of the complexity, some examples of boundary events (and events that are not considered boundary events) are provided in Appendix II.

4.12 Status of loss event

The status field shows whether the loss is related to an open event, or whether the event is closed/settled. In principle all events, open and closed, need to be submitted. Whenever there are company specific or event specific reasons not to do so, open events may be disregarded when submitting data to a loss data consortium.

4.13 Reinsurance flag (yes/no)

To allow for filtering of data for reinsurers (or reinsurance companies within an insurance group), it is reported whether the event originated in a reinsurance business unit. The rationale is that the loss profile for reinsurers might differ from the loss profile for direct insurers.

As with any data field, this flag can only be used for analysis purposes when there are sufficient companies submitting losses to ensure anonymity.

5 Qualitative data fields

For events leading to large losses, additional data fields are required to support a qualitative analysis. The threshold is set at EUR 500,000. Above this threshold, more detailed information needs to be provided using the qualitative data fields.

5.1 Root cause

The list of options for indicating the root cause of an event (Level 1 and Level 2) is shown below. In case of multiple root causes, the general principle is to attribute the event to the category with the largest impact on the event.

- **People**
  - *Employee qualification, technical skills, competencies*
  - *Employee availability (composition of team, overwork, illness)*
  - *Employee conduct (lack of: motivation, integrity, honesty)*
  - *Human error, oversight error*
  - *Others*
- **System**
  - *Insufficient IT/Infrastructure, hard- and software availability, capacity*
  - *Insufficient IT security*
  - *Insufficient supply (energy, electricity, telecommunications, etc.)*
  - *Others*
- **Process**
  - *Inadequate process/control design and workflows*
  - *Inadequate process/control documentation, procedures, policies*
  - *Inadequate business continuity & crisis management*
  - *Inadequate vendors/outsourcing agreements & management*
  - *Inadequate data quality*
  - *Lack of automatisation*
  - *Others*
- **External causes**
  - *Natural disaster*
  - *Epidemic/Pandemic*
  - *Default/Misconduct of third party (vendor/service provider/outsourcer)*
  - *Inferior quality or unsatisfactory adherence to delivery deadlines of a third party (vendor/service provider/outsourcer)*
  - *Man-made catastrophe (terrorism, vandalism, criminal acts, etc.)*
  - *Changes in political environment*
  - *Changes in legal or regulatory environment or practices*
  - *Client fraud*
  - *Intermediary fraud/misconduct*

– *Others*

Examples for each root cause are provided in Appendix III.

5.2 Function

The following function categories have been defined (in alphabetical order) to describe the function where the event originated:

1 Accounting & finance
2 Actuarial pricing
3 Actuarial reserving
4 Audit
5 Claims handling
6 Customer service & policy administration
7 Facilities
8 HR
9 Investment & treasury
10 IT
11 Legal & compliance
12 Marketing
13 Outsourcing
14 Outward reinsurance
15 Procurement
16 Product development
17 Risk management
18 Sales & distribution
19 Tax
20 Underwriting
21 Other

When the event originated in multiple functions, the event needs to be reported in the "Other" category.

5.3 Description

The description is an open ended data field. The following aspects need to be included in the description:

- *What happened?*
- *Why did it happen?*
- *How is the impact calculated? The type of costs that were included in the analysis, plus details of the calculation if necessary (whenever possible within the privacy boundaries).*
- *Any mitigation actions/response by management to avoid future events (on a high level basis).*

For reporting, it is essential to avoid: abbreviations understandable for third parties, names of employees, counterparties, or department names. To guarantee anonymity of the data submission, each company is responsible for making the description such that the event can never be linked to the company.

5.4 Benchmarking data

To allow for scaling data, company specific data needs to be reported:

- *Gross Written Premium (GWP)*
- *Assets under management*
- *Operating profit*

The values for these parameters need to be reported separately for each business line.

6 Other risks

6.1 Legal and regulatory risk

Regarding legal and regulatory risk, an event needs to have an element of operational failure in order to qualify as operational risk. A change in regulations or laws can be an OpRisk event, depending on the time period to which the change is related:

- Future changes of regulations or laws are not OpRisk events.
- Retrospective changes of laws, with the consequence of a P&L impact, qualify as OpRisk events.

In line with the event type definitions, any breach of current regulation is an OpRisk event.

7 Appendix I: Event types

This appendix provides detailed descriptions and examples for the event types.

Level I	Name and description	
1	**Internal Fraud** Internal fraud risk is the risk due to deliberate abuse of procedures, systems, assets, products and/or services of a company involving at least one internal staff member (i.e. on payroll of the company) who intend to deceitfully or unlawfully benefit themselves or others.	
Level II	**Name and description**	**Examples**
1.1	**Unauthorised Activity** Breaches of authority which are not criminal activity. E.g. employee may be dismissed but not prosecuted. Includes the risk of loss caused by unauthorised employee activities, approvals or overstepping of authority.	Intentional mis-marking of positions. Invalid authorization of exposures or expenditures. Mandate breaches.
1.2	**Internal Theft & Fraud** Activity is criminal in nature and would result in prosecution. Includes the risk of misappropriation of assets, collusive and corruptive fraud and financial reporting fraud risk.	Embezzlement. Claim fabrication. Forgery. Kickbacks/bribes. Extortion. Expense reimbursement schemes. Payroll schemes. Insider trading for personal gain. Deliberate misstatements or omissions of amounts or disclosures of financial statements (e.g. concealed liabilities, fictitious revenues, improper disclosures).
1.3	**System Security Internal – Wilful Damage** Includes the risk of financial loss due to activities going undetected such as unauthorised changes to key security settings, repeated unsuccessful attempts to log into a sensitive system, and insertion of malicious software.	Unauthorized appropriation of confidential information whether in electronic or paper format. Computer malevolence (e.g. viruses, files destruction, hacking, denial of service attacks). Social engineering (e.g. faking the account of a colleague).
Notes: The key difference between Event type 1 and Event type 2 is the involvement of people on the payroll of the company. If this involvement exists, it is Internal Fraud, if this involvement does not exist, it is External Fraud. **Fraud by tied agents (meaning agents which only sell own insurance products) is considered as internal fraud.**		

Level I	Name and description	
2	**External Fraud** Events arising from acts of fraud and thefts, or intentional circumvention of the law, actuated by third parties, including customers, vendors and outsource companies (including sub-vendors and sub-contractors), with the goal of obtaining a personal benefit, damaging the Company or its counterparties (for which the Company pay), or damage Company's assets. Includes all forms of cyber risk, and frauds by clients and external parties (i.e. parties which do not collaborate usually with the Company and have no access to the Company's systems, such as non-mechanized brokers).	
Level II	**Name and description**	**Examples**
2.1	**External Theft & Fraud**	Theft of Company's assets such as personal computer or vehicles. Sale of confidential

	Theft/Robbery of tangible and intangible assets by third parties (without violation of Company system). Fraud by third parties, including customers, vendors and outsource companies, for the purpose of personal economic advantage and causing damage to the Company. This does not include: a) Collusion with a member of staff which is considered Internal Fraud. b) System related fraud.	information to third parties. Industrial espionage. Intellectual property theft. Cheques theft. Fake claims. Fraudulent surrenders. False certificates or medical records. Fake car theft. Fraudulent estimation of damage. Non-existent damaged reported in claims request. False witnesses. Fraudulent change of beneficiary. Policy written by false agents or false agencies. Misrepresentation on risk assets by customers. Fraud by financial advisors or brokers.
2.2	**System Security External – Wilful Damage** Hacking or attempt to access Company systems, improper use and manipulation of information or to stole or damage data on systems.	Theft of data/files information. Unauthorized appropriation of confidential information whether in electronic or paper format. Computer malevolence (e.g. viruses, files destruction, hacking, denial of service attacks). Social engineering (e.g. faking the account of a colleague).
Notes: See comments for Event type 1.		

Level I	**Name and description**	
3	**Employment Practices & workplace Safety** Events arising from acts/omissions, intentional or unintentional, inconsistent with applicable laws on employment relation, health, safety and diversity/discrimination acts the Company is responsible for.	
Level II	**Name and description**	**Examples**
3.1	**Employee Relations and Employment practices** Events related to mistakes or impermissible actions towards employees in the relationships with the Company, due to the failure to comply with the existing rules, laws, regulations related to employment relations, internal codes of conduct, and due to incidents related to Internal labour disruptions.	Breach of arrangements concerning the protection of a staff member's private life. Breach of human resource regulations (labour rights, collective conventions). Employee without any employment contract. Errors in employment contract. Change of contract without employee's agreement. Recruitment cancelled after contract signed. Contract termination without justifications. Lawsuits in case of an employee's illness or injury. Lawsuits related to calculation of tax and benefit positions. Lawsuits related to calculation of salary. Invasion of privacy.
3.2	**Safe Workplace Environment** Events related to employee claims for personal injury and lack of safety in the workplace for employees and third parties, due to the failure to comply with the existing laws on health and safety in the workplace. Under this category falls the failure to comply with mandatory worker insurance programs (in case of an accident).	Employee health and safety rules events (e.g. accidents at work or occupational diseases). Events relating to general liability (e.g. slips and falls of customers, partners or suppliers). Failure to comply with a relevant health and workplace safety regulation. Workers compensation.
3.3	**Diversity & Discrimination**	The bullying, harassment, abuse or molestation of a member of staff.

	Events related to workplace equality and discrimination arising under employment laws or internal company rules. Workplace and employment discrimination events should be distinguished from "public" diversity or discrimination events involving clients or citizens in general. The latter should be recorded under the "Improper Business or Market Practices" sub-category.	Lawsuits related to discrimination (related to gender, race, religion, age, nationality, etc.). Favouritism towards some employees (hiding their inappropriate behaviour).

Notes:

Main features:

- Involvement of employees with the Company's liability (meaning only employees, not internal parties).
- The ''Safe Workplace Environment'' category includes third parties involved in events occurred on property for which the Company is responsible.

Main distinctions:

- Robbery events are excluded.
- Disaster events are excluded.
- Only employees are meant and not the internal parties in general sense.

Level I	**Name and description**	
4	**Clients, Products & Business Practices** Unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements) and corporate stakeholders e.g. regulators, or from the nature or design of a product.	
Level II	**Name and description**	**Examples**
4.1	**Suitability, Disclosure & Fiduciary** The suitability, disclosure and fiduciary duty sub-category covers operational risk events arising from regulatory breaches or failures that impact customers, clients or trading partners.	Shareholder's liability. Fiduciary breaches / guideline violations. Suitability / disclosure issues. Retail consumer disclosure violations. Breach of privacy. Misuse / non intentional disclosure of confidential information. Aggressive sales. deceptive sales practice. concealment. Misselling. Account churning. Conduct risk beyond breaching laws. Violation of data protection laws.
4.2	**Improper Business or Market Practices** The improper business or market practices sub-category covers operational risk events arising due to alleged improper business practice.	Anti-trust behaviour. Improper external reporting practices. Improper trade / market practices. Market manipulation. Insider trading (on the firms account / for the companies benefit, if for individual benefit it is internal fraud). Unlicensed activities whether products or services. Money laundering activities. Inappropriate discrimination / diversity events in the marketplace or applying to the general public. Violation of substantive business contractual reserves. Lack of compliance with regulations or industry standards. Failed reporting requirements (to clients). Breach of sanctions and embargos. Retrospective change of law or regulations.

4.3	**Product Flaws** The product flaws sub-category covers events where the product was not correctly designed or priced (e.g. due to model errors). This includes retroactive legal changes.	Inadequate model implementation (e.g. in pricing models)/ model errors. Breach of pricing policy. Non-compliance of products with applicable internal or external requirements. Inadequate approval/certification proceeding for new products and new activities. Inadequate processes concerning complex and sensitive operations.
4.4	**Selection, Sponsorship & Exposure** The selection, sponsorship and exposure sub-category covers events arising due to a failure to properly investigate a client business partner in accordance with internal guidelines or arising due to unplanned costs.	Losses incurred due to a company exceeding the exposure limits for business partners (excluding clients). Politically Exposed Person screening. Improper business partner due diligence or improper RFP process. Failures in reinsurance purchase.
4.5	**Advisory Activities** The advisory activities sub-category should be used where an operational risk event arises due to a failure to meet obligations written in the advisory contract.	Incidents related to consultancy type of business. Client is not given the service that they have been led to believe they would receive. Inappropriate performance of advisory activity.
Notes: Categories 4 and 7 have similarities as they are both dealing with client related processes. In general, the events in Level I category 4 will be related to incidents were a law is violated, and the incidents in Level I category 7 will be related to mistakes without breaching a law.		

Level I	**Name and description**	
5	**Damage to Physical Assets** Losses arising from loss or damage to physical assets from natural disasters or other events.	
Level II	**Name and description**	**Examples**
5.1	**Natural disasters** Losses to physical assets as a consequence from adverse events from nature or climate.	Earthquake. Tsunami. Flood. Storm. Hail / Snow. Storm surge. Mudslide. Landslide.
5.2	**Accidents & Public Safety** Accidents, leading to damage of physical assets, or threatening employees or the public.	Fire. Explosion. Pipe break. Malfunction of infrastructure. Collapse of buildings. A visitor to the premise is injured as a result of one of these events.
5.3	**Wilful Damage & Terrorism** Damage to physical assets through wilful damage by terrorists or individual or groups.	Terrorist attack. Arson. Explosion (wilful. rather than accidental). Threat to employee wellbeing by a 3rd party. Political demonstrations. Rioting (civil unrest).
Notes: -		

Level I	**Name and description**
6	**Business Disruption and System Failure** Loss events associated with the interruption of business activity due to internal or external system and/or communication system failures, the inaccessibility of information and/or the unavailability of utilities and other externally driven business disruptions which may harm also personnel.

Level II	Name and description	Examples
6.1	**Internal System Failure** Loss events associated with the interruption of business activity due to internal system dysfunction, end user computing dysfunction or breakdown and/or internal communication system failures and/or the inaccessibility of information and/or loss of data	Internal Software failures. Internal System unavailability/downtimes (due to system bugs). Internal System performance problems. Internal Server or host performance problems. Internal Hardware outages. Internal network outage. Internal Loss of data.
6.2	**External System Failure** Loss events associated with the interruption of business activity due to external system, external IT supplier failures and/or external communication system failures, and/or unavailability of public utilities.	External Software failures. External System unavailability/downtimes due to system bugs. External System performance problems. External Server or host performance problems. External Hardware outages. External network outage. External Loss of data. Utility disruptions. External telecommunications network outage. Transportation disruptions. Pandemic/epidemic related disruptions.
Notes: A subsidiary that is under control of the company is considered internal.		

Level I	Name and description	
7	**Execution, Delivery & Process Management** Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.	
Level II	**Name and description**	**Examples**
7.1	**Transaction Capture, Execution & Maintenance** Failures in timeliness, completeness or appropriateness of the process.	Miscommunication. Data entry. Maintenance or loading error e.g. data quality issues. Missed deadline or responsibility. Model / system mis-operation e.g. using old data. Wrong data or wrong assumptions. Accounting error / entity attribution error. Other transaction process task mis-performance. Delivery failure. Collateral management failure. Reference Data Maintenance. Incorrect registration of a client switching funds in a unit linked project. Wrong calculation of reserves. Duplicate payments. Mistakes in commission calculations. Derivatives failures.
7.2	**Monitoring & Reporting** Untimely, incorrect, or inappropriate reporting to regulators or other governing bodies.	Failed mandatory reporting obligation e.g. reporting to governing bodies. Inaccurate external report (loss or fine incurred) e.g. quarterly fillings. Wrong tax filings.
7.3	**Customer Intake & Documentation** Incidents arising from process failure related to new clients (not related to a violation of laws).	Client permissions / disclaimers missing. Legal documents missing / incomplete / not "fit for purpose" / inadequately executed. Issues with regular client onboarding process. Missing risk assessment in the underwriting process. Other failures (without breaching laws).

7.4	**Customer / Client Account Management** Incidents from failed maintenance and administration of existing client records.	Unapproved access given to accounts. Incorrect client records (loss incurred). Negligent loss or damage of client assets. Incorrect payments to clients due to incorrect client status. Incorrect adjustments to contracts.
Notes: Type 7.4 is related to "business as usual" processes for existing clients. In contrast 7.3 relates to processes related to new clients. On the relation between Level I types 4 and 7, see the notes under type 4 in this appendix.		

8 Appendix II: Boundary events

To support the decision process of whether an event is a boundary event or not, the following tables provide examples of boundary events, the loss amount to be reported to the database for such events, or the event type in case the event is not a boundary event.

Boundary event examples

Associated risk	Activity	Description	Boundary event?	Loss amount
Market Risk	Asset valuation	Price fixing in collaboration with the counterparty so that the company suffers the loss.	Yes	Difference with actual price
Market Risk	Hedging	Non-hedging, over-hedging or under-hedging leading to a loss.	For asset manager: No For insurance: Yes	Loss caused by the hedging mistake
Market Risk	Position taking	Error in market order (mix sell with buy, mix amount with number of shares) leading to an involuntary limit breach.	For asset manager: No For insurance: Yes	Loss caused by the error
Market Risk	Position taking	Acquisition of assets not allowed by the investment policy.	Yes	Loss/gain after unwinding the transaction
Market Risk	Asset valuation	Error in the pricing model for derivatives.	Yes	Difference with actual price
Credit risk	Asset valuation	Counterparty default and guarantee could not be executed.	Yes	Loss caused missing or wrong set-up of the guarantee
Insurance risk (non-life)	Claims handling	Payment of false or fraudulent claims (claims fraud).	Yes	Total amount of false claim
Insurance risk (non-life)	Claims handling	Deliberate overestimation by insurance assessor.	Yes	Only the overestimation part
Insurance risk (non-life)	Claims handling	Involuntary error in applying deductible or limit.	Yes	The amount paid that should have been deducted (if the amount is less than the deductible, use the full amount)
Insurance risk (non-life)	Data entry	Higher claims because of a non-authorized change in policy conditions or in policy premium.	Yes	The increase in claim
Insurance risk (non-life)	Claims handling	Legal litigation (or settlement) in claims payment. Disagreement with client on claim height, caused by errors/omissions in contract.	Yes	Anything above the expected amount, plus the legal costs
Insurance risk (non-life)	Claims handling	Jurisprudential decision impacting negatively entire portfolio of existing liabilities.	If underlying internal OpRisk error or retrospective changes in legislation: Yes	Change in liabilities

			A difference in interpretation: No	
Insurance risk (life)	Claims handling	Falsification of the cause of death (e.g. suicide disguised as accident).	Yes	Claims amount
Insurance risk (life)	Claims handling	Non reported death (for longevity guarantees).	Yes	Claims amount that is paid too much or too long
Insurance risk (life)	Position taking	Client falsifies information in order to get the desired insurance policy.	Yes	Amount paid out

Not-boundary event examples

Most examples below are not considered boundary events as they are pure operational risk events.

Associated risk	**Activity**	**Description**	**Event type level II**
Market Risk	Position taking	Unauthorised / fictitious position taking resulting in a false representation of the actual position of the portfolio.	Unauthorised activity
Market Risk	Securities management	Errors or mistakes on securities positions (e.g. derivatives) managed outside of the IT system.	Transaction capture, execution and maintenance
Credit risk	Position taking	Bankruptcy of an broker or tied agent unable to pay collected premiums to the insurance company.	Internal or External fraud
Credit risk	Position taking	Supplier or vendor going bankrupt. Insurer faces compensation payments because of failed delivery to clients.	Transaction capture, execution and maintenance
Credit risk	Asset valuation	Counterparty bankruptcy and sending falsified information to improve its credit rating or hide its insolvency.	External fraud
Credit risk	Credit management	Failures in debt collection processes when a creditor defaults (e.g. exceeded legal limitation period for lodging the credit claim).	Transaction capture, execution and maintenance
Credit risk	Credit management	Inability to use the guarantee covering the credit when a creditor defaults (e.g. by loss of contract).	Transaction capture, execution and maintenance
Insurance risk (non-life)	Data entry	Errors in data entry on policy contracts and conditions (e.g. the client's conditions as agreed upon during the underwriting process are wrongly recorded leading to less premiums received).	Transaction capture, execution and maintenance
Insurance risk (non-life)	Position / risk coverage	Reinsurance premium not paid or paid late.	Transaction capture, execution and maintenance
Insurance risk (non-life)	Position / risk coverage	Breach of contract agreements (e.g. information and data sharing agreements).	Transaction capture, execution and maintenance
Insurance risk (non-life)	Position / risk coverage	Failure to transfer a claim to a reinsurer or claim communicated beyond deadline.	Transaction capture, execution and maintenance

Insurance risk (non-life)	Claims handling	Double claims payment (to the same client).	Transaction capture, execution and maintenance
Insurance risk (non-life)	Data entry	Inability to load specific policy guarantees or conditions even if authorized (e.g. because of limitations in the IT systems) – usually corporate or high severity risks (e.g. cat risk).	Transaction capture, execution and maintenance
Insurance risk (life)	Position taking	Counterfeit life insurance policy manually processed (i.e. not in the systems) where the company remains liable (for instance Ponzi scheme by an agent).	External fraud
Insurance risk (life)	Claims handling	Payment to wrong beneficiary (fraud).	Transaction capture, execution and maintenance
Insurance risk (life)	New Product	Launch of product lacking the proper authorisations and leading to restitution of all premiums collected.	Clients, Products, and Business practices
Insurance risk (life)	New Product	Error when publishing interest rate.	Transaction capture, execution and maintenance
Insurance risk (life)	Position taking	Client buys insurance but does not get full information about risks and disclaimers – later sues the insurer.	Suitability, Disclosure & Fiduciary
Insurance risk (life)	New Product	Misinterpretation of term sheet conditions.	Clients, Products, and Business practices

9 Appendix III: Root causes

The table below provides examples of the different Level 1 and Level 2 root causes.

Level 1	Level 2	Explanations and examples
People	Employee qualification, technical skills, competences	- Inadequate identification of competences required for an organizational role - Ineffective evaluation of personnel competences and technical skills - Inadequate recruiting and selection of human resources - Inadequate personnel training
	Employee availability (composition of team, overwork, illness)	- Capacity problems - Inadequate workforce planning
	Employee conduct (lack of: motivation, integrity, honesty)	- Inadequate mobility plans, job rotation plans - Inadequate identification of talents and key personnel - Inadequate verification of references and ethical profile of the applicant - Inadequate valuation of human resources performances - Inadequate incentives and compensation systems
	Human error, oversight error	- Misunderstanding, exceeded deadline, incorrect data input or storage of data - Inadequate diffusion of control culture
	Others	
System	Insufficient IT/Infrastructure, hard- and software availability, capacity	- Including software or programming errors - Lack/inadequacy of maintenance and updating of IT infrastructure (hardware or software) - Inadequate technical support - Lack/inadequacy of appropriate measures and processes for reporting IT failures, for managing incidents and data security issues - Lack/inadequacy of IT infrastructure (software or hardware) licensing management
	Insufficient IT security	- Insufficient firewalls, virus detectors, insufficient building and facility security - Lack/inadequacy of measures for controlling logical access and for tracking activities/operations - Lack/inadequacy of backup procedures of archives and software - Lack/inadequacy of a disaster recovery plan
	Insufficient supply (energy, electricity, telecommunications, etc.)	- Outages of telecommunication, outlook outages - Inadequate selection and management of telecommunication infrastructures and utility service - Lack/inadequacy of maintenance and technical support for the telecommunication infrastructure and utility service
	Others	
Process	Inadequate process/control design and workflows	- Organisation, clarity of roles and responsibilities, too many interfaces, complexity, insufficient product development, inadequate project management - Inadequate organizational unit sizing - Inadequate definition of proxies and authorizations
	Inadequate process/control documentation, procedures, policies	- Including escalation procedures, ambiguous assignment of tasks, competencies or responsibilities - Inefficiencies in the measurement and reporting of process performances

	Inadequate business continuity & crisis management	- Inappropriate plan, inappropriate recovery site (e.g. too near to main office) , lack of regular testing, lack of proper communication plans. - Lack of business continuity plan related to human resources.
	Inadequate vendors/outsourcing agreements & management	- Inadequate preliminary evaluation of the nature and importance of activities to be outsourced. - Inadequate outsourcing contracts and monitoring of Service Level Agreements (SLA).
	Inadequate data quality	
	Lack of automatisation	- Insufficient end-user computing management, manual interfaces and hand-offs. - Excessive use of spreadsheet.
	Others	
External Causes	Natural disaster	Flood, fire, storm, earthquakes, etc.
	Epidemic/Pandemic	Diseases.
	Default/Misconduct of third party (vendor/service provider/outsourcer)	Includes fraud and bankruptcy of a third party, counterparty, provider.
	Inferior quality or unsatisfactory adherence to delivery deadlines of a third party (vendor/service provider/outsourcer)	Outsourcer, vendor, counterparty.
	Man-made catastrophe (terrorism, vandalism, criminal acts, etc.)	
	Changes in political environment	Strikes, civil war.
	Changes in legal or regulatory environment or practices	Unfavorable court decisions, retroactive changes of law.
	Client fraud	Claims fraud.
	Intermediary fraud/misconduct	Fraud, misconduct, data leakage, misselling of sales intermediaries like brokers, financial advisors where the company is liable for.
	Others	

Disclaimer:

Dutch law is applicable to the use of this publication. Any dispute arising out of such use will be brought before the court of Amsterdam, the Netherlands. The material and conclusions contained in this publication are for information purposes only and the editor and author(s) offer(s) no guarantee for the accuracy and completeness of its contents. All liability for the accuracy and completeness or for any damages resulting from the use of the information herein is expressly excluded. Under no circumstances shall the CRO Forum or any of its member organisations be liable for any financial or consequential loss relating to this publication. The contents of this publication are protected by copyright law. The further publication of such contents is only allowed after prior written approval of CRO Forum.

The CRO Forum is supported by a Secretariat that is run by
KPMG Advisory N.V.

Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands
www.thecroforum.org