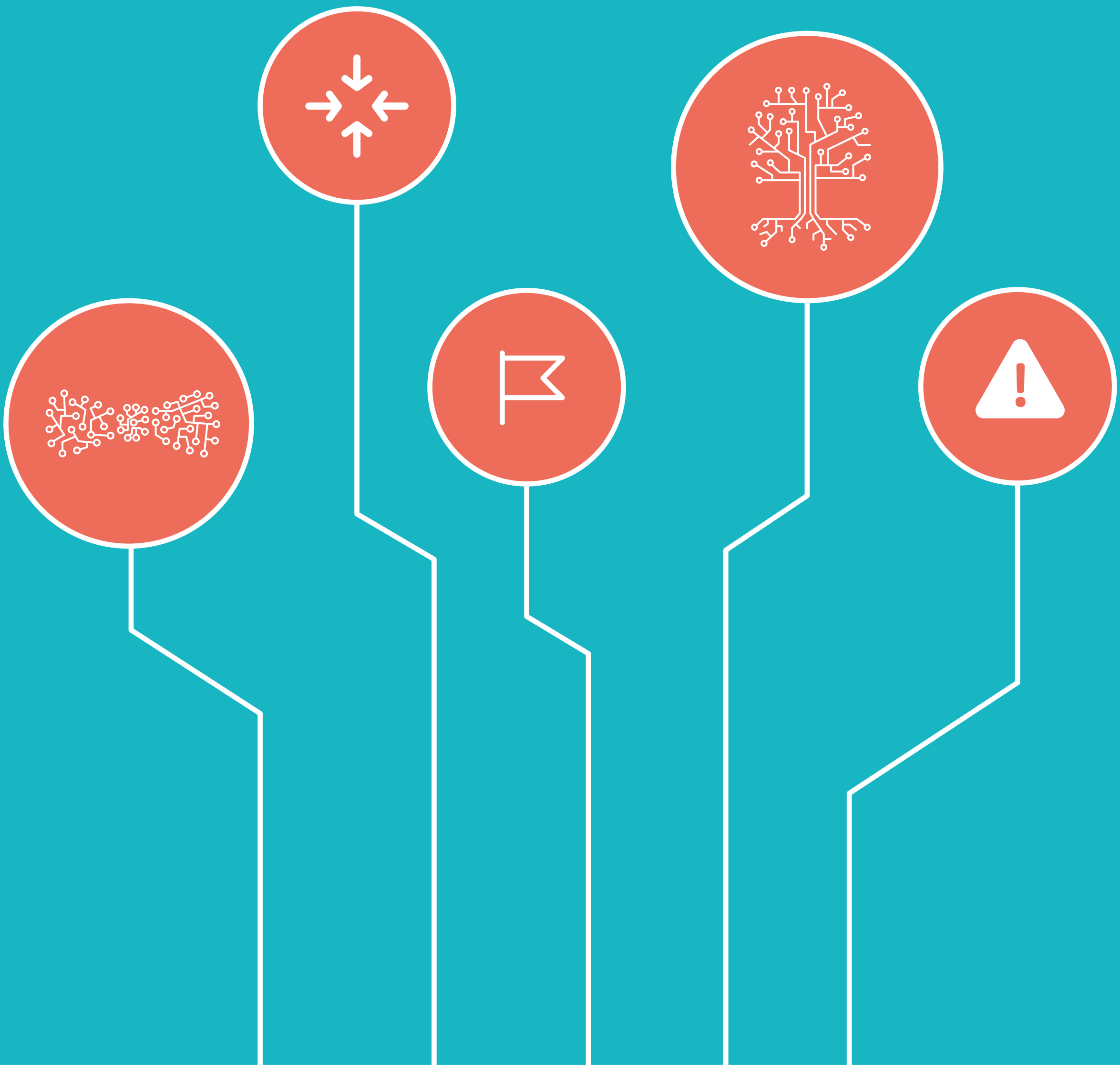
Extended ORX Reference Taxonomy for operational and non-financial risk - Causes & Impacts

FULL REPORT - NOVEMBER 2020



OLIVER WYMAN

O.R.X

ORX contacts:

Dr Luke Carrivick
Director of Research and Information

luke.carrivick@orx.org

Steve Bishop
Head of Risk Information & Insurance

steve.bishop@orx.org

Oliver Wyman contacts:

Tom Ivell
Partner

thomas.ivell@oliverwyman.com

Ramy Farha
Partner

ramy.farha@oliverwyman.com

Valerie Wong
Principal

valerie.wong@oliverwyman.com

Follow ORX:

@ORX_Association

@ORX_Association

Follow Oliver Wyman:

@Oliver Wyman

@OliverWyman

orx.org | oliverwyman.com

Executive summary

The next phase for this important strategic priority

In November 2019, we published the ORX Reference Taxonomy for Operational and Non-financial Risk. At the time, we stated our belief that this is an important strategic development for the risk management community. It creates a common point of reference and thereby solid ground for industry discussion regarding the development of operational risk taxonomies and lays the foundations for the consistent industry sharing of risk insights and data for the years to come.

Based on the taxonomies of 60 financial services firms, the ORX Reference Taxonomy reflects the changes we have witnessed in the operational risk profile over the last 15 years. Risks such as cyber, conduct and third party are included and are described in a way that aligns to the risk priorities of an organisation, whilst the taxonomy still retains a clear link back to the Basel Event Types.

Industry feedback on the reference taxonomy has been positive. Institutions are increasingly using it for benchmarking and to support development of their own taxonomies; a number are even beginning to fully adopt the taxonomy. ORX has also implemented the taxonomy into ORX News to test coherence and to provide enhanced functionality. Subscribers can now filter, search and report on publicly known events using these more contemporary categories in the ORX Reference Taxonomy.

The Extended ORX Reference Taxonomy

It became clear when developing the 2019 publication that complementary cause and impact categories would support the understanding and use of the ORX Reference Taxonomy. Covering the cause-event-impact 'Bow Tie' model in the Extended ORX Reference Taxonomy would provide a more insightful view of how the taxonomy can be applied in practice.

Applying a similar methodology to last year, and again supported by Oliver Wyman, the reference cause and impact categories presented have also been developed using the wisdom of crowds. These categories consolidate taxonomy information collected from 50 financial services firms into a single view of causes and impacts. They are also a first iteration, designed to complement and extend the existing ORX Reference Taxonomy. They should encourage discussion, continue to promote developments in taxonomies, as well as help lead the industry towards a convergence of approaches.

Key considerations

When reading this report and reviewing the results it is important to consider:

1. It is a reference

The published categories are a reference and are part of the Extended ORX Reference Taxonomy. They will not yet be adopted in ORX loss data services, but can be used as a resource to encourage thinking, to benchmark and enhance your existing organisation data, and potentially be adopted wholesale or with customisation.

2. There is an ongoing link to Basel

Once again, we observed a clear connection to Basel, with many of the causal categories aligning to the Basel definition of operational risk (people, process, systems, external). There were notable observations including:

An extended level 1

Whereas most members have 4-5 level 1 causal categories, we did note some examples with further granularity at level 1 (particularly expanding people and process).

A cause and risk event overlap

We observed an overlap between some causal data and the 2019 ORX Reference Taxonomy events. Perhaps unsurprisingly, this overlap exists especially due to the prevalence of the contemporary risk themes such as data, information security and model.

3. Impacts have moved beyond financial concerns

Only 22% of members submitting impacts limit their scope to financial categories. There is a clear trend to consider and understand non-financial impacts, such as on reputation or customers, when evaluating risk exposure or assessing the impact of risk events.

4. Cause and impact categories appear to be work in progress

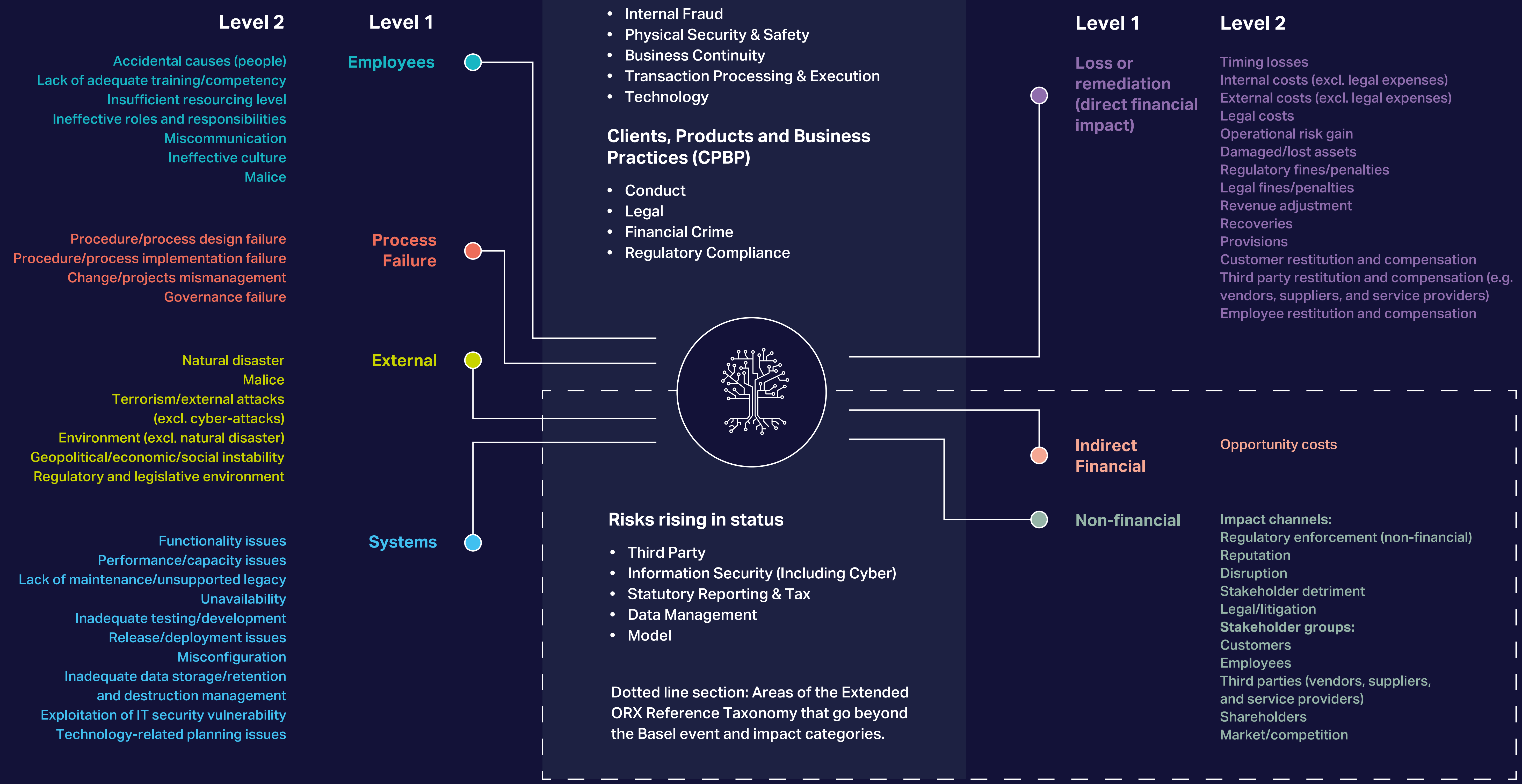
Given the levels of overlap observed in the data, particularly between causes and risk events, and through discussions with members, it appears many organisations have not yet dedicated equivalent effort to the development of cause and impact categories as they have to risk event taxonomies. This is, however, reported as a priority for ORX members going forward and means that publishing a robust industry reference is particularly timely.

5. Balancing the granularity of a taxonomy with the ability of the business to use it

It is important to balance the need of a risk function to understand and analyse risk data in depth and the need to effectively implement a taxonomy in a business. We aimed to achieve this outcome with the Extended ORX Reference Taxonomy through the combination of basing the results on member data, maintaining the principle of making the taxonomy intuitive and easy to understand, running an extensive review process with an industry advisory panel, having only two taxonomy levels and providing practical guidance, definitions and examples.

ORX Taxonomy: Causes and Impacts

See pages 16 to 19 for the full list of risk events, causes and impacts.



Causes

Level 2	Level 1
Accidental causes (people) Lack of adequate training/competency Insufficient resourcing level Ineffective roles and responsibilities Miscommunication Ineffective culture Malice	Employees
Procedure/process design failure Procedure/process implementation failure Change/projects mismanagement Governance failure	Process Failure
Natural disaster Malice Terrorism/external attacks (excl. cyber-attacks) Environment (excl. natural disaster) Geopolitical/economic/social instability Regulatory and legislative environment	External
Functionality issues Performance/capacity issues Lack of maintenance/unsupported legacy Unavailability Inadequate testing/development Release/deployment issues Misconfiguration Inadequate data storage/retention and destruction management Exploitation of IT security vulnerability Technology-related planning issues	Systems

Level 1 Risk Events

Events closely related to Basel

- People
- External Fraud
- Internal Fraud
- Physical Security & Safety
- Business Continuity
- Transaction Processing & Execution
- Technology

Clients, Products and Business Practices (CPBP)

- Conduct
- Legal
- Financial Crime
- Regulatory Compliance

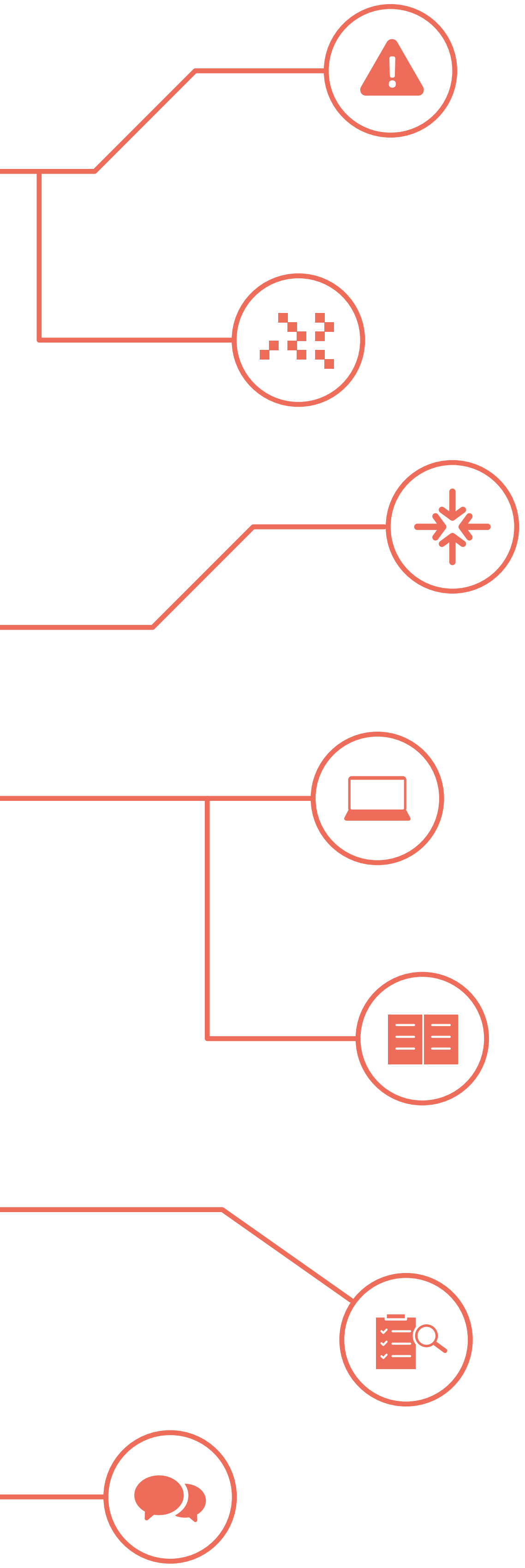
Risks rising in status

- Third Party
- Information Security (Including Cyber)
- Statutory Reporting & Tax
- Data Management
- Model

Dotted line section: Areas of the Extended ORX Reference Taxonomy that go beyond the Basel event and impact categories.

Impacts

Level 1	Level 2
Loss or remediation (direct financial impact)	Timing losses Internal costs (excl. legal expenses) External costs (excl. legal expenses) Legal costs Operational risk gain Damaged/lost assets Regulatory fines/penalties Legal fines/penalties Revenue adjustment Recoveries Provisions Customer restitution and compensation Third party restitution and compensation (e.g. vendors, suppliers, and service providers) Employee restitution and compensation
Indirect Financial	Opportunity costs
Non-financial	**Impact channels:** Regulatory enforcement (non-financial) Reputation Disruption Stakeholder detriment Legal/litigation **Stakeholder groups:** Customers Employees Third parties (vendors, suppliers, and service providers) Shareholders Market/competition



Introduction

Complementing the 2019 ORX Reference Taxonomy

When developing the 2019 ORX Reference Taxonomy, it became clear that complementary cause and impact categories would assist with both the understanding of the taxonomy and support members to further develop their own work. They would also allow better benchmarking and create a better understanding of industry trends and developments. This extended cause-event-impact taxonomy continues to be published as a reference and continues to be aimed at encouraging ongoing industry dialogue and a path to industry consensus on a new taxonomy standard, supporting the sharing of data and information across the industry.

The cause and impact categories

ORX is publishing cause and impact categories that are complementary with the 2019 ORX Reference Taxonomy. Using member data as the key input, ORX is pleased to have:

1. **Developed reference cause and impact categories – both to level 2**
2. **Provided definitions and examples to support understanding of the cause and impact categories**
3. **Published guidance on how to use the cause-event-impact Extended ORX Reference Taxonomy**

Method

ORX, supported by Oliver Wyman, reviewed causes and impacts from 50 ORX member taxonomies (collected in 2020 from banks and insurers). Based on this review, initial draft categories were developed and were evaluated and challenged by a member advisory group.

Data remains in the driving seat

In the report on the 2019 work we discussed that, although often evolving from the Basel Event Types, many organisations have divergent taxonomies, particularly for the more contemporary risks (such as information security, third party and cyber).

In a similar vein, we observe the same pattern with the cause and impact categories collected in 2020. The causes are often based on original Basel definition of operational risk (people, process, systems and external) and there is a core set of financial impacts observed (often aligned to regulatory and accounting standards). However, it is clear over time that organisations have also evolved these categories, reflecting changes in their risk profile, businesses, and regulatory environment.

Observations from the members' data

There are several observations that can be made on the member cause and impact taxonomy data reviewed. These include:

- **A continued link to Basel**

  There is a clear link in the member data with the Basel definition of operational risk (considering people, process, system, and external factors), as the majority of the cause categories contain these 4 categories with some member taxonomies containing an augmented number of level 1 categories.

- **Impact categories have evolved beyond financial**

  Whereas there is a relatively clear set of common financial impacts, driven by regulatory and accounting standards, only a minority of members providing data (22%) exclusively use financial categories. There is a diverse set of non-financial impacts along two leading dimensions: "impact channel" i.e. how the organisation is impacted (e.g. its reputation is tarnished); and "stakeholder group" i.e. who is impacted by the operational risk event (e.g. customers of the member).

- **The use of flags and themes**

  Flags are being used by some members as a design choice to help identify additional characteristics from their risk data.

- **Causal and impact taxonomies appear to be work in progress**

  Cause and impact categories are less well developed and mature than the risk event taxonomies.

Balancing the granularity of a taxonomy with the ability of the business to use it

A final observation, and a subject of discussion and consideration when completing this work, is the need to consider both the objective of a risk team to effectively analyse data to provide insights and the need for a business to be able to understand and apply the taxonomy. A complicated taxonomy, poorly implemented, can risk a deterioration in quality of operational risk data.

As a result, the Extended ORX Reference Taxonomy has been designed with the intention of achieving this balance. It reflects how taxonomies have evolved since Basel. Based on member data, it takes note of a clear industry trend to reflect contemporary risk causes, risk events, and impacts in a language recognised by a business. It has been designed to allow practitioners and the business to capture and understand the increased complexity and interlinked nature of operational risk in financial services. It has also been limited to two levels and has been built with a guiding principle to be intuitive and easy to understand. There is clear guidance supporting use of the taxonomy, as well as definitions and examples.

However, this increased complexity in the operational risks facing the industry – particularly driven by the rapid pace of digitalization – may also present an opportunity. As risk functions look to apply digital techniques, tools such as machine learning and natural language processing could be used to apply new taxonomies to the data with limited or no business intervention, reducing the training need and enhancing data quality.

What next?

The Extended ORX Reference Taxonomy will continue to be published as a reference. It distils the common features of causal and impact categories from members into an industry view.

During 2021, ORX intends to seek further feedback from members on the extended taxonomy and will then run a full review of the taxonomy in 2022.

At that point the hope is to see further industry convergence and to be able to progress towards the Extended ORX Reference Taxonomy becoming a standard for sharing information across the industry.

ORX News

ORX has now implemented the 2019 ORX Reference Taxonomy into ORX News, a service which catalogues operational risk events reported in the media, allowing members to use it for searching and reporting on stories. We have also used it as part of other information services and research projects.

We will continue to seek opportunities to use the taxonomy where appropriate and will consider how we begin to use this Extended Taxonomy too.

Find out more about ORX News

The remainder of the report

The rest of this report...

- Sets out the reference cause and impact categories
- Provides further details on the approach taken to develop the categories
- Key observations on the member data collected
- Some case study examples of how the cause-event-impact model can be applied

This report is also accompanied by the level 1 and 2 cause and impact categories, guidance on how to use the Extended ORX Reference Taxonomy and definitions and examples of each of the categories across the cause-event-impact model.

ORX would also like to thank all members who provided their causal and impact categories, and particularly those who were part of the member advisory group.

Developing the Extended ORX Reference Taxonomy

The bow tie structure

The Extended ORX Reference Taxonomy is an event-based taxonomy based on the "bow tie" method, which distinguishes causes, risk events and impacts (see Figure 1):

Cause

Underlying environment that allows risk events to develop; multiple causes can be mapped to one risk event.

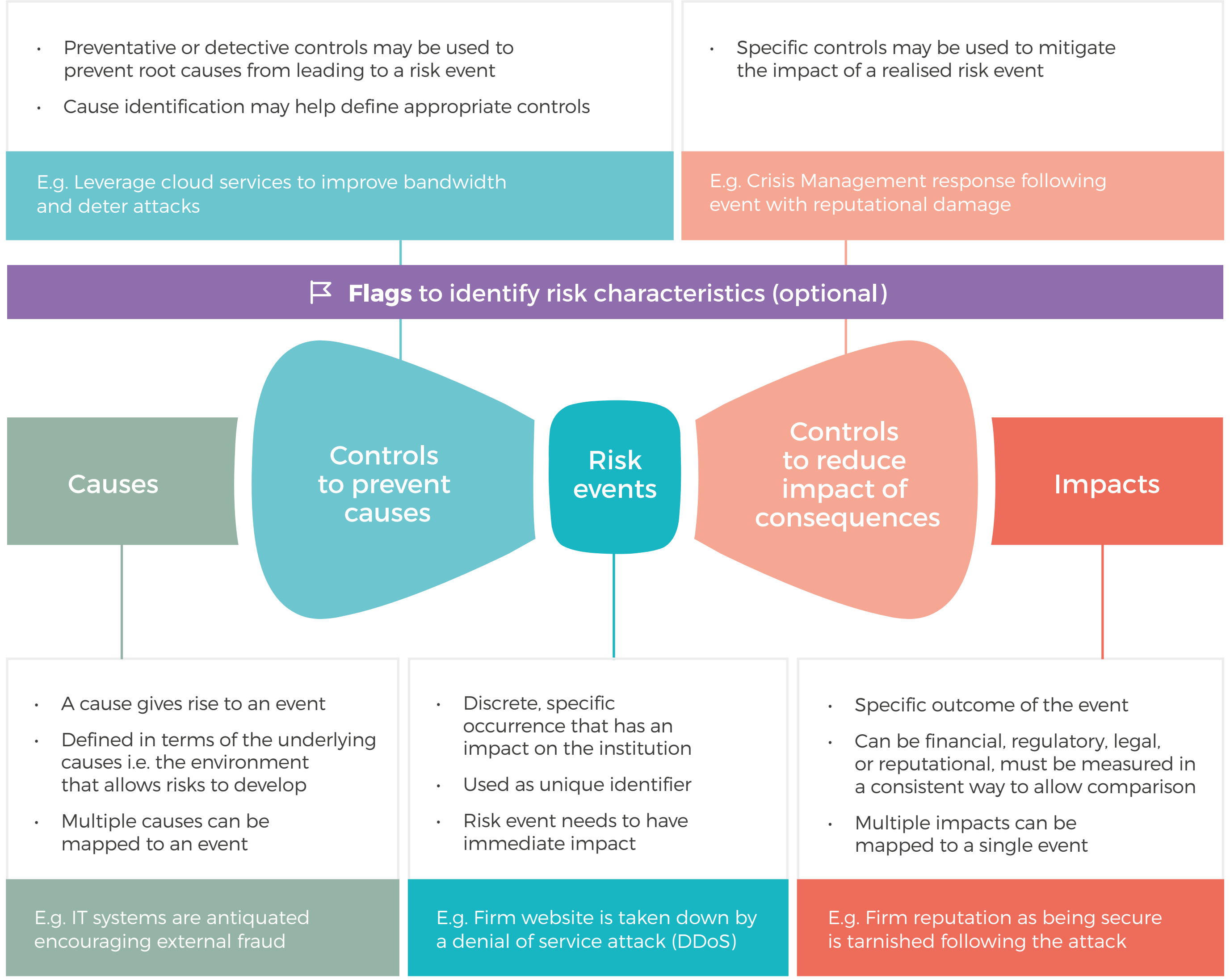
Event

Discrete, specific occurrence, one degree removed from the impact.

Impact

Direct and/or indirect consequence of a risk event for an organisation; multiple impacts can be assigned to one risk event.

Figure 1 Bow Tie Method


Flags to identify risk characteristics (optional)
Causes
Controls to prevent causes
Risk events
Controls to reduce impact of consequences
Impacts

- Preventative or detective controls may be used to prevent root causes from leading to a risk event
- Cause identification may help define appropriate controls

E.g. Leverage cloud services to improve bandwidth and deter attacks

- Specific controls may be used to mitigate the impact of a realised risk event

E.g. Crisis Management response following event with reputational damage

- A cause gives rise to an event
- Defined in terms of the underlying causes i.e. the environment that allows risks to develop
- Multiple causes can be mapped to an event

E.g. IT systems are antiquated encouraging external fraud

- Discrete, specific occurrence that has an impact on the institution
- Used as unique identifier
- Risk event needs to have immediate impact

E.g. Firm website is taken down by a denial of service attack (DDoS)

- Specific outcome of the event
- Can be financial, regulatory, legal, or reputational, must be measured in a consistent way to allow comparison
- Multiple impacts can be mapped to a single event

E.g. Firm reputation as being secure is tarnished following the attack

There are also **three elements** that can be used to **supplement** the bow tie methodology:

1. Controls

Controls are specific pre-defined measures taken to prevent causes from occurring, to prevent risk events from resulting in an impact or to mitigate the impact of the risk event. Controls do not, however, form part of the risk taxonomy and organisations typically reflect their controls in a control library. When recording a risk assessment (e.g. RCSA) or loss event, organisations often capture complementary information on associated controls.

2. Flags

Flags are voluntary, additional data that a firm can use to identify additional risk attributes. Organisations may use a flag to capture information allowing for analysis of related risks independent of the cause, risk event, or impact classification. A current example would be a flag used to identify Covid-19 related risks or risk events.

3. Risk theme

Risk themes are combinations of the above data elements and can be used to describe a "reporting lens".

Methodology for causes and impacts

Member data has been the principle driver behind the cause and impact classification, ensuring that – where possible – the Extended ORX Reference Taxonomy reflects the majority view among ORX members, noting that taxonomies of individual members have idiosyncratic features driven by factors such as regulatory environment, business lines and/or organisational design. Our analysis often identified more than one way of representing risks through the bow tie structure. Consequently, expert judgment was carefully exercised where the analysis provided more than one possible approach to the taxonomy, which included extensive review by a member advisory panel.

Design principles

As with the 2019 risk event taxonomy design work, several design principles were applied to guide the process:

1. Scope includes the current Basel taxonomy and relevant regulations

For causes, this means the 4 causes (people, process, system, external) provided in the Basel definition[1] are considered and that any additional categories are consistent with the Basel definition. For impacts, this means, at a minimum, that all regulatory requirements for loss submission that are directly related to impacts of operational risk are included in the taxonomy.

2. Bow tie structure of the taxonomy needs to be internally coherent

Risk elements should not be classified in more than a single component of the bow tie structure.

3. Taxonomy is stable and sufficiently future-proof

Where there is discretion between segmentation dimensions, we generally prioritise stability. Where newer risk themes were included, we have included some signposting.

4. Taxonomy captures drivers of risk beyond individual control failure

While risk events usually involve control failures, causal categories should not reference individual control failures but rather capture the underlying reasons. Similarly, impacts should not refer to individual control failures.

5. No reference to specific regulations

Neither causes nor impacts should reference specific regulations, to ensure applicability across the diverse regulatory environments that members operate in.

6. Taxonomy is comprehensively exhaustive with minimal overlap

Within each component of the bow tie, categories should cover the scope of the cause/impact universe with minimal overlaps.

7. Taxonomy is intuitive and easy to understand

For best practical application, the taxonomy should be clear and simple to use.

[1] See compilation of the June 2004 Basel II Framework: Bank for International Settlements. "Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version." (2006).

Development approach

The approach we have taken to develop the cause and impact categories is also consistent with the 2019 work on the risk event taxonomy. We have used the member data in a systematic and transparent way. Initially this was to form a view of the potential level 1 categories and, subsequently, to determine and refine the level 2s. Specifically, the working steps were:

1. Re-basing of level 1

Initial data cleaning involved a re-levelling of submitted categories where appropriate to achieve a comparable set of data.

2. Assigning level 1 categories

For level 1 categories, the main dimensions were identified. Furthermore, data entries not applicable to the operational risk taxonomy were excluded from the analysis (example: Strategic risks such as "business model inadequate").

3. Identifying and assigning level 2 categories:

The same step was then repeated for the respective dimensions of level 2 categories within each level 1 category.

During the 2019 analysis of the ORX event taxonomy, 275 out of a total of 5,297 data entries received from ORX members were excluded on the basis that they represented causes or impacts. These were used to further validate this most recent analysis.

An ORX member taxonomy advisory group consisting of 11 financial institutions, including representation from both the banking and insurance industry and from various geographies and jurisdictions, was formed. The group confirmed the direction of travel, provided feedback on the design of the taxonomy and offered perspectives as end users of the taxonomy. These financial institutions were consulted on the draft versions of this document to ensure the Extended ORX Reference Taxonomy is fit-for-purpose and intuitive to use.

Scope and exclusions

Some tangential aspects of operational risks are excluded to ensure relevance of the categories and the consistency of the bow tie structure. Excluded elements are:

Within causes

- Themes that contribute to operational risk but are generally considered too "far removed" to be able to directly cause an operational risk event (e.g. an organisation strategy, or organisational/legal structure).
- Control failure as a cause, as design principle 4 states that specific control failures should be out of scope of a risk taxonomy.
- Intermediate manifestations of risk which sit in between causes and risk events, specifically "model risk" and "data management". To preserve the internal coherence of the extended taxonomy, these two categories are only placed in the risk event taxonomy to avoid duplication between the cause and risk event categories.

Within impacts

Accounting items used to track the stages of operational risk events (e.g., "pending losses" and "rapid recoveries").

Others

- Near misses
- Organisational identifiers (e.g. business unit)

Flags and risk themes are useful supplementary tools that describe other risk attributes (in the case of a flag) or a "reporting lens" (in the case of a risk theme). They are further discussed on pages 13 and 15 respectively.

Observations from member cause and impact data

There are several observations that can be made on the member cause and impact data reviewed. These include:

A continued link to Basel

There is a clear link in the member data with the Basel definition of operational risk (considering people, process, system, and external factors). It is also notable that these core causal categories have also been augmented and, in some cases, expanded at level 1 (although the vast majority have between 4 and 5 level 1 causes). Where members have expanded beyond the 4 core categories, they have often used a combination of more granular categories to expand people and process. The more popular level 1 categories not directly related to Basel include governance, change/ projects, and data.

Impact categories have evolved beyond financial

Whereas there is a relatively clear set of common financial impacts, driven by regulatory and accounting standards, only a minority of members providing data (22%) exclusively use financial categories. Members are adopting a wide range of non-financial impacts, often considering impacts beyond the perimeter of the financial institution such as those on customers or the market. Most of the non-financial impact data can be divided into two groups: impacts in the form of the 'impact channel' (e.g. on reputation or disruption) and impacts that are on the 'stakeholder group' (e.g. customers or employees). There also appears to be a wide range of practices when it comes to capturing and assessing of non-financial impacts.

The use of flags and themes

Flags are being used by some members as a design choice to help identify additional characteristics from their risk data. They appear to be commonly used to enhance a taxonomy (~50% of the participating members submitted data for flags), rather than be formerly part of a taxonomy. Uses include flags as attributes providing additional information on a risk (e.g. linking a risk event to a customer complaint), as a link to a regulation (e.g. GDPR), to capture additional information on pertinent issues in the existing operating environment (e.g. Covid-19) or to link to a broader risk theme (such as conduct, data, third party or privacy). Flags or themes can be used to undertake further analysis on risk data, viewing information through a different lens and avoiding disruption to a taxonomy.

Causal and impact taxonomies appear to be work in progress

It is apparent from the data analysis, as well as discussions with the advisory panel, that cause and impact categories are less mature and not given the same degree of attention as risk event taxonomies. Whereas Basel has often been used as the base for level 1 causes, we observed overlap between causes and risk events and divergence amongst level 2s. This observation is often made for more contemporary risk areas, such as data, model, and information security, which may be lacking industry-wide standards and are frequently interlinked and complex in nature. We understand from discussions with members that they expect to undertake further work in this area in the future, hopefully using the Extended ORX Reference Taxonomy to develop their thinking.

Flags and risk themes

A notable trend from the data is the increasing popularity of the use of flags and risk themes, with around half using flags or risk themes alongside their cause and impact categories. These are optional additional structures that assist organisations in identifying certain risk characteristics outside of the formal bow tie taxonomy structure (for risk flags), or group information in a useful manner. Here we provide some insight into the use of flag and themes, but stress they are outside the scope of the ORX Reference Taxonomy.

Flags

Flags are additional design choices that a firm can use to identify risk characteristics. Examples of flags identified in the ORX members data include:

- Attributes that provide a link to additional information, e.g. linking a risk event to customer complaints
- Sets of regulations relevant to the risk event
- Organisations may capture a flag to allow analysis of related risks independent of the cause, risk event, or impact classification, e.g. a "Covid-19" flag

An example of a number of different risk events linking to a flag would be GDPR: the possible risk events relating to this one flag could include:

- **Unavailability of data**

  If the data subject requests information on how the institution uses his/her personal data but that information is not available.

- **Data privacy breach**

  If the institution shares the data with a third party without the prior consent of the data subject.

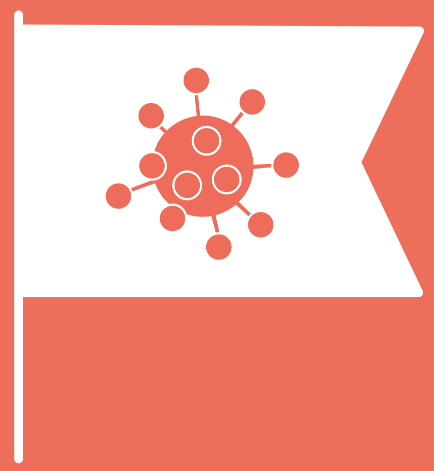
- **Poor data quality**

  If the data pertaining to the data subject is inaccurate.

- **Inadequate data architecture**

  If the data subject requests the right to erase but the data architecture is built in such a way that is linked to other static data, making the tracing of all the relevant datapoints to be erased impossible.

Flags should only identify additional risk characteristics outside the bow tie construct. Table 1 provides an overview of flags observed within the member data that offer such options while being consistent with the bow tie methodology.



Coronavirus flag

ORX issued guidance this year on how to capture operational risk impacts of coronavirus. Treating the pandemic as a cause, events arising would be classified in the Reference Taxonomy under a number of categories such as failures in business continuity planning, transaction processing & execution errors, physical security and safety concerns and fraud. The reference taxonomy methodology approach would also advocate grouping these events using a 'pandemic flag' to allow collective analysis and reporting.

ORX members can view more information here

Not a member yet? View more information here

Table 1: Identified flags consistent with the Extended ORX Reference Taxonomy

Flag category	Explanation/specific example
Sets of regulation	FATCA, GDPR, AML Legislation (FICA, POCA, POCDATARA)
Grouped events	Covid-19
Corporate social responsibility	Corporate Social Responsibility risks
Customer complaint	Events brought to light as a result of customer complaints
Audit finding	Events brought to light as a result of audit findings
Market loss: operational risk component[2]	Component in a market risk loss that can be attributed to a trading execution error
Credit loss: operational risk component[3]	Component in a credit risk loss that can be attributed to an operational failure in the credit approval process
Insurance loss: operational risk component[4]	Component in an insurance risk loss that can be attributed to an involuntary error in applying deductible or limit due to operational failure

ORX members' data has surfaced several flags that can be internally consistent with the members' own taxonomies if the taxonomies are tailored and therefore diverge from the Extended ORX Reference Taxonomy – see Table 2.

Table 2: Further identified flags that are used by members for tailored taxonomies

Where member flag is located in the Extended ORX Reference Taxonomy	Flag
Causes	Third party
	Technology
	Process risk
Events	Conduct e.g. sales practice
	IT and cyber risk events
	Business continuity
	Data e.g. information governance
	Fraud
	Regulatory compliance e.g. notifiable event
	Personal information/privacy
	Technology risk
Impact	Conduct
	Financial risk impact
	Reputational risk
	Legal/litigation

Note that there are additional data fields that organisations record as part of data collection (mandated by regulation or otherwise) which we have excluded for the purposes of the classification of flags. Examples include:

- Other data fields that describe the risk, e.g. the process within which the risk materialised/ department from which the risk event originated
- Data fields relevant to managing the workflow of loss reporting

[2] Share of losses due to market prices changes on outstanding positions that is attributable to operational risk
[3] Share of losses due to counterparty default (failure to meet a contractually pre-determined obligation) that is attributable to operational risk
[4] Share of losses or of adverse change in the value of insurance liabilities (whether Life or Non-Life), due to inadequate pricing and provisioning assumptions that is attributable to operational risk

Risk themes

Organisations may wish to group information pertaining to a theme or topic in order to determine its organisational-level view on that risk. We have identified such topics as "risk themes".

Themes are discretionary structures that exist to help risk practitioners logically structure data for risk management. Unlike cause, risk event, impact, or flags, risk themes can encompass a single component or multiple components of the bow tie structure. Risk themes differ from flags in that flags can capture additional data outside the bow tie (e.g., flags tracking risk events that were discovered through internal audit) whereas themes are only linked to components within the bow tie.

Some examples of risk themes include:

Themes that can be identified through a single component of the bow tie

- "Conduct" theme: Depending on local definitions of Conduct, the theme might be defined as a combination of fraud (internal and external) from the risk event categories, stakeholder detriment and customers and market/competition from the impact categories.

Themes that span across multiple components of the bow tie:

A **"People"** theme might be defined as the employees category from cause, people category from risk event as well as a stakeholder detriment impact on employees.

A **"Data"** theme might include a system cause (e.g. inadequate data storage/retention and destruction management) and a data management risk event.

A **"Technology"** theme might span from systems causes via technology failure risk events and could include a disruption impact.

A **"third party"** theme might cover risk events linked to a third party (via the external – third parties cause) as well as risk events of mismanagement of third parties.

Appendix: Extended ORX Reference Taxonomy

Cause categories

Table 3: Reference operational risk cause categories

Level 1	Level 2
Employees	Accidental causes (people)
	Lack of adequate training/competency
	Insufficient resourcing level
	Ineffective roles and responsibilities
	Miscommunication
	Ineffective culture
	Malice
Process failure	Procedure/process design failure
	Procedure/process implementation failure
	Change/projects mismanagement
	Governance failure
External	Natural disaster (e.g. pandemic, earthquakes, floods etc.)
	Malice (e.g. by vendors, suppliers, service providers, customers, counterparties etc.)
	Terrorism/external attacks (excl. cyber-attacks)
	Environment (excl. natural disaster)
	Geopolitical/economic/social instability
	Regulatory and legislative environment
Systems	Functionality issues
	Performance/capacity issues
	Lack of maintenance/unsupported legacy
	Unavailability
	Inadequate testing/development
	Release/deployment issues
	Misconfiguration
	Inadequate data storage/retention and destruction management (cause)
	Exploitation of IT security vulnerability
	Technology-related planning issues

Risk events

Table 4: Reference operational risk events

Level 1	Level 2
People	Breach of employment legislation or regulatory requirements
	Ineffective employment relations
	Inadequate workplace safety
External Fraud	Third party/vendor fraud
	Agent/broker/intermediary fraud
	First party fraud
Internal Fraud	Internal fraud committed against the organisation
	Internal fraud committed against customers/clients, or third/fourth parties
Physical Security and Safety	Damage to organisation's physical asset
	Injury to employee or affiliate
	Damage or injury to public asset
Business Continuity	Business continuity planning failure/event mismanagement
Transaction Processing and Execution	Processing/execution failure relating to clients and products
	Processing/execution failure relating to securities and collateral
	Processing/execution failure relating to third party
	Processing/execution failure relating to internal operations
	Change execution failure
Technology	Hardware failure
	Software failure
	Network failure
Conduct	Insider trading
	Anti-trust/anti-competition
	Improper market practices
	Pre-sales service failure
	Post-sales service failure
	Client mistreatment/failure to fulfil duties to customers
	Client account mismanagement
	Improper distribution/marketing
	Improper product/service design
	Whistleblowing
	Breach of code of conduct and employee misbehaviour

Risk events (continued)

Table 4: Reference operational risk events

Level 1	Level 2
Legal	Mishandling of legal processes
	Contractual rights/obligation failures
	Non-contractual rights/obligation failures
Financial Crime	Money laundering and terrorism financing
	Sanctions violation
	Bribery and corruption
Regulatory Compliance	Ineffective relationship with regulators
	Inadequate response to regulatory change
	Improper licensing/certification/registration
	Breach of cross-border activities/extra-territorial regulations
	Prudential risk
Third Party	Third party management control failure
	Third party criminality/non-compliance with rules and regulations
	Inadequate intra-group agreements/SLAs
Information Security (including cyber)	Data theft/malicious manipulation of data
	Data loss
	Cyber risk events
	Data privacy breach/confidentiality mismanagement
	Improper access to data
Statutory Reporting and Tax	External financial and regulatory reporting failure
	Tax payment/filing failure
	Trade/transaction reporting failure
Data Management	Unavailability of data
	Poor data quality
	Inadequate data architecture/IT infrastructure
	Inadequate data storage/retention and destruction management
Model	Model/methodology design error
	Model implementation error
	Model application error

Impact categories

Table 5: Reference operational risk impact categories

Level 1	Level 2
Loss or remediation (direct financial impact)	Timing losses
	Internal costs (excluding legal expenses)
	External costs (excluding legal expenses)
	Legal costs
	Operational risk gain
	Damaged/lost assets
	Regulatory fines/penalties
	Legal fines/penalties
	Revenue adjustment
	Recoveries
	Provisions
	Customer restitution and compensation
	Third party restitution and compensation (e.g. vendors, suppliers, and service providers)
	Employee restitution and compensation
Indirect financial impact	Opportunity costs
Non-financial impact	Impact channels: - Regulatory enforcement (non-financial) - Reputation - Disruption - Stakeholder detriment - Legal/litigation
	Stakeholder groups: - Customers - Employees - Third parties (vendors, suppliers, and service providers) - Shareholders - Market/competition

About ORX

ORX is the largest operational risk association in the financial sector and has been a leading support for the industry since 2002.

For nearly two decades, we have been an ever expanding global community, bringing together thousands of operational risk professionals to share knowledge, expertise and experience.

Our services include a range of solutions focused on effective management and measurement of operational and non-financial risk. This includes global loss data exchange, an extensive research programme and a series of events held around the world.

We not only support individual organisations to assess their vulnerability to losses, but we also shape industry-wide development of best practice.

ORX is owned and managed by over 95 financial firms from all over the world. As a not-for-profit organisation, we invest all income back into providing high-quality benefits for operational and non-financial risk professionals. This ultimately helps develop the future direction of the discipline.

About Oliver Wyman

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialised expertise in strategy, operations, risk management, and organisation transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS	1 212 541 8100
EMEA	44 20 7333 8333
ASIA PACIFIC	65 6510 9700

The information and opinions in this report were prepared by Oliver Wyman and ORX. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman and ORX have made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman and ORX disclaim any responsibility to update the information or conclusions in this report. Oliver Wyman and ORX accept no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. This report may not be sold without the written consent of Oliver Wyman and ORX.

ORX and Oliver Wyman have prepared this report with care and attention. ORX and Oliver Wyman do not accept responsibility for any errors or omissions within this report. ORX and Oliver Wyman do not warrant the accuracy of the advice, statement or recommendations in this report. ORX and Oliver Wyman shall not be liable for any loss, expense, damage or claim arising from this report. The content of this report does not itself constitute a contractual agreement, and ORX and Oliver Wyman accept no obligation associated with this report except as expressly agreed in writing.

This Extended ORX Reference Taxonomy guidance is provided free of charge to all ORX members. It is available to other financial organisations – please contact communications@orx.org for further details. Commercial use of both the summary and Extended ORX Reference Taxonomy by consultants or other firms for any financial gain is not permitted without express permission from ORX and will incur a charge.

OLIVER WYMAN

O.R.X