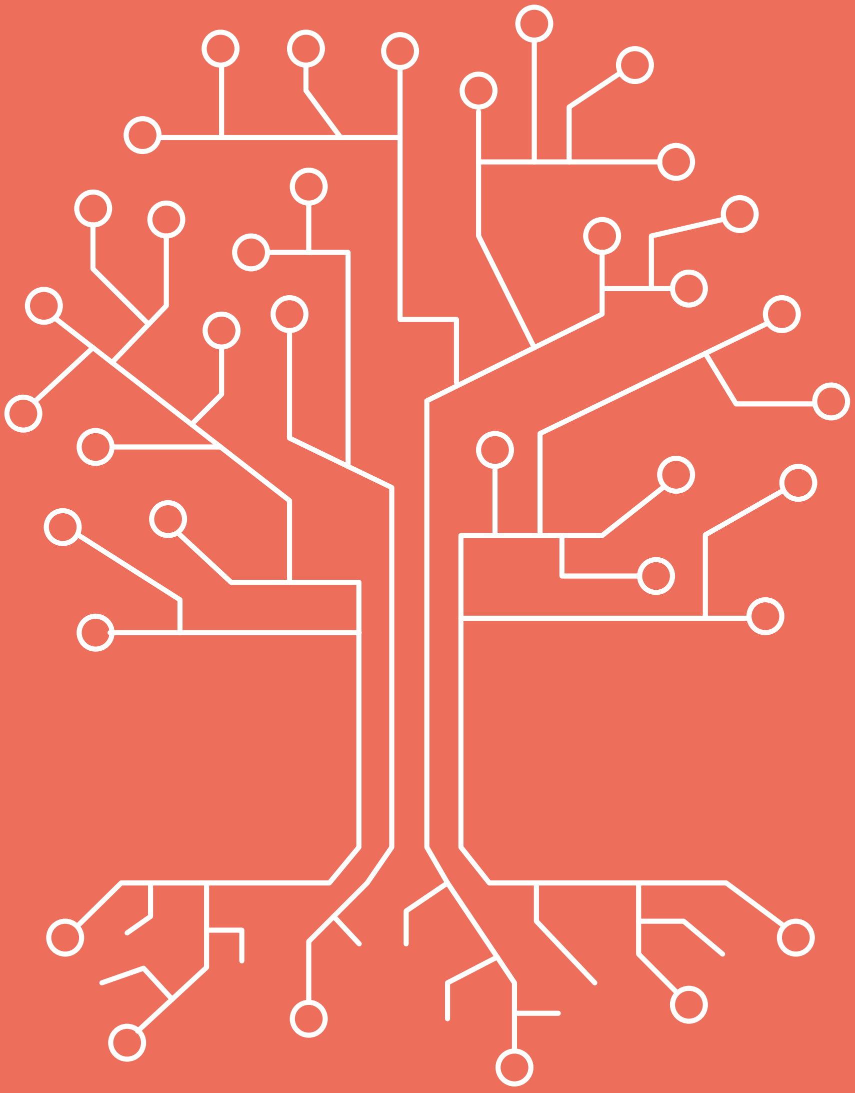


The ORX Reference Taxonomy for operational and non-financial risk

FULL REPORT

OLIVER WYMAN

O.R.X

ORX contacts:

Dr Luke Carrivick
Head of Research and Information

luke.carrivick@orx.org

Steve Bishop
Head of Insurance and Risk Information

steve.bishop@orx.org

Oliver Wyman contacts:

Evan Sekeris
Partner

evan.sekeris@oliverwyman.com

Thomas Ivell
Partner

thomas.ivell@oliverwyman.com

Valerie Wong
Engagement Manager

valerie.wong@oliverwyman.com

Follow ORX:

@ORX_Association

@ORX_Association

Follow Oliver Wyman:

@Oliver Wyman

@OliverWyman

orx.org | oliverwyman.com

Executive summary

A strategic priority for ORX and the operational and non-financial risk community

There has been a substantial change in the operational risks faced in financial services over the last 15 years. Risks such as Conduct, Cyber and Third Party have risen in importance and now dominate boardroom agendas. How organisations think about this expanding portfolio of threats and manage them in a consistent way is underpinned by their risk taxonomy.

This changing risk profile, combined with a recent shift of focus away from capital measurement towards risk management, means that many organisations are updating their operational risk taxonomies. In doing so, they are deviating from **Basel Event Types**[1] and in the absence of a common standard, we have observed a great deal of divergence.

The strategic priority of this ORX initiative, supported by Oliver Wyman, was to create a common point of reference and thereby solid ground for industry discussion about developing operational risk taxonomies. This lays the foundations which allow consistent industry sharing of insights and data over the coming years.

An industry point of reference

The ORX Reference Taxonomy[2] presented here is our first iteration of a full taxonomy that goes deeper into level 2 risks. It is an enhancement of the **award-winning level 1 reference taxonomy** which was developed in 2018.[3] At this stage it is provided as a guide to the industry and to encourage a convergence of thinking; it is not intended as a standard and will not be adopted in the ORX global and regional loss data exchange services. It consolidates information from 60 different taxonomies into a single coherent reference.

To best use this work, it is important to understand that:

1. This is a reference

We have published a reference taxonomy which collates many individual operational risk taxonomies in a sensible way. It is intended as a useful resource against which organisations can benchmark and improve practice. It is unlikely to meet every need without some customisation.

2. It can be used in different ways

Given the thematic nature of some risks (such as cyber), it is possible to adapt the ORX Reference Taxonomy to meet your business needs. For example, users could create meaningful groups of level 2 risks which do not appear within the same level 1 in the reference taxonomy, or they could align reference taxonomy level 2 risks to alternative level 1 risks in their own taxonomy.

3. There is a connection to Basel

It is important to note that taxonomies had not moved completely away from Basel Event Types; more accurately, they had evolved and expanded them. We observed common changes, and the reference reflects this:

- **A change of language**

  Some risks closely corresponding to Basel Event Types, but with a change of language.

- **Greater focus on misconduct**

  Risks which expand the Clients, Products and Business Practices category and provide greater granularity, such as Compliance, Financial Crime and Misconduct.

- **An elevation of material concerns**

  Risks that have risen in prominence and are elevated to level 1. This includes Information Security, Cyber, Data, Model and Third Party.

In 2020 ORX plan to produce a corresponding cause and impact taxonomy, in addition to progressing work on controls, in order to provide a comprehensive reference. The ORX Reference Taxonomy will also be incorporated into the **ORX News**[4] service.

[1] https://www.bis.org/bcbs/qisoprisknote.pdf

[2] This more detailed ORX Reference Taxonomy and 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. There is also a public summary of the ORX Reference Taxonomy which is freely available for all financial organisations to benefit from. Commercial use of both the summary and detailed 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. (Copyright ORX 2019)

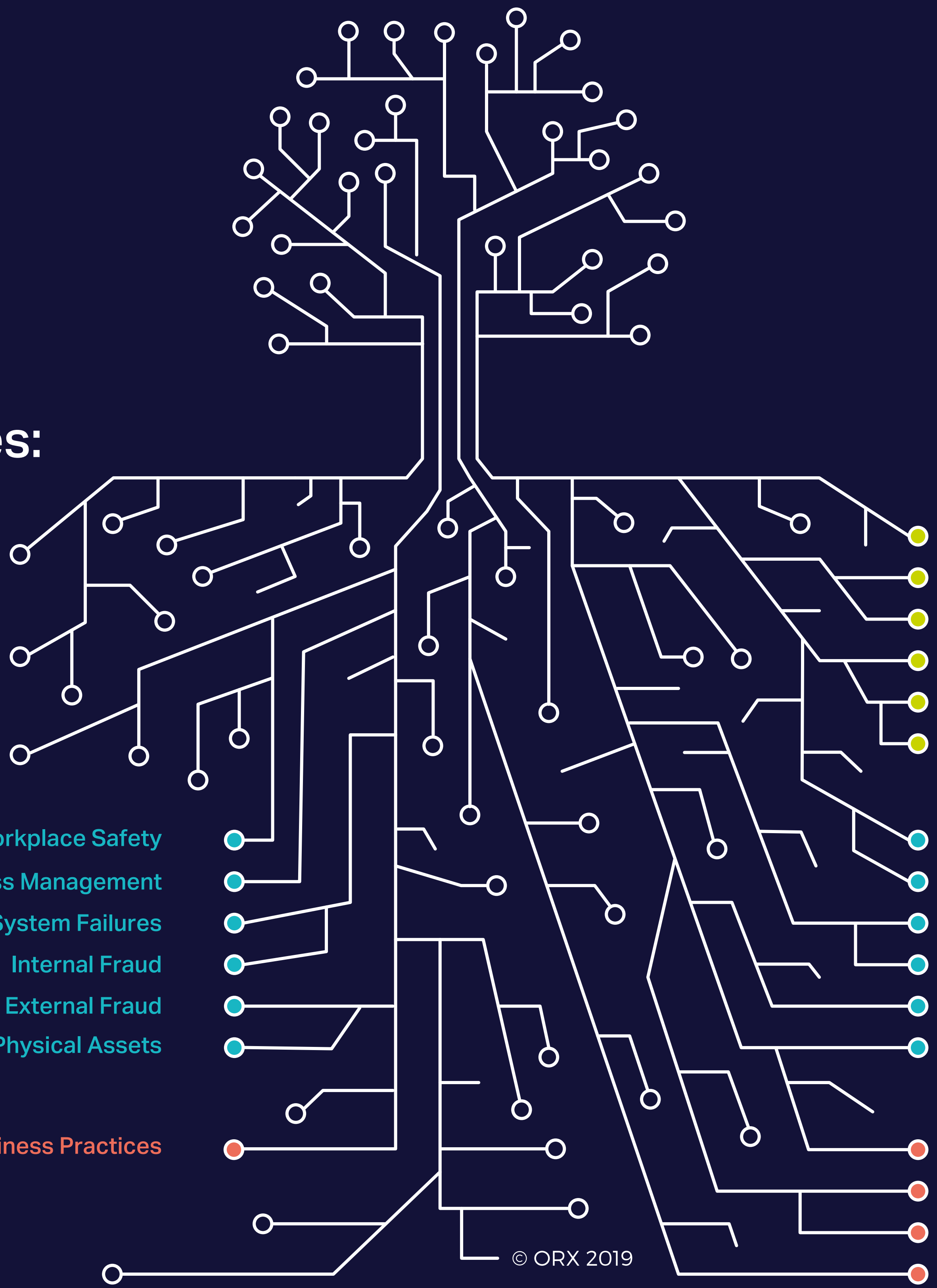
[3] https://managingrisktogether.orx.org/news-and-blogs/orx-wins-initiative-year-2019-operational-risk-awards

[4] https://managingrisktogether.orx.org/orx-news

ORX Reference Taxonomy

This infographic shows the connection of the ORX Reference Taxonomy to the Basel Event Types

Below are the level 1 event types in the ORX Reference Taxonomy (2019). For the level 2 event types, see page 24. During 2020, ORX plan to produce a corresponding cause and impact taxonomy, in addition to progressing work on controls, in order to provide an even more comprehensive reference.



Basel Event Types:

Operational Risk

- Employment Practices & Workplace Safety
- Execution, Delivery & Process Management
- Business Disruption & System Failures
- Internal Fraud
- External Fraud
- Damage to Physical Assets

Conduct / Compliance

- Clients, Products & Business Practices

ORX Reference Taxonomy Level 1s:

- Third Party
- Statutory Reporting and Tax
- Business Continuity
- Data Management
- Information Security (including Cyber)
- Model

Risks that have risen in prominence and are elevated to level 1

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

Risks closely corresponding to Basel Event Types, but with a change of language

- Legal
- Conduct
- Financial Crime
- Regulatory Compliance

Risks which expand the Clients, Products and Business Practices category and provide greater granularity and focus on misconduct

Introduction

A level 1 reference taxonomy

In 2018, an **ORX research study**[5] developed an emerging level 1 ORX Reference Taxonomy. 90% of the study's participants had adopted a taxonomy which captures the key risks they see in today's business environment, and one which is defined in a language familiar to their business leaders.

It was, however, important to note that a significant majority had not moved completely away from Basel Event Types – more accurately they had evolved and expanded them. This held true for participants who self-identified as following a Basel structure, but also true to an extent with those who self-identified as having developed their own taxonomy.

In some cases, we have observed more wholesale changes, particularly with participants who self-identified as having developed their own taxonomy. This allows more freedom in the way they can express their risk profile. It in turn often results in a larger number of level 1 risks (compared to the Basel structure), reflecting the desire to elevate certain risks to higher prominence.

A full reference taxonomy

There has been significant interest from ORX members, the wider industry and regulators in the 2018 taxonomy work. Building on this, ORX has been pleased to work with Oliver Wyman and using a larger set of taxonomy data to:

1. **Develop an updated ORX Reference Taxonomy, including level 2 risks**
2. **Provide guidance to support and explain the taxonomy**

This taxonomy can be used as a key reference to benchmark against and to observe industry trends. It is not a standard specifically intended to be adopted wholesale but can assist organisations in developing their taxonomies, provide industry evidence to support change and allow them to accelerate their thinking.

[5] Developments in risk taxonomies (2018)

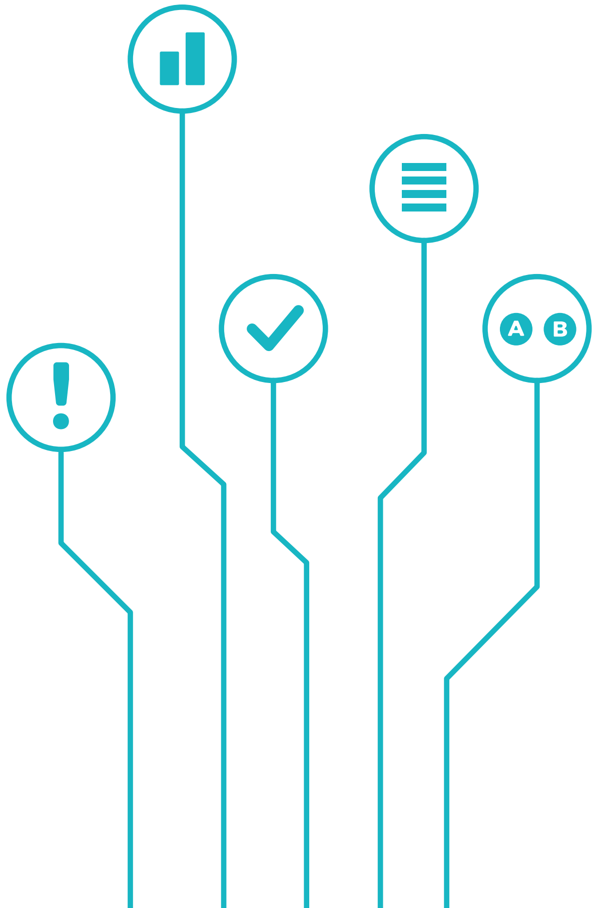
Method

Working with Oliver Wyman, ORX reviewed an expanded data set of 58 ORX member taxonomies (collected from banks and insurers).[6] This was used to validate the 2018 level 1 reference, derive suitable supporting level 2 risks and to develop guidance.

We have then worked with a member advisory group to review, update and finalise the taxonomy.

During this work, several principles have been applied to develop the ORX Reference Taxonomy, namely that it should:

- Be risk event based[7]
- Be designed to include two levels
- Be intuitive and easy to understand
- Cover the scope of – and map back to – Basel Event Types
- Be mutually exclusive and collectively exhaustive (to the extent possible)



Data in the driving seat

The data collected demonstrates that there are numerous equally valid approaches to risk taxonomy construction. Differences can arise because of an individual organisation's decisions regarding both the risks to include and where to position them. These decisions are influenced by external factors, for example jurisdictional trends. They could also be influenced by idiosyncratic factors, such as internal organisational structures or the businesses in which an organisation operates.. Establishing a taxonomy is not a perfect science and often requires the application of common sense and compromise.

The factors above, as well as the absence of industry-wide taxonomy developments, highlight the need for ORX to enhance the Reference Taxonomy and develop the level 2 categories.

Central to this development has been the use of ORX member taxonomy data in a systematic and transparent way. Initially, data was used to validate and update the level 1 categories identified as part of the 2018 ORX study. Further analysis has then been undertaken to assist in the development of the supporting level 2 risks for the enhanced version in this report.

This analysis to develop level 2 risks involved:

- Identification of the "risk dimensions" used to describe each level 1/level 2 risk, for example under External Fraud, level 2 risks in participant taxonomies are linked to dimensions including actor, item, product and channel.
- The adoption of either the most common approach to level 2 risks or, where significant divergence was observed, using the most consistent approach to determine level 2 risks.
- Review and feedback from the member advisory group of the risks where practice diverged the most.

[6] Two member taxonomies were added subsequently which were used to validate the proposed ORX Reference Taxonomy, taking the dataset to 60.

[7] As opposed to cause or impact based; see page 26 on the bow tie methodology

Observations from the taxonomy data

The review of the taxonomies highlighted several themes from across the data set and the detail of the taxonomy analysis is set out in the next section of the report.

Some interesting notable observations include:

- **Increase in level 1 size and use of risk "themes"**

  Relative to the Basel Event Types, there is an overall increase in the number of level 1 risks in the taxonomies collected. On average there were 14 level 1 risks versus the 7 original level 1 Basel Event Types. Another way of capturing increasing prominence in certain risk types is the use of risk "themes" as standalone risk categories, for example Conduct and Cyber.[8]

  The increase of both level 1 risks and in the use of risk themes potentially reflects a more developed and granular approach to defining operational risk. It may also reflect the increased number of risks uniquely recognised under the operational risk umbrella.[9]

- **Use of different dimensions**

  For several risks, members use a combination of different "dimensions" to define their level 2 risks. This was particularly evident for Conduct – where dimensions observed relate to market integrity, products and services, as well as clients and business practices. Different dimensions were also evident for External Fraud (as mentioned in the "Data in the driving seat" section above) and for Internal Fraud (similar to External Fraud).

  Although the combinations of dimensions used can appear illogical, this pattern may have evolved as taxonomies are developed over time. Categories being added to respond to new threats or risks, or new regulatory areas of focus. Often organisations do not have the luxury of starting their taxonomy again.

- **Control failures**

  Often participating taxonomies included level 2 risks that could be classed as causes and/or control failures. Given the increasing likelihood that organisations are penalised for inadequate control frameworks or control failures without strictly having had an event occur, this may reflect a pragmatic approach to incorporate events that could lead to an impact.

Divergence was evident

In addition to the observations above, there was divergent practice evident in the participant taxonomies. The widest range of practice was seen within the risks that have risen in prominence – those often described as more "thematic" than pure risks (as per the control failures observation). This included Cyber, Conduct and Third Party.

Analysis highlighted that ORX members take different approaches to categorising these risks. Approaches observed included the use of such categories as level 1 risks, using impact and causal taxonomies to support classification, as well as the use of flags to indicate where an event may relate to more than one risk type.

As an example of the variances observed, an event captured as External Fraud may have a cyber-attack at its cause. Depending on an organisation's approach, this could be classified as Cyber, or as an External Fraud with a Cyber cause, or as an External Fraud tagged with a Cyber flag. A further example is a technology failure event that may impact customers. This could be recorded as Conduct, or as a technology failure with a customer or conduct impact, or as a technology failure tagged with a Conduct flag.

These variances may well have arisen due to a lack of an industry standard covering such risks. Organisations' taxonomies have grown organically, gaining idiosyncratic features influenced by factors such as the organisation's approach to risk management, their jurisdiction and regulator.

Later in this report there is further analysis of the industry approaches taken for the categorisation of Cyber, Conduct and Third Party, as well as a further explanation of the approach and logic applied when developing these areas in the ORX Reference Taxonomy.

[8] ORX has also explored cyber definitions and taxonomies as part of our **Cyber Risk Management (CISR) Programme**.

[9] https://managingrisktogether.orx.org/research/role-and-scope-op-risk

Why a reference and what next?

Given the observations and areas of divergence described for certain risks, ORX believe it is extremely helpful to publish this taxonomy as a reference. The aim at this stage is to help develop consistent industry thinking rather than provide a taxonomy intended as a wholesale standard.

The ORX Taxonomy is intended to capture the wisdom of crowds and has distilled many of the successful features of operational risk taxonomies from across the industry.

It will not currently be used for the ORX global loss data exchange services. However, ORX will seek feedback from its membership, the wider industry and regulators, including understanding where it has been adopted and the results of any benchmarking work. We also intend to re-run the project in 12 to 18 months' time.

Iteratively updating the taxonomy will allow ORX to collect updated member taxonomies and review the effectiveness of the reference, helping ensure it remains relevant and inclusive of key industry risks, and monitor potential convergence towards a future industry standard.

ORX Reference Taxonomy in action

ORX will use the reference taxonomy during 2020 in **ORX News**.[10] This will allow it to be tested in action and support subscribers to the ORX News service in searches and reports.

We also aim to use the taxonomy in other information services and products, particularly focusing on how we analyse and report on material risks.

[10] https://managingrisktogether.orx.org/orx-news

The remainder of the report

The rest of this report sets out:

- Further analysis and information on the member taxonomy data collected
- The approach adopted for analysing the information and developing the ORX Reference Taxonomy
- Deep dives looking at approaches to Cyber, Conduct and Third Party
- The ORX Reference Taxonomy level 1 and level 2 risks

This report is supported by the full ORX Reference Taxonomy and guidance document which additionally sets out the level 1 and 2 risk definitions, as well as guidance on how the taxonomy can be used.

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

Developing the ORX Reference Taxonomy

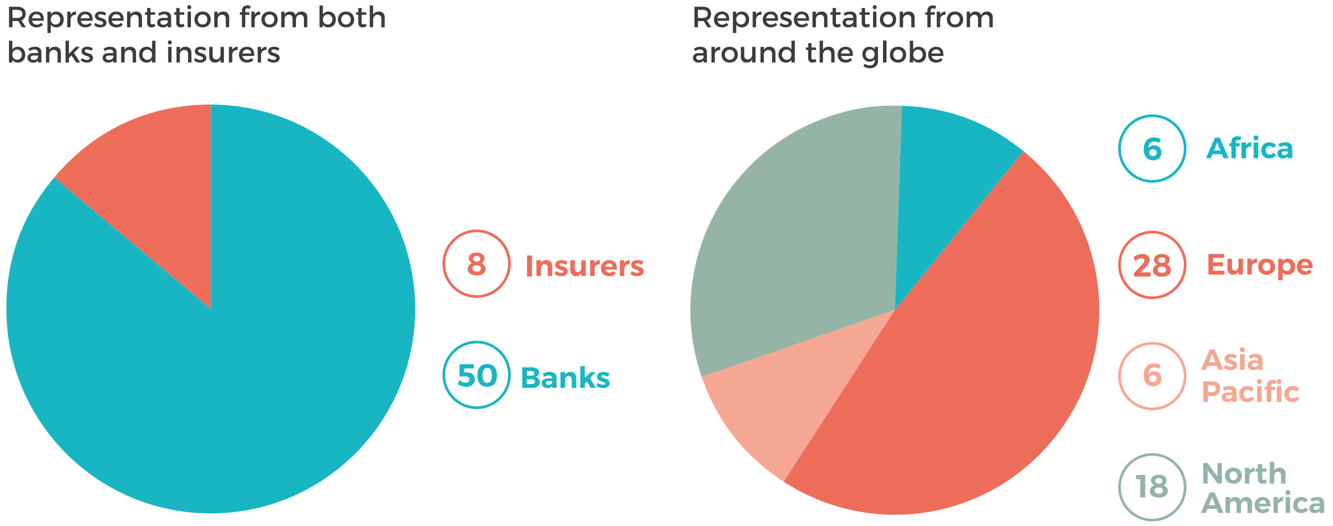
Overview of the ORX member taxonomy data

The dataset used to develop the ORX Reference Taxonomy comprised of the operational risk taxonomy of 58 ORX members, with good representation across the banking and insurance industry, as well as geographical regions.

Two additional member taxonomies were received following the initial analysis which were used to validate the reference taxonomy – taking the total dataset to 60.

Figure 2 demonstrates that there was a wide spread of risks present in these member taxonomies, with an interquartile range of 38 – 116 risks at the most granular level.

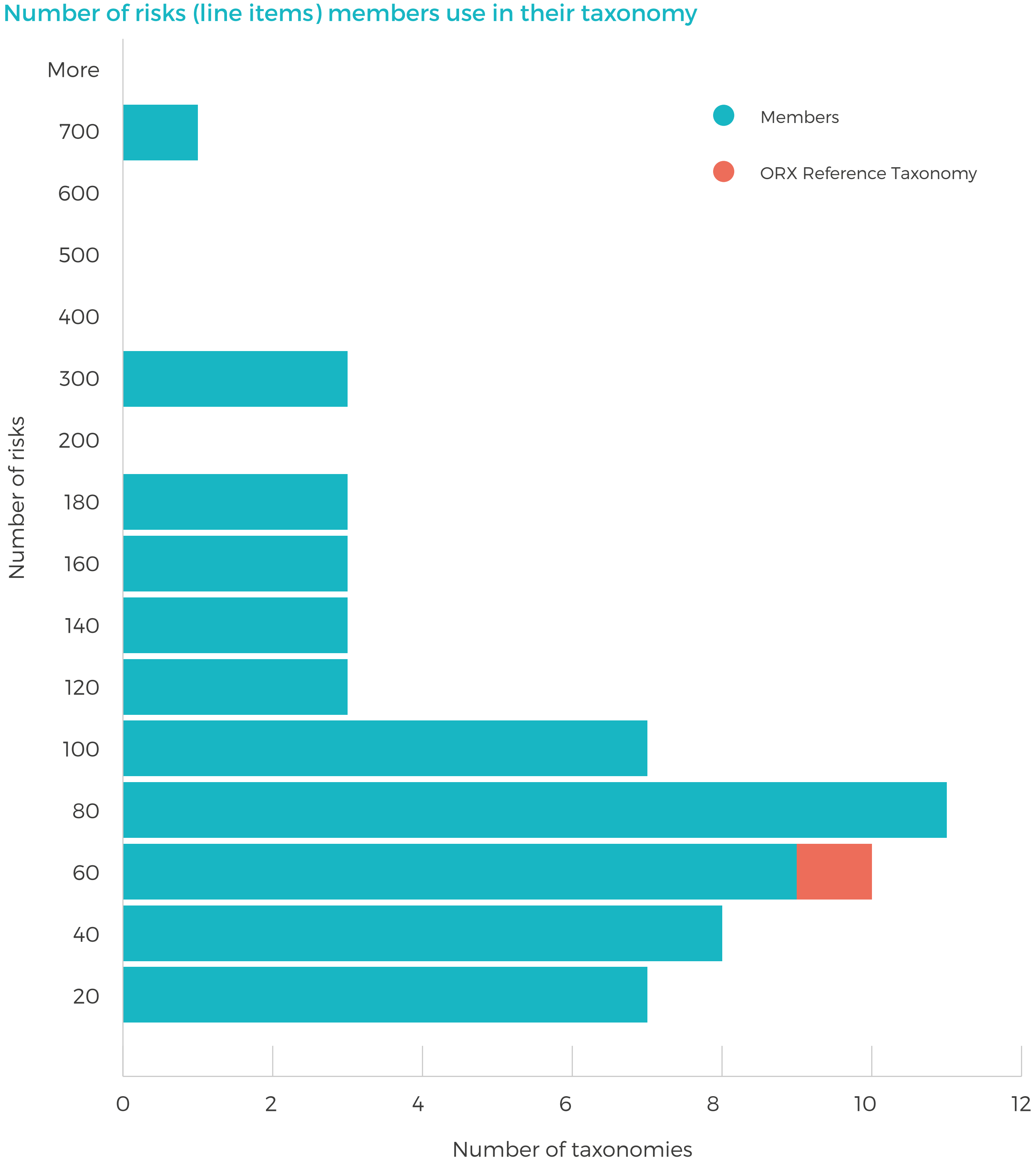
Figure 1. The 58 ORX members who participated in this exercise represented both the banking and insurance industries, as well as geographical regions



Summary

58 ORX member taxonomies were used as a basis for the data analysis, with an additional two used to validate the reference taxonomy approach. The ORX members in the dataset represent both the banking and insurance industry, as well as a range of geographical regions.

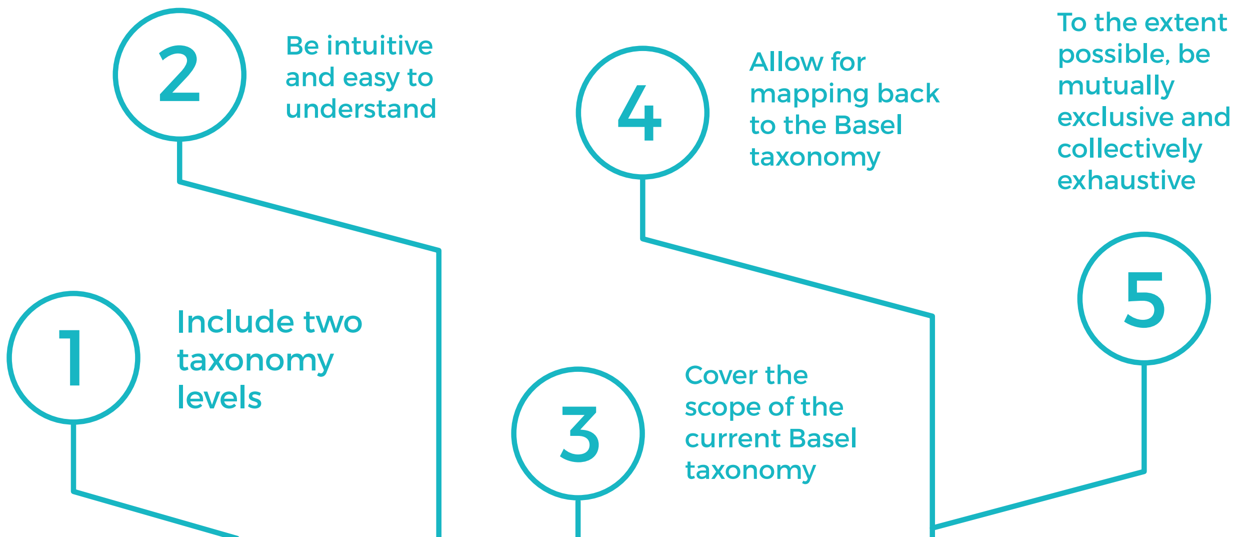
Figure 2. Distribution of the number of risks used in the 58 members' taxonomies shows a wide range of granularity at the lowest risk level.



Interquartile range: **36-116** Median: **69** ORX Reference Taxonomy: **61**

Method for constructing the ORX Reference Taxonomy

The ORX Reference Taxonomy was constructed to follow five design principles:



1 Include two taxonomy levels

2 Be intuitive and easy to understand

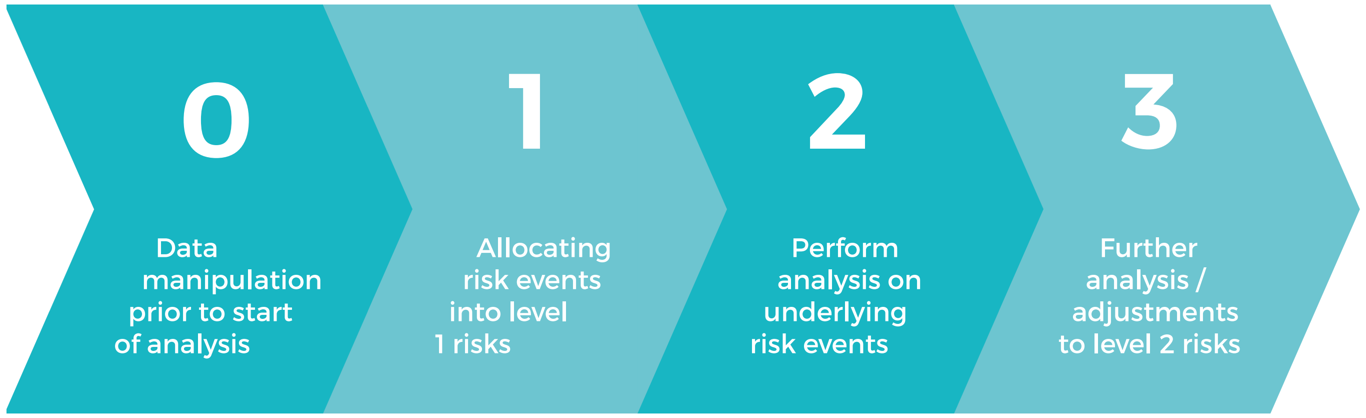
3 Cover the scope of the current Basel taxonomy

4 Allow for mapping back to the Basel taxonomy

5 To the extent possible, be mutually exclusive and collectively exhaustive

The method for constructing the ORX Reference Taxonomy is outlined in Figure 3.

Figure 3. Approach to constructing the Reference Taxonomy



0 Data manipulation prior to start of analysis

1 Allocating risk events into level 1 risks

2 Perform analysis on underlying risk events

3 Further analysis / adjustments to level 2 risks

0:
- Resetting the levels
- Assigned harmonised level 1 risks from members' taxonomies to the level 1 Reference Taxonomy

1:
- Group risks into distinct risk themes that form the basis of the level 1 categorisation
- Starting point is the level 1 reference taxonomy published in "Development in risk taxonomies" (July 2018)

2:
- For each level 1 risks, determine the most common categorisation(s)
- Assign each risk event to the level 2
- Adjust the set of level 2 categories as required by the data

3:
- Where the data has presented multiple ways of categorising the data, further analysis is performed to determine the most suitable method
- Feedback from advisory group panel (group and bilateral meetings) is incorporated to ensure the usability of operational risk practitioners

Using the data

In order to analyse the taxonomy data effectively, two key data manipulations were performed prior to the start of the analysis:

- Resetting the levels – the levels in the ORX Reference Taxonomy follow the same structure as the Basel taxonomy i.e. level 1 is positioned at the level as Internal Fraud, External Fraud, Employment Practices and Workplace Safety etc.; level 2 is at the level of Unauthorised Activity and Theft and Fraud under Internal Fraud. However, ORX members take a variety of approaches. Some define level 1 as Operational Risk, as part of their wider enterprise-wide risk management framework. Some anchor their level 0 risks as the Basel level 1 risks, and their level 1 risks at the same level as the Basel level 2 risks. As a consequence, the levels needed to be harmonised to ensure a like-for-like comparison during the analysis.
- The starting point of the analysis was the level 1 risks defined in the ORX 2018 study published in July 2018 titled "**Development in risk taxonomies**".[11] Following the harmonisation of the risk levels, we validated the ongoing appropriateness of the level 1 risks from the 2018 study and then assigned the harmonised level 1 risks from members' taxonomies to these risk events (using the names and descriptions, where available, provided by members).

Analysis undertaken

The 2018 ORX study titled "Development in risk taxonomies" highlights the need in the industry for improved risk taxonomies, whilst recognising the challenges in designing and integrating a new reference taxonomy. The paper outlined the emerging ORX Reference Taxonomy (in the form of level 1 risk events[12]). This previous analysis formed the basis of our work here to extend the reference taxonomy to level 2.

We subsequently performed a thorough review and analysis of taxonomies submitted by the 58 ORX members. Based on the members' data, a first version of the most common categories was determined. A semi-dynamic process followed: each risk event was assigned to a level 2 risk, and the risks were adjusted during the analysis to ensure it remained coherent (i.e. intuitive, exhaustive and non-overlapping). For some level 1 risks, the identification of "risk dimensions" was a useful stepping-stone to allow us to be able to correctly articulate the different but equally valid approaches members used to classify risk events. An example would be under External Fraud, where the universe of External Fraud can be subdivided into the following possible dimensions:

- Actor i.e. the party committing the fraud against the organisation
- Channel e.g. ATM, online fraud etc.
- Product e.g. card fraud, loan fraud, insurance claims fraud etc.
- Type e.g. misappropriation, forgery, theft etc.

Summary

The ORX Reference Taxonomy is designed to include two levels. It should be intuitive and easy to use. To the extent possible, it contains risks that are mutually exclusive and collectively exhaustive, and it should cover the full scope of the original Basel taxonomy.

Our construction approach is data driven. Member data has therefore been central to the development of this reference taxonomy, ensuring that, wherever possible, it represents common practice among organisations. Where our analysis identified more than one way to approach a risk theme within the risk taxonomy, we strived to represent the majority view or selected one that was most applicable to most members.

During the exercise, a subset of 8 members formed an advisory panel who confirmed our approach, gave extensive feedback on the design of the taxonomy and provided perspectives as the end users of the taxonomy.

[11] https://members.orx.org/orx-publications/developing-industry-op-risk-taxonomy-phase-one

[12] The paper outlines 15 level 1 risks. Given the requirement outlined in the five design principles to map the ORX Reference Taxonomy back to the Basel taxonomy, the decision was made to split Fraud into Internal Fraud and External Fraud. There were also some minor adjustments to the names of some level 1 risks e.g. Transaction Processing is now Transaction Processing and Execution; Financial Reporting and Tax is now Statutory Reporting and Tax

Member data in the driving seat

Member data has been central to the development of the ORX Reference Taxonomy, ensuring that, wherever possible, it represents common practice among organisations. Member taxonomies have idiosyncratic features. These are driven by factors such as regulatory environment, business profile and/or organisational structure. Where our analysis identified more than one way to approach a risk theme within the risk taxonomy, we strived to represent the majority view or selected one that was most applicable to most members.

To ensure our analysis led to a reference taxonomy that is usable by operational risk practitioners, a taxonomy advisory group was formed. This consisted of 8 ORX member organisations with representation from both the banking and insurance industry, and from various geographies and jurisdictions. This group gathered during the exercise to confirm the direction of travel, to feed back on the design, and to provide perspectives as the end users of the reference taxonomy. They were also consulted extensively, providing feedback on the resulting draft taxonomy and the guidance to ensure the final taxonomy was fit-for-purpose and intuitive to use.

An example – classifying the level 2 risks under Financial Crime

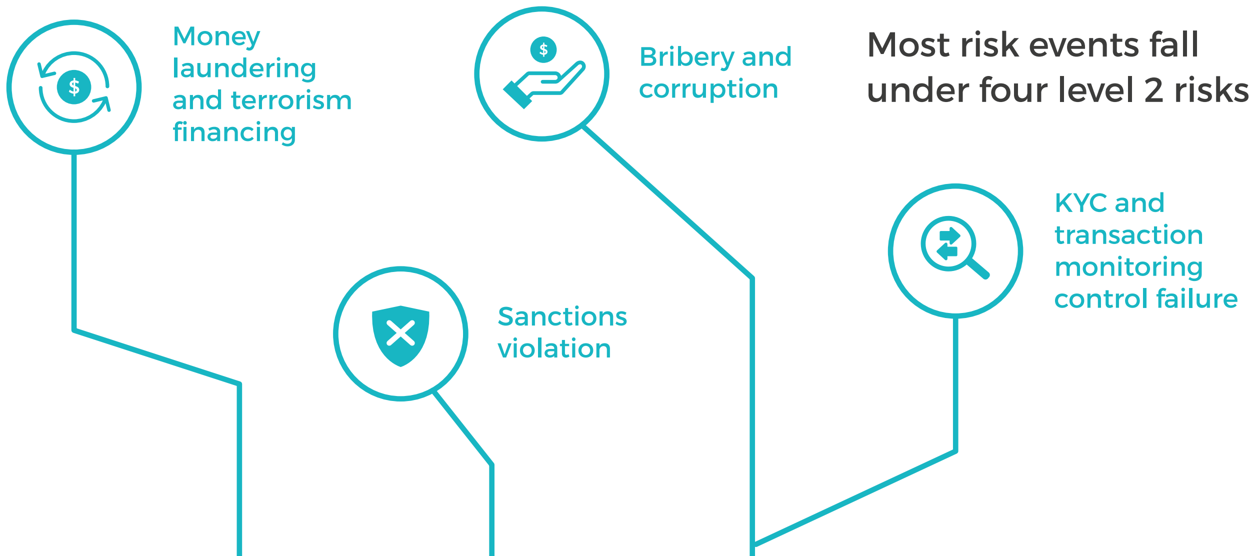
Let us illustrate our approach to establishing level 2 risks with a brief example on Financial Crime.

1. Given the analysis performed for the July 2018 level 1 reference taxonomy, our starting point was selecting the risk events identified under level 1 risk Financial Crime, broadly covering money laundering, financing of terrorism, sanctions, bribery and corruption, and actions resulting in financial crime-related regulatory breaches.
2. Our analysis showed that most of the risk events defined by members fall under the four level 2 risks shown in the diagram below.
3. We then made some final adjustments based on analysis of risks falling outside the four categories above:

   Employees not understanding legal or regulatory obligations with respect to money laundering and sanctions was a risk which breached our design principles as it would commonly be classified as a cause and was excluded.

   The organisation not being able to demonstrate adequate procedures to detect or prevent bribery and corruption was recognised as a potential risk event as it could directly lead to enforcement, fines etc. and was added to the list above.

Most risk events fall under four level 2 risks


Money laundering and terrorism financing
Bribery and corruption
Sanctions violation
KYC and transaction monitoring control failure

Further observations on the taxonomy data

Basel versus organic taxonomies

Members were asked to indicate whether they followed the Basel taxonomy structure or if they had developed their own taxonomy structure from the ground up.

Of the 58 initial sets of member taxonomies received, 25 members indicated that their taxonomy followed or was evolved from the Basel structure, whilst 33 indicated that they had developed their own structure.

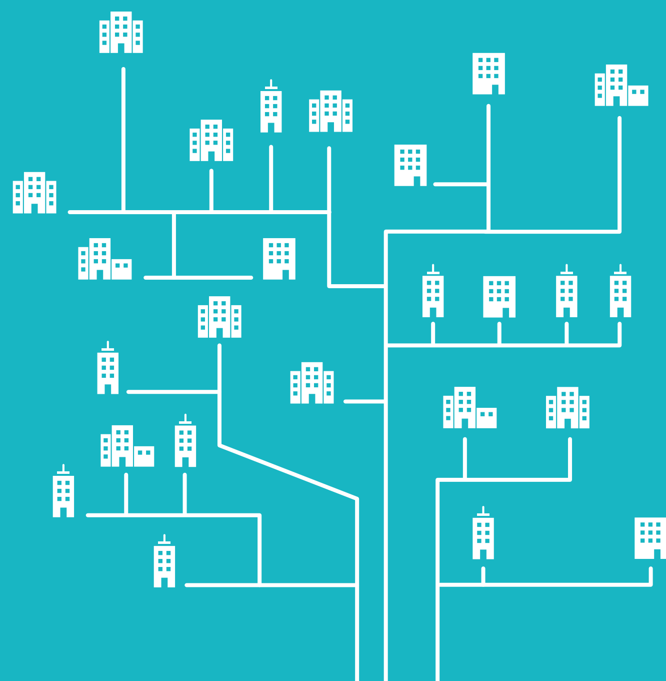
An overview of the risk events found in the Basel-based versus the self-developed taxonomies is shown in Figure 4.

Summary

Of the 58 taxonomies, 25 members indicated that their taxonomy was based on or evolved from the Basel structure, whilst 33 indicated they had developed their own structure.

We observed divergent practices amongst the members, even within those who indicated that they had followed the Basel structure. A range of risks currently receiving attention by members and regulators, but not included in the original Basel taxonomy (at level 1), have been added as level 1 risks by members within their taxonomical structure, e.g. Conduct, Financial Crime, Technology etc. This observation illustrates the evolving nature of taxonomies and confirms the value of defining the new ORX Reference Taxonomy.

25 members based on their taxonomy on the Basel structure



33 members developed their own taxonomy structure

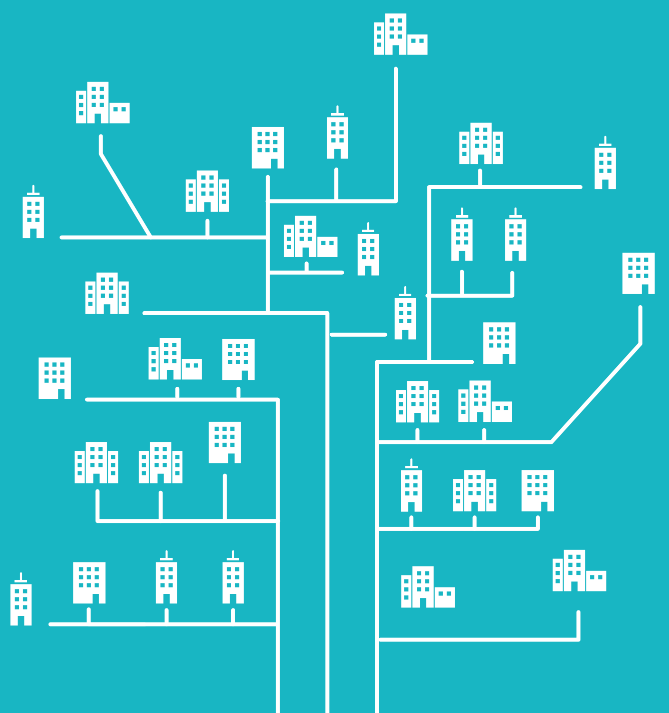
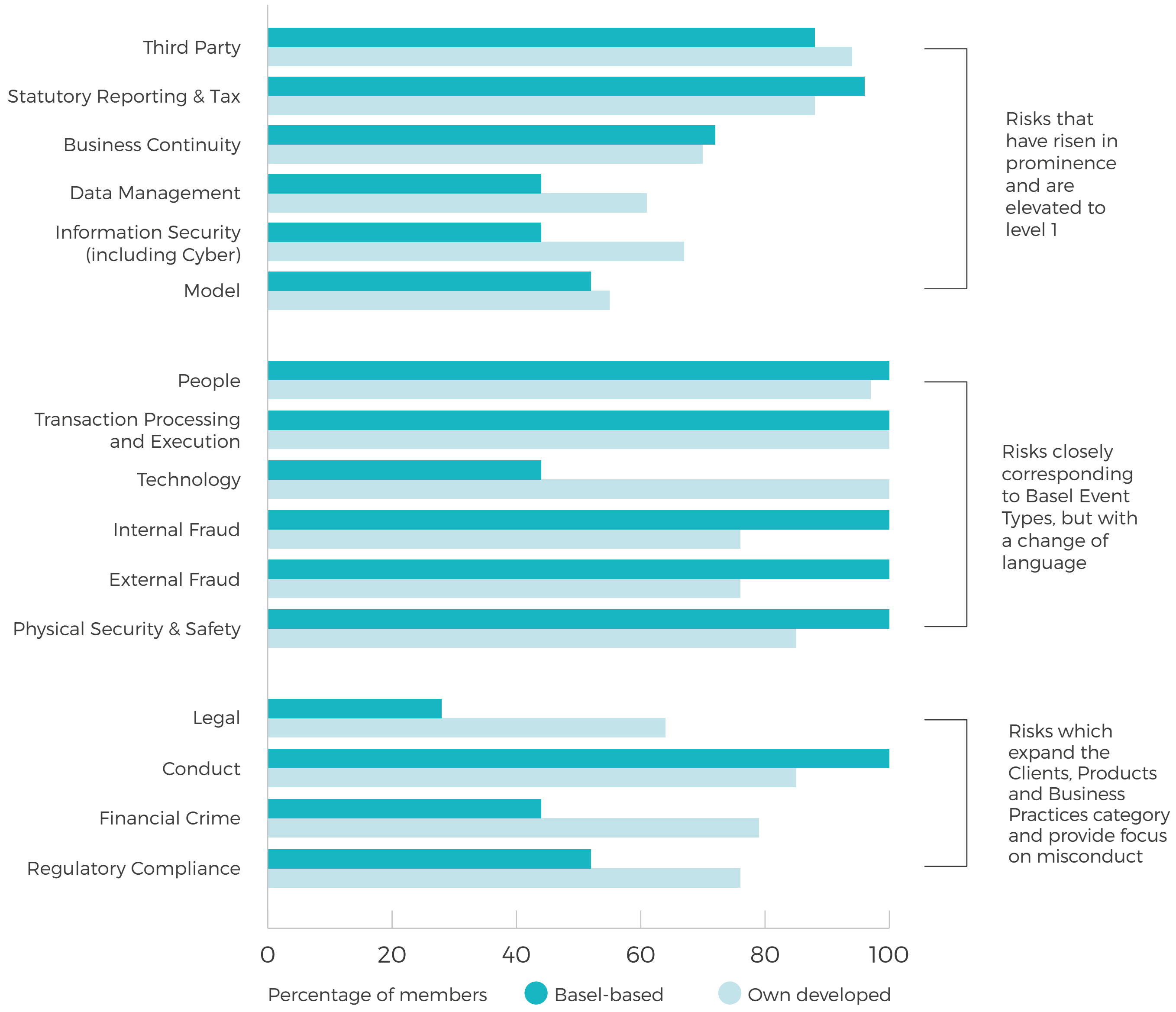


Figure 4. Level 1 risks featuring in Basel-based versus self-developed taxonomies (as a percentage of the total number of taxonomies respectively)



Increased number of level 1 risks

Figure 4 shows that the number of level 1 risks has increased from 7 Basel event types to 16 in the ORX Reference Taxonomy. Notably, this includes a range of risks that have risen in prominence and are elevated to level 1, but not included in the original Basel taxonomy (at level 1). This observation is valid for both those firms using a Basel-based taxonomy, as well as those having developed their own. Financial Crime, and Technology-related level 1 risks (Technology, Information Security including Cyber and Data Management) are examples of risks which have recently risen in prominence. The fact that this is observable (to different degrees) for both groups examined illustrates the need for members to evolve their risk taxonomies over time and hence confirms the value of this exercise to develop an industry reference taxonomy.

What is also evident from the data is that a taxonomy developed from the ground up creates more choices. Therefore, unsurprisingly, a larger proportion of self-developed taxonomies contained such risks. They also often included an increased number of level 1 risks, compared to Basel, reflecting these choices and the desire to elevate certain risks.

The need for evolution, however, does not appear equally pressing across all areas of the operational risk universe. There are risk types which have largely been retained by both groups of members. These include Transaction Processing and Execution, where all members have a category representing this risk. People, Third Party and Statutory Reporting & Tax were also largely retained, with only minor differences to Basel. This is noting that Third Party and Statutory Reporting and Tax have not been standalone level 1 risk types in the original Basel taxonomy, represented as Vendors and Suppliers and Monitoring and Reporting respectively – both level 2 risks under Execution, Delivery and Process Management.

There also remain areas of divergence across members, not limited to whether their taxonomies are Basel-based. Just over half of the taxonomies examined included Model as a level 1 risk. A possible interpretation is that Model risk is sometimes treated as a separate risk type alongside operational risk.

Use of risk themes

There is an emerging pattern in the member taxonomies of thematic risks as standalone level 1 risk categories, for example Conduct and Cyber. It was observed that the associated level 2 risks are often a grouping of risks associated to the theme, but which are relatively tightly defined (potentially in an attempt to avoid overlap and duplication across categories). This pattern may reflect the rise of such risks in the industry where organisations want to highlight them in their common operational risk language. It may also reflect how seriously organisations are taking these risks, reflecting the changes seen in the business and risk environment.

Use of “risk dimensions”

For some level 1 risks, members use combinations of different “risk dimensions” to define the level 2 risks. This is particularly prominent for:

- Conduct: the dimensions used relate to lack of market integrity, inappropriate behaviour towards customers, improper products and services and improper business practices
- External Fraud: actor, item, product and type
- Internal Fraud: target, channel, item, type and device

It is observed that rarely a single dimension is used exclusively for defining one risk, suggesting the implementation of the dimensions has been organic and perhaps in response to the ever-changing threats/risks, or regulatory focus. Short of revamping the entire taxonomy, organisations have opted for a less wholesale method of keeping up with the evolving risk environment.

Control failures

Some members have included certain level 2 risks that are, strictly speaking, causes/control failures. Examples observed include causes such as staff mismanagement, attrition and key person risk within People risk and third party non-performance within Third Party risk. Examples of controls failures, or control frameworks, include third party management control failure and KYC control failure.

This pattern may reflect the need to be pragmatic in constructing a taxonomy. This includes level 2 risks where there has been significant management and/or regulatory attention, particularly where control framework failures can result in events (e.g. fines for weak AML controls). The inclusion of certain control failures as events, therefore, reflects the increasing likelihood that organisations are penalised or fined for inadequate controls, leading to certain control failures becoming an event in their own right.

Deep dives

In this section, we discuss six level 1 risks in more detail, including: Conduct, technology-related level 1 risks i.e. Technology, Data Management and Information Security (including Cyber), and Third Party.

The section covers:

- Our observations of relevant industry trends:

  We look at evolution of the risk type as well as regulatory pressures that have brought the risks into the forefront of risk management. We also describe the trends and practices that we have observed in the categorisation of the underlying risks from the dataset of ORX members.

- Our approach to categorising the risk:

  More than one approach to categorise these risks is observed. Therefore, our approach was to select a categorisation method that is most commonly observed (as evidenced by the dataset) and that produces an internally consistent reference taxonomy i.e. minimising conflict or overlap with other level 1 risks, not leaving any gaps, and respecting the bow tie philosophy.

Conduct:

The majority of members represent Conduct through a separate level 1 risk category. Upon analysis, this contained risks that can be thought to have a significant or primary Conduct impact such as compromise of market integrity or inappropriate behaviour towards customers. Such risk events may also lead to financial loss, but the Conduct impact provides the rationale for grouping them under a Conduct category.

In keeping with the practice observed by the majority of members, the ORX Reference Taxonomy thus contains a level 1 risk event, Conduct, the scope of which is based on the most prominent risk events found in ORX member taxonomies.

We recognise that many more risks can have a Conduct impact and therefore organisations may wish to look beyond those risks listed in the ORX Reference Taxonomy to establish a holistic view of Conduct. An often-cited example of the need for this is a sustained systems outage leading to customer detriment. Because of this, the use of Conduct as a level 1 category might appear somewhat optional. If a comprehensive view of Conduct requires a full view of related impacts across the taxonomy, the use of a Conduct category may risk inappropriately narrowing the perception of Conduct as a risk management discipline. Yet the benefits of elevating the topic to level 1 with the associated governance and visibility appears to have outweighed such concerns at the majority of member organisations.

Whereas many ORX members do include a Conduct category, we fully acknowledge the different and divergent approaches used by others. It is important that an organisation uses an approach appropriate to their needs and we encourage organisations to continue to define their own approach to managing Conduct. This is very much why ORX is positioning this as a reference taxonomy and not as a wholesale standard.

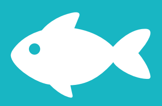
Cyber/technology risks:

Events in this area can be interlinked as they rarely occur in isolation. We have chosen to approach these risks in a manner that we believe reflects the majority member view, and that allows us to produce an internally consistent taxonomy. The resulting three level 1 risks are:

- Information Security (including Cyber): including cyber events and data-related security events
- Data Management: data events, excluding data-related security events
- Technology: failure of hardware, software and network

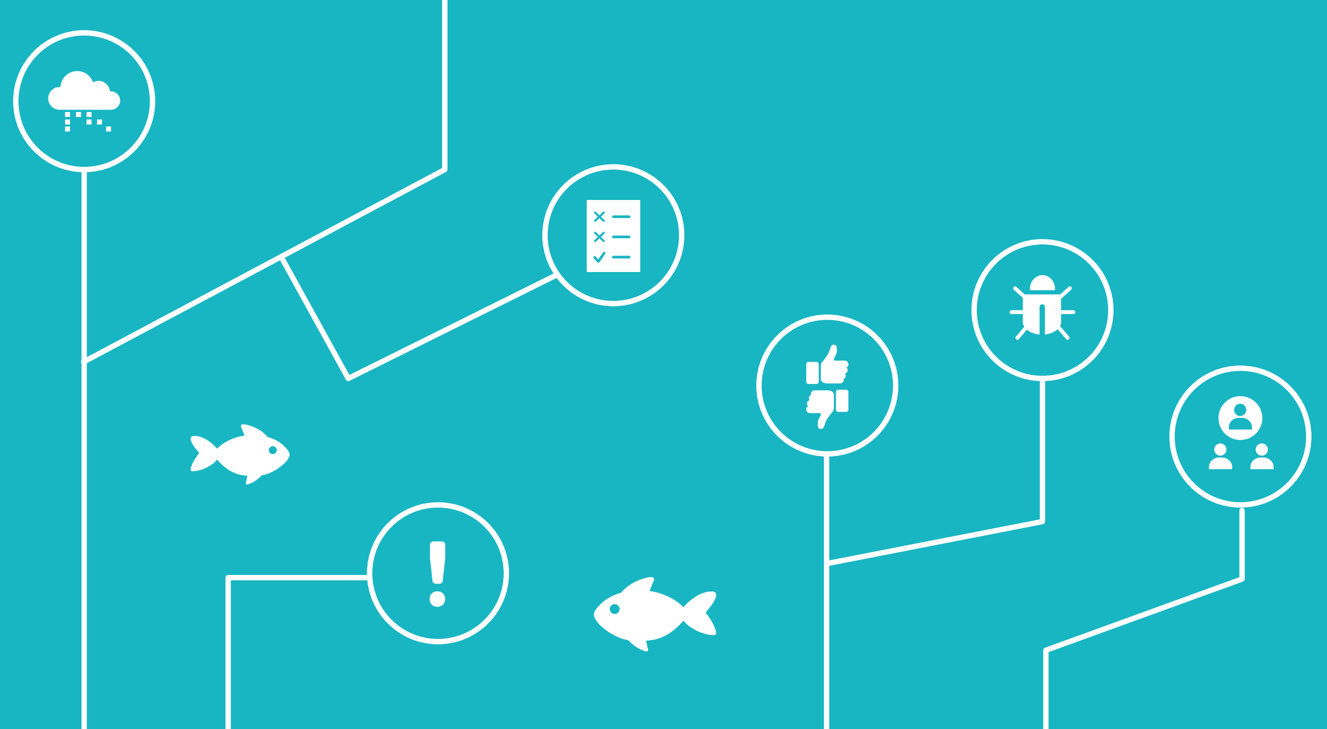
Third party:

To ensure a clear separation between categories and to avoid overlap with other level 1 risks, we have selected a narrow definition of Third Party to only cover risks that relate to the use of a third party e.g. onboarding, management and termination of a third party engagement.



Summary

Our analysis showed that the industry has yet to find consensus on a small number of operational risks for which we found divergent approaches. We include a deep dive on these risks as part of this report.



Conduct

Industry context

Following the recent trend towards heightened regulatory scrutiny, Conduct has quickly risen to the top of many corporate risk agendas, and now represents one of the **top industry concerns**.[13] The increased scrutiny has been fuelled by a series of well-publicised misconduct events, e.g. the 2016 FX rate-rigging scandal that led to almost €5 billion in combined regulatory penalties.[14] Meanwhile, dedicated structures to supervise Conduct have emerged, with multiple jurisdictions adopting the "twin-peaks" model which separates macro-prudential supervision from Conduct oversight.[15]

While the importance of Conduct – both to regulators and the industry – is undeniable, there exists significant variation in the way Conduct is defined and categorised across jurisdictions. The variation results in substantial divergence between ORX member taxonomies, with a wide range of associated risk event types. A significant minority of member taxonomies do not explicitly include Conduct, with it being considered a cause, impact or as a risk theme represented by a flag.

We wish to emphasise that having Conduct reflected as a risk category does not preclude reporting a broader view on Conduct through the use of impact categories or flags. It is therefore possible to both maintain a Conduct event category and report a broader view at the same time. It is equally possible to report a broad view of Conduct without it being recognised as a level 1 risk event.

Our approach

In developing a reference taxonomy that encompasses Conduct, we are hoping to provide a common language when discussing the multiple facets of Conduct. Notwithstanding, it is important that an organisation uses an approach appropriate to their needs and we encourage organisations to continue to define their own approach in defining and managing Conduct.

To serve the above purpose and also capture the jurisdictional diversity of Conduct issues, we have articulated the scope of Conduct based on the preponderant categories found in ORX member taxonomies, and those that are considered to have a primarily Conduct impact. Indeed, the dataset supports the use of a distinct Conduct level 1 risk, with the majority of members representing Conduct through a separate risk event category:

- Almost a quarter of the ORX members (14 out of 58) explicitly define these risks under a level 1 banner called Conduct.
- A further 23 members use the Basel terminology, Clients, Products and Business Practices, or a variation thereof to group risks which have a predominant Conduct impact. Examples of level 2 risks under this terminology include Suitability, Breach of duties to customers, Advisory Activities, Customer Service Issues/Complaints Handling, Aggressive Practices etc.
- A further 6 members refer to the underlying Conduct risk types without using an overarching banner to group these (either the Conduct or Clients, Products and Business Practices).
- 6 members do not explicitly refer to Conduct risk types or use terminology that implies the risk is included in the event taxonomy.

Lower level Conduct risk types were grouped into four categories which distinguish Conduct in the context of markets, customers, products/services, and internal practices, i.e.

1. **Lack of market integrity – level 2 risks include:**
   a. Insider trading
   b. Anti-trust/anti-competition
   c. Improper market practices
2. **Inappropriate behaviour towards customer – level 2 risks include:**
   a. Pre-sales service failure
   b. Post-sales service failure
   c. Client mistreatment/failure to fulfil duties to customers
   d. Client account mismanagement
3. **Improper products and services – level 2 risks include:**
   a. Improper distribution/marketing
   b. Improper product/service design
4. **Improper business practices – level 2 risks include:**
   a. Whistleblowing
   b. Breach of code of conduct and employee misbehaviour

We recognise that many more risks can have a Conduct impact and therefore organisations may wish to look beyond those risks listed in the ORX Reference Taxonomy to establish a holistic view of Conduct. An often-cited example of the need for this is a sustained systems outage leading to customer detriment.

Because of this, the use of Conduct as a level 1 category might appear somewhat optional. If a comprehensive view of Conduct requires a full view of related impacts across the taxonomy, the use of a Conduct category may risk inappropriately narrowing the perception of Conduct as a risk management discipline. Yet the benefits of elevating the topic to level 1 with the associated governance and visibility appears to have outweighed such concerns at the majority of members.

The potential need to obtain a holistic view of conduct has also led to the wider use of causal and impact taxonomies, as well as the use of flags for analysis and reporting. For example, a systems outage that results in customer detriment may be recorded as a technology event with customer impact and/or with a Conduct flag.

Cyber/technology risks

Industry context

Technology risk has in recent years become one of the leading risk agenda items for both private and public organisations. Rapid technological advances and increasing digitalisation have resulted in data being central to the vast majority of business processes.

While the use of new information technologies has generally enabled faster, smoother and more precise operations, organisations have had to balance the trade-off between the efficiency gains with the increased exposure in technology-related risks. A particular concern is the constantly evolving cyber threat landscape which puts at risk not only internal operations, but also confidential customer information.

[13] Operational Risk Horizon report, ORX (2019): https://members.orx.org/orx-publications/operational-risk-horizon-2019

[14] ORX News, 2016

[15] For example, in 2013 the UK's Financial Services Authority was split into the Prudential Regulation Authority and the Financial Conduct Authority under a 'twin-peaks' system

Our approach in defining level 1 cyber/technology risks

Developing a common taxonomical understanding of technology-related risks is a key facilitating factor for sharing threat information effectively. Our data-driven approach was to define these risks under three level 1 risks:

1. **Information Security (including Cyber) – broadly divided into two groups of level 2 events:**
    - Cyber Events (independent of the presence of system or data compromise): Our data supports the emergence of cyber as a key risk. 9 ORX member taxonomies contain standalone risk events that refer to cyber events. Although it can be argued that this is usually a cause of an event (e.g. fraud, information security breach, system outage), there are instances where this can be a standalone event e.g. DDOS attack leading to customers unable to use online banking.
    - Data-related security events: All of the following level 2 events are defined as standalone events i.e. independent of the presence of a cyber-attack, system outage, or consequences (e.g. used to steal funds/ identity of customer)
        - Improper access to data
        - Data theft/malicious manipulation of data
        - Data loss

2. **Data Management:**

    21 ORX member taxonomies out of the 58 contain standalone data events:

    - Over half of these (12 of the 21) contain the following level 2 data-related events
        - Unavailability of data
        - Poor data quality
    - Almost two thirds (14 members of the 21) contain the following level 2 Data Management events:
        - Inadequate data architecture/IT infrastructure
        - Inadequate data storage/retention and destruction management

3. **Technology:**

    Of the 40 ORX members whose taxonomies contain standalone technology risk events, 35 have used a type of failure (e.g. no longer fit for purpose, not performing as expected, not available) as a dimension to distinguish level 2 risks; 19 members use the distinction of Hardware, Software,[16] Network to segregate the level 2 risks. We have selected the parts of the system that failed (Hardware, Software, Network) to distinguish the level 2 risks, as the type of failure can imply cause and therefore may inadvertently mix the different parts of the bow tie (i.e. cause, event, impact).

Our approach to the categorisation of interlinked events

Given the interdependent nature of the risk category, certain risk events may be directly tied to other events, each of which could separately lead to an impact, such as a regulatory fine. In these cases, we have recommended capturing two distinct (but linked) risk events using appropriate level 2 risks. Recognising that it may be challenging in practice to classify one incident as two separate events, an alternative approach could be to use reporting tools (such as a flag) to identify a risk event as related to Information Security when a member deems it more appropriate for the primary categorisation to be to another event type (or vice versa).

Examples of these events include:

- Cyber-attacks leading to privacy breaches are considered two separate risk events mapped to the level 2 risks of Cyber events and Data privacy breach/confidentiality mismanagement under Information Security.
- System failures leading to data privacy breaches, and likewise, cyber-attacks with systems compromise, each represent two separate risk events mapped to Technology and Information Security. Fraud committed via an internal or external information security event, e.g. an employee stealing client data to embezzle client funds, constitutes an Information Security event, and a separate Internal/External Fraud event.

The proposed approach allows for the identification of different sets of controls that are associated with separate risk events.

[16] Software would include applications, middleware and operating systems; utilities would be a subset of applications

Third Party

Industry context

As noted in Oliver Wyman's publication on the **increasing modularisation of financial services**,[17] firms are using more third party suppliers than ever before to support a wide range of their BAU operations, from specialist services, back office process and risk capital etc.

Third parties are used to create scale efficiencies or to access expertise that is too difficult or too costly to build internally, leading to a robust rate of growth of new entrants, particularly in the Fintech space. Regulatory attention on third party risks has therefore also grown in tandem, and consequently it is now considered one of the top emerging risks.[18]

The increasing exposure to third parties and suppliers has created a new layer of operational risk for which regulators are holding financial organisations accountable across jurisdictions. Meanwhile, the rising interconnectedness of third and fourth party networks poses significant new challenges to the management and monitoring of these risks.

A unified understanding of third party risks is therefore of key importance. A major challenge in developing taxonomical guidance is the scale and breadth of outsourcing arrangements.

Our approach

There are broadly two types of risks related to the use of third parties:

- Events caused by third parties:

    These are events that could occur with or without the use of a third party e.g. payments system outage could be caused by a third party (if the payments process is provided by a third party) or by the organisation (if the process is managed in-house).

- Events relating to the use of a third party:

    These are events that would only occur if the organisation engaged a third party. Most commonly these are events relating to a third party control failure (e.g. failure to perform proper onboarding checks), third party violating applicable regulations when performing services for/on behalf of the organisation, or third party not adhering to the organisation's standards.

To ensure a clear separation between categories, we have chosen to only include events relating to the use of a third party. We have therefore selected a relatively narrow definition of Third Party:

- Third party management control failure: Failure to develop and maintain an adequate third party control framework
- Third party criminality/non-compliance with rules and regulations: Risk of third party violating applicable rules and regulations[19]
- Inadequate intra-group agreements SLA: Intra-group arrangements not meeting requirements

Our approach is supported by the data from the 58 ORX members' taxonomies:

- Of the 58 members, 53 have Third Party as a standalone risk type
- Of the 53 who have Third Party as a standalone risk type, only 13 member taxonomies contain risk events that, using the above definition, we would classify as other level 1 risks e.g. Business Continuity event caused by a third party

Notwithstanding, members may wish to consider using specific reporting tools (e.g. flag) to capture and aggregate all risk events that are directly linked to a third party cause or that have a direct impact on third parties e.g. for reporting and analysis purposes.

[17] Modular Financial Services, The New Shape of the Industry, Oliver Wyman, 2016: **https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/jan/OliverWyman_ModularFS_final.pdf**

[18] Operational Risk Horizon report, ORX (2019)

[19] Third party criminality/non-compliance with rules and regulations under Third Party is distinct from Third party/vendor fraud under External Fraud, as in the former case the target is not the organisation, whist in the latter case the target of the fraudulent activity is the organisation.

The ORX Reference Taxonomy[20]

Level 1 Risks	Level 2 Risks
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 & Safety	Damage to organisation's physical asset
	Injury to employee or affiliates outside the workplace
	Damage or injury to public asset
Business Continuity	Inadequate business continuity planning/event management
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

Level 1 Risks	Level 2 Risks
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
	KYC and transaction monitoring control failure
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

[20] This more detailed ORX Reference Taxonomy and 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. There is also a public summary of the ORX Reference Taxonomy which is freely available for all financial organisations to benefit from. Commercial use of both the summary and detailed 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. (Copyright ORX 2019)

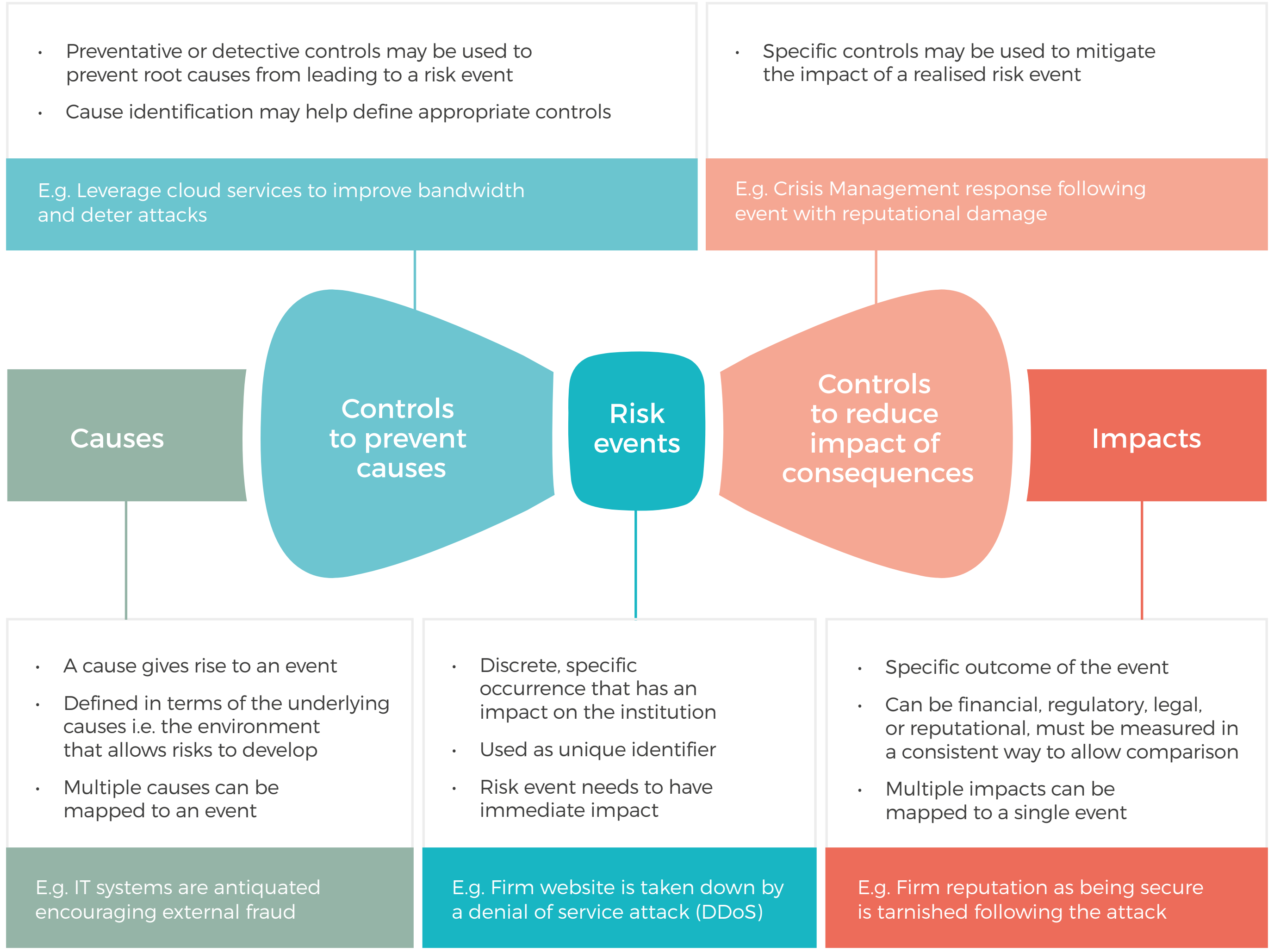
Appendix: bow tie methodology

The ORX Reference Taxonomy is based on the “bow tie” method (see Figure 5), which distinguishes between causes, events, impacts and controls. These are defined as follows:

- **Cause**: The risk causes constitute the underlying environment that allows risk events to develop. These causes therefore go beyond the immediate triggers of an event, such as control failure. Multiple causes can be mapped to an event.
- **Event**: The risk event is the central element of the framework, and is a discrete, specific occurrence, one degree removed from the impact on the organisation or its stakeholders.
- **Impact**: The risk event can have direct and/or indirect impact on an organisation and its stakeholders. Multiple impacts can be assigned to a risk event.

Figure 5. Bow Tie Method

The “bow tie” method is used to ensure that only such events are captured by the taxonomy which plausibly lead to a direct impact.



- 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

Causes
Controls to prevent causes
Risk events
Controls to reduce impact of consequences
Impacts

- 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

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 detailed ORX Reference Taxonomy guidance is provided free of charge to all ORX members. It is available to other financial organizations – please contact communications@orx.org for further details. Commercial use of both the summary and detailed 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.

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

OLIVER WYMAN

O.R.X