Guidance document

O.R.X

ORX Reference Control Library for operational and non-financial risk

Managing risk together

orx.org

Contents

3 Introduction

4 How to access the library

5 The library structure

6 What is the ORX Reference Control Library?

7 Approach used to develop the library

10 General and specific control observations on level 1 risk types

Introduction

A move to use control libraries

Over recent years, a growing number of financial services organisations have independently developed operational and non-financial risk (ONFR) control libraries to provide greater structure and standardisation in how internal controls are identified, assessed, reported, and ultimately managed. While organisations report that the development and maintenance of a control library deliver clear benefits, it is both a complex and time-consuming process, **with a majority of libraries taking 1-2 years to develop**. Furthermore, at an industry level, the lack of standardisation of controls across financial services organisations both extends the time that it takes to develop a library and limits the scope for benchmarking and sharing of insights across organisations.

Development of an ORX Reference Control Library

Against this backdrop, ORX, along with McKinsey & Co. as a knowledge partner, have developed an industry Reference Control Library for ONFR in financial services ("the ORX Reference Control Library" or "the library"). The ORX Reference Control Library builds on the success of the **ORX Event Type Reference Taxonomy**, is based on control data collected from nearly 50 FS organisations (the majority of such data available from the membership) and contains controls covering the scope of, and aligned to, the ORX Event Type Reference Taxonomy. At the time of publication in early 2022, the ORX Reference Control Library is the most comprehensive global effort of its kind across financial services organisations.

What the ORX Reference Control Library provides

ORX believes that this library, while not intended to be an exhaustive list of controls, advances the industry's practice in this area. When using the library, it is important to note that:

- **It is a reference** – This first version provides a broad view of the typical key controls used by a range of ORX members for each risk. It is informed by a wide range of organisations across a variety of geographies and business lines (both banking and insurance). As a result, there will be controls in the library that may not be applicable to every financial services organisation.
- **It can be used in a number of ways** – Given the thematic nature of some risks, the library can be approached in different ways and can be adapted to your business as required. Because of its origins in industry data, the library provides a good guide to the typical controls to be considered. However, depending on your organisation's business mix and risk profile, some controls may be less relevant, and you may also wish to be more or less granular. In addition, some controls may align to risks different to those mapped in the ORX Reference Control Library. Section 4 on "Specific control observations" includes more details.

ORX will seek feedback from our members on the library and will evaluate the need to update it in the future. We are conscious that the business environment is continuing to evolve at pace and organisations report that they are currently developing or enhancing libraries. Both factors may drive the need for future iterations based on enhanced member data.

Purpose of this document

The purpose of this document is to:

Summarise the aims and anticipated benefits of using the library

Explain how to access the library

Clarify the structure of the library

Share the methodology and considerations used to create the library

Aims of the ORX Reference Control Library

The key aims of the library are to support organisations to:

- Benchmark their internal control instances or library against industry practice and inform control enhancements/control optimisation activities
- Expedite the development of their own control library (if they are developing one)
- Provide additional guidance to the first line of defence when carrying out their risk and control assessment processes
- Develop and standardise controls practices across the financial services industry

In the future, we also hope that the library can be used as part of ORX data sharing services, increasing the risk management learnings that can be taken from scenarios, loss data, etc.

How to use this document

This document is intended as user guidance for interpreting and applying the ORX Reference Control Library.

- Section 2 summarises the structure of the library
- Section 3 describes the approach used to develop the library, including inputs and considerations
- Section 4 sets out key observations and guidance for the library controls by each level 2 risk (as set out in the ORX Event Type Reference Taxonomy).

How to access the library

The library can be accessed in the following two ways:

1 **In a digital format** – The digital view allows the controls to be more easily displayed against each L2 risk.

2 **In an Excel spreadsheet** – This format may be useful if benchmarking against internal control instances or an existing internal library.

Access the library

The library structure

The ORX Reference Control Library is a collection of reference controls organised systematically to two control levels. It is intended to serve as a guide to the typical key controls used to mitigate ONFR across the financial services industry and, as a result, it is more granular and comprehensive than a control taxonomy. The library includes 761 level 2 controls, which is close to the median size of the organisations' control libraries used to inform its development. The library is linked to the ORX Event Type Reference Taxonomy, as shown in the diagram on page 6. The diagram provides examples of each of the fields (e.g., level 1 risk).

In the library:

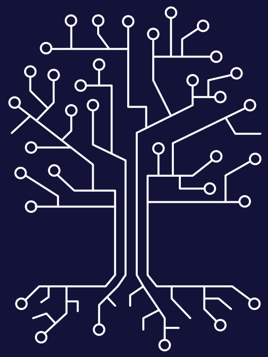
- Risks are categorised in line with the ORX Event Type Reference Taxonomy (level 1 risks and level 2 risks).
- Controls are presented following a two-level structure as follows:
  - Level 1 reference control: these are general control categories (e.g., governance and oversight) and may therefore apply to multiple risk types.
  - Level 2 reference control: these involve a greater level of detail – reference controls at this level are specific to the level 2 risk that they address. Each level 2 has a sanitised description leveraged from member data.

The ORX Reference Taxonomy

The ORX Reference Control Library is aligned to the risk categories in the ORX Reference Taxonomy.

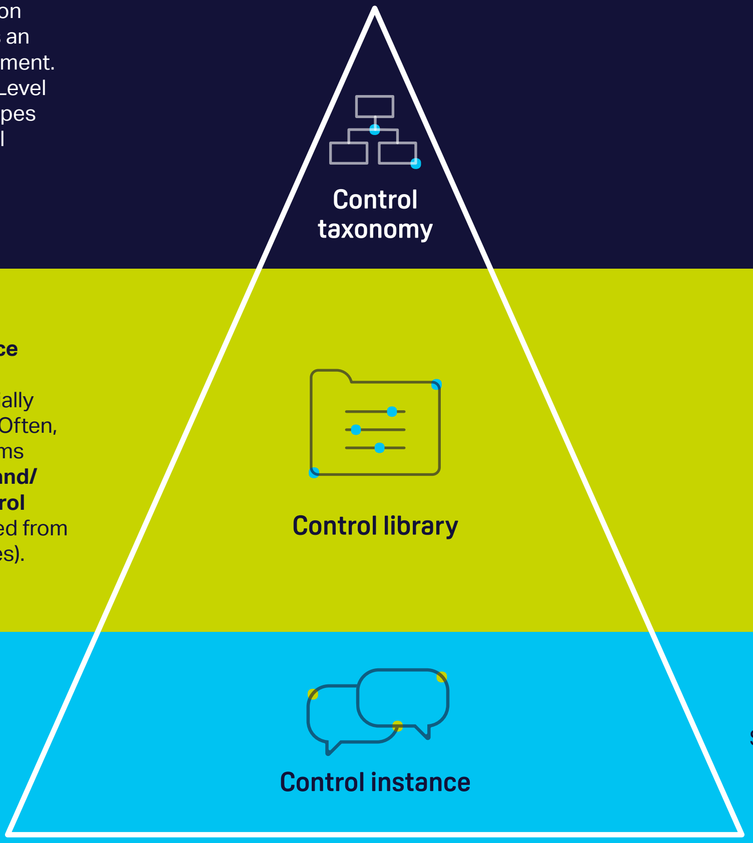
The ORX Reference Taxonomy for operational and non-financial risks is made up of the Event Type Taxonomy, covering level 1 and level 2 risks, and the Cause and Impact Taxonomy, which provides even more insight.

The taxonomy incorporates more contemporary risks (for example cyber, conduct and third party) while not moving completely away from the Basel Event Types.



Download the full report and guidance

What is the ORX Reference Control Library?



A high-level classification of the types of controls an organisation may implement. This typically contains Level 1 and Level 2 control types supported by high-level objectives.

Control taxonomy

High level/generic

Categorisation of controls

Used during RCSA to categorise controls

Typically less than 100 control categories

A collection of **reference controls organised systematically**, potentially to **two or three levels**. Often, data is described by firms as **control objectives and/ or their minimum control standards** (often derived from group/corporate policies).

Control library

More granular

Reference controls

Used to instruct/guide 1LOD on required controls

Range >100 to >20,000 control categories

A specific **local occurrence** of a control. It may be linked/mapped to a library control or taxonomy control category, and typically more **detailed and tailored** to the specific local circumstance.

Control instance

Most granular

Specific local occurrences of controls

Used during RCSA and control monitoring and assurance activities

Range from >500 to the 10,000s of control instances

Snapshot of the library

Control ID	FC3	FC4	FC5
ORX Reference Taxonomy Risk Level 1	Financial Crime	Financial Crime	Financial Crime
ORX Reference Taxonomy Risk Level 2	Bribery and corruption	Bribery and corruption	Bribery and corruption
Control Level 1	Due diligence	Due diligence	Due diligence
Control Level 2	Contract ABC checks Associated party/person due diligence	Contract ABC checks	Employment and Work Opportunities Employee ABC checks
Control Description	Controls in place to ensure that all Associated Persons have been identified and risk assessments have been completed and recorded as per the AP Policy.	Controls to ensure contracts are reviewed to identify bribery and corruption related risks and escalate for resolution.	Screen employees to identify any corruption or bribery related issues affecting onboarding

Approach used to develop the library

Inputs

The development of the ORX Reference Control Library was informed by the following inputs:

The set of level 1 and level 2 risks identified in the 2019 ORX Reference Risk Taxonomy

Published in October 2019, **the ORX Event Type Reference Taxonomy** provides a consistent language for the industry to refer to when speaking about operational and non-financial risk and proposes a way to categorise these risks. The taxonomy was the base against which the controls were mapped and organised.

Control data submitted by 47 ORX members

Member data has been central to the development of the ORX Reference Control Library, ensuring that, wherever possible, it represents widespread practice among institutions. It is important to note that members' control libraries vary significantly in focus (on account of idiosyncratic features driven by factors such as the regulatory environment, business profile and/or organisational structure) and in size and detail (the total number of controls in the libraries reviewed ranged from 100 to 20,000+ controls).

A set of principles to guide the design

The ORX Reference Control Library was designed to follow these principles:

1. Cover the scope of the ORX Event Type Reference Taxonomy
2. Allow for mapping back to the ORX Event Type Reference Taxonomy
3. Include two control levels
4. As far as possible, provide a broad coverage of key controls for each risk type, not an exhaustive list
5. Reflect control levels that are representative of the input data received
6. Where a control is used to mitigate multiple risks, e.g., Customer Due Diligence controls, the control is mapped against each relevant risk

Review and input from the Risk Control Advisory Panel

As part of this effort, ORX formed a Control Advisory Panel consisting of member institutions with representation from both the banking and insurance industries and from various geographies/jurisdictions. The group met regularly to confirm the approach, provide feedback on the design of the library and offer perspectives as the end users of the library.

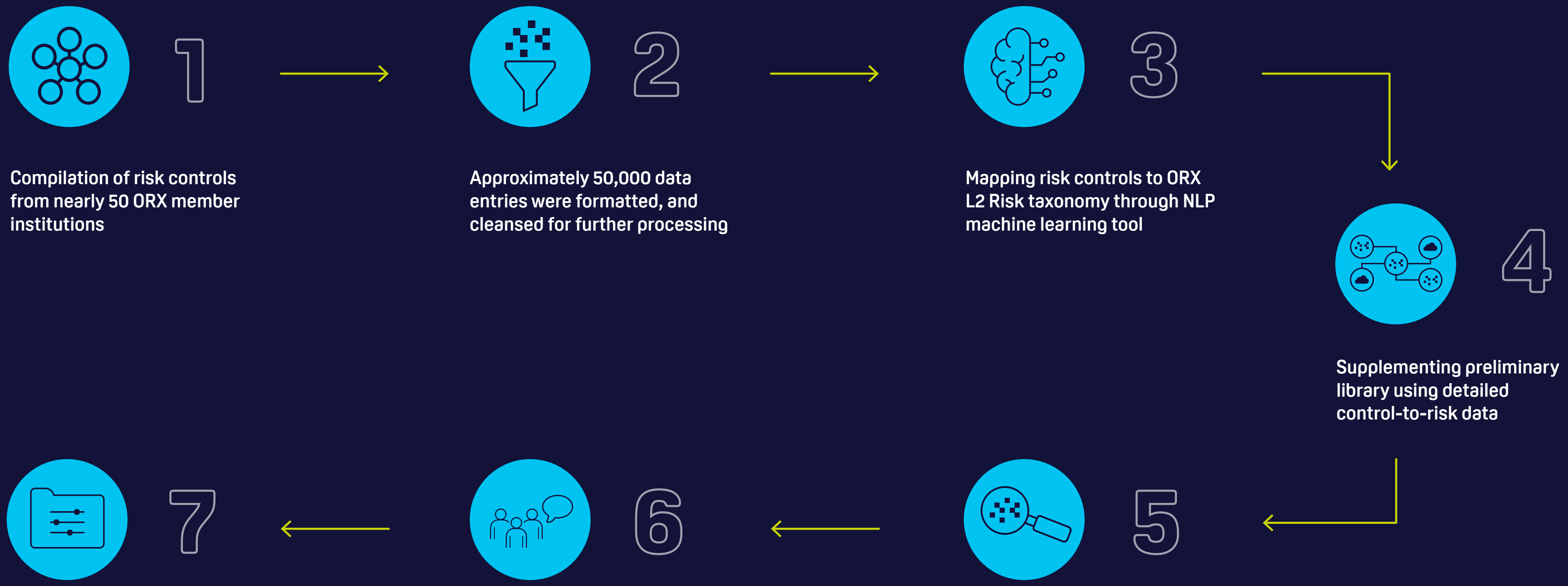
Reference Control Library methodology

In developing the ORX Reference Control Library, data was, again, in the driving seat. As with the ORX Event Type Reference Taxonomy, the control library is based on control taxonomy and library data collected in 2021 from nearly 50 member institutions (banks and insurers).

How we developed the library of controls for each of the level 2 risks::

1. Nearly 50 ORX member institutions shared control data
2. ORX member control data with approximately 50,000 data entries were formatted and cleansed
3. The control data were organised using machine learning, through a Natural Language Processing (NLP) tool
4. The controls were then refined using control-to-risk mappings provided by some member institutions
5. The data was reviewed by McKinsey domain experts and ORX, considering both coherence and completeness
6. The data was reviewed by a panel of experts from ORX member firms (including risk specialists) and feedback was incorporated into both the library and the accompanying guidance document
7. ORX Reference Control Library finalised and published

How we developed the ORX Reference Control Library



1 Compilation of risk controls from nearly 50 ORX member institutions

2 Approximately 50,000 data entries were formatted, and cleansed for further processing

3 Mapping risk controls to ORX L2 Risk taxonomy through NLP machine learning tool

4 Supplementing preliminary library using detailed control-to-risk data

5 Refinement of library using ORX, McKinsey experts

6 Refinement of library using Advisory Panel inputs

7 Publish ORX Reference Control Library

Considerations in data gathering and use

Data considerations and how they were addressed

Institutions have different risk management structures and processes in place, as well as being at various levels of maturity and at different stages in their control framework design. The control data provided by each of the participating ORX member institution for this exercise varied significantly in structure, format, and granularity, as described below. A manual review and data cleansing process was conducted to address the two points below prior to using the NLP tool.

Structure and source formatting: As anticipated, there were variations across member institutions' libraries relating to how controls were documented both in terms of detail and dimensions (e.g., some controls were mapped to processes, other controls were mapped to risks, and others did not have any mapping).

Granularity: In addition, the level of granularity between the controls and descriptions also varied significantly in terms of content and specificity (e.g., some controls were very specific and descriptive, while others were very high level and generic).

Methodological considerations

1. One of the design principles was for the ORX Reference Control Library to be primarily anchored in ORX member data and to be representative, therefore, of industry practices. For a small number of less mature risk types (e.g., Model Risk), expert judgement was also used to supplement the controls.
2. Since the use of NLP can potentially lead to false positives (e.g., artificially mapping a control to a risk that it was not designed to address), we conducted expert reviews of all resulting controls to address these instances.
3. Manual mapping of the controls to the L1 and L2 risks of the ORX Event Type Reference Taxonomy was also performed through expert judgement since the majority of the controls provided by member institutions did not have any specific risk mapping structure.
4. Where available, industry standards (e.g., NIST for Cyber Risk and COBIT Technology controls) were used to support the review of the libraries.
5. Certain controls are used to mitigate multiple risk types. In general, we found that this can vary depending on each organisation's individual risk taxonomy and governance structure. Where possible, we have tried to limit overlap by ensuring that each control within each library has the relevant specificities for the risk type. This is particularly the case for many controls within the Information Security library. In some instances, controls that mitigate more than one level 2 risk have been duplicated in those additional subcategories to ensure that the adequate controls are present for each sub-risk. An example of this is Customer Due Diligence controls, which are used to mitigate Financial Crime and Fraud Risks.

Considerations for refresh

ORX will seek feedback from members on the library and will evaluate the need to update it in the future. We are conscious that the business environment is continuing to evolve at pace and organisations report that they are currently developing or enhancing libraries. Both factors may support the need for future iterations based on enhanced member data.

As a result, the following non-exhaustive list of considerations will result in a review and potential enhancement of the ORX Reference Control Library to ensure that it remains a relevant guide for all members across the industry.

Types of considerations include:

- A number of member organisations submitting a new set of control data that vary materially from the existing set
- Evolving industry practices or regulatory expectations resulting in an increased focus on newer types of controls to manage risks associated with new technology, software, and products (e.g., digital assets)
- Industry practices changing significantly in how risks are mitigated (e.g., organisations shifting to automated controls or those using artificial intelligence)
- Significant enhancements in NLP technology leading to more sophisticated and more comprehensive initial risk mapping

General and specific control observations on level 1 risk types

Below are some general and risk specific observations that arose in the process of developing the library, along with explanations setting out how we have approached them.

General observations

Some controls mitigate more than one risk type

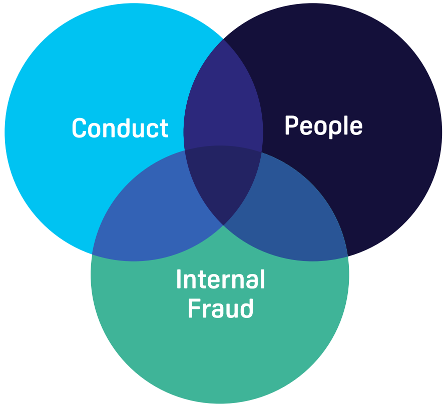
A recurring observation throughout the build of the ORX Reference Control Library was that some controls can mitigate more than one type of risk. A prime example of this is Information Security Risk, where individual controls often mitigate more than one level 2 risk type. Where the controls are identical, they are shown in the following ways:

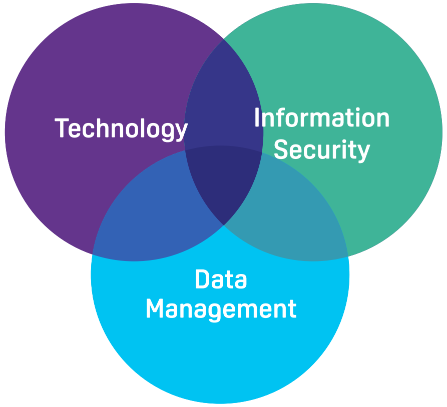
In the digital explorer – The digital explorer, available on the ORX members' website, enables these controls to be more easily shown against each applicable level 2 risk.

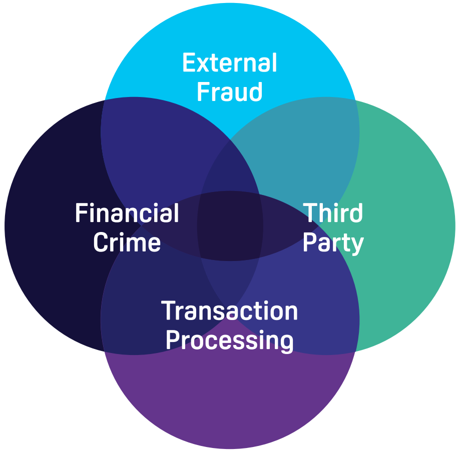
In the Excel spreadsheet – These controls are shown once, usually against the most applicable level 2 risk type. Other applicable level 2 risk types that the controls mitigate are shown in the column entitled 'Other applicable ORX Ref Taxonomy - Risk L2'.

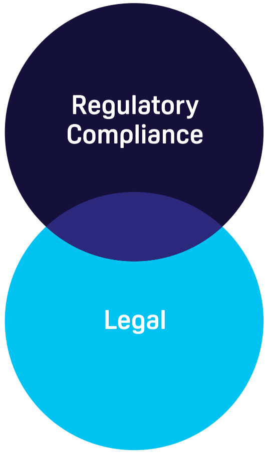
Institutions' mappings of controls to risk types vary depending on their internal risk taxonomy

As institutions' risk taxonomies and control mappings vary, it is advisable to consider certain L1 risk types in groupings. For example, if reviewing Conduct risk controls in the library, it is also worth considering certain other risk type controls that are closely related – in this case, People risk and Internal Fraud risk controls. Doing so should provide a more holistic view. The diagrams below suggest some key risk type groupings where there may be benefit in considering the library controls more holistically.









Control themes

Another lens through which to view controls is control themes, which were identified to support the use of the library. The control themes identified are as follows: change management, conduct and behaviour management, employee management, encryption, incident management, regulation management and third-party management. These are all control themes that span multiple risk types and are often managed within an institution by 1LOD and/or 2LOD teams/functions who may find this a useful lens to view controls.

Definition of a control and what's included

Organisations have different approaches to defining control libraries.

Example 1: Many include policies and training as specific controls, while some do not allow these to be included (based on the rationale that having a policy or training in itself, without other controls, will not prevent an adverse event from happening).

Example 2: Some controls in the library relate to the "establishment of roles and responsibilities". While different institutions will have varying views on the inclusion of such types of controls, our view is that clarity around roles and responsibilities is key for the effective management of all risk types and therefore should be included in the library.

Given the member data collected, the ORX Reference Control Library includes specific controls relating to policies and training and the establishment of roles and responsibilities.

Specific risk-based observations

People

Some controls in the People risk section focus on conduct and behaviour management, employee due diligence, and employee safety, and therefore overlap with other risk categories such as Conduct, Internal Fraud, and Physical Security and Safety. Typically, controls were mapped to the most relevant library based on the specificity of their descriptions, although other similar controls are present in other risk categories.

External fraud

Some controls in the External Fraud categories (e.g., fraud risk profiling, fraud risk scoring, etc.) are critical for identifying potential fraud occurrences across all types of external fraud risks and therefore apply to all three level 2 risks, i.e., (i) Third party/vendor fraud, (ii) Agent/broker/intermediary fraud, and (iii) First party fraud. As such, they have been duplicated across each section to ensure that the library is comprehensive and reflects industry practice.

In addition, some controls across the External Fraud library refer to due diligence. Due diligence controls overlap across a number of different risk types including Internal Fraud and Third Party/Vendor Fraud. In general, we have sought to ensure that each control description in each risk library is specific to address the risk type that it is mapped to. However, there are some overlaps in cases where the same control addresses and mitigates more than one risk type in its description.

Specific risk-based observations (cont)

Internal fraud

The Internal Fraud risk section has two level 2 risks: (i) Internal fraud committed against the organisation and (ii) Internal fraud committed against customers/clients, or third/fourth parties. Although the two types of risk appear similar, the target is fundamentally different (i.e., an employee stealing from the organisation itself vs. an employee stealing from the organisation's customers). Therefore, controls are considered individually for each type of risk. As a result, some controls across Internal Fraud that are relevant to both level 2 risks were duplicated across each section to ensure that the library is comprehensive and reflects industry practice.

In a similar way to the External Fraud section, some of the controls under Internal Fraud also refer to due diligence since they are an important part of a comprehensive suite of controls for fraud risk. Another library with which Internal Fraud controls intersect is Conduct.

Physical Security & Safety

In a similar way to the People risk section, several controls in the Physical Security and Safety library relate to employee safety. Therefore, similar controls are found in both risk sections.

Business Continuity

Some controls in the Business Continuity library refer to business continuity plans (BCP) and others to disaster recovery plans (DRP). Although they may appear similar, BCP and DRP are distinct activities and require different sets of testing and controls to be in place. Business continuity planning focuses on continuing operations in the event of a disruption, while disaster recovery planning focuses specifically on the restoration of functionality in critical technology. Therefore, relevant controls such as BCP resilience testing are duplicated across this library to address DRP resilience testing individually. Some controls also address service continuity plans (SCP), which is a subset of BCP that focuses specifically on the immediate-to-long-term action taken to minimise impact to customers in the event of a disruption.

Transaction Processing and Execution

Given that every financial institution processes transactions in their own unique way, several controls within the Transaction Processing and Execution category were either extremely specific to a particular institution or very generic and not sufficiently informative. As such, and with the support of experts, a number of refinements were made to synthesise and standardise the control descriptions in this section.

Specific risk-based observations (cont)

Technology

Technology risk overlaps with Information Security risk, particularly in areas such as inventory management and endpoint protection. In most cases, controls were mapped to one risk type based on the specificity of the control description and how it matches to the ORX Event Type Reference Taxonomy description.

Conduct

Conduct risk includes 12 level 2 risks in the ORX Event Type Reference Taxonomy. As a result, there may be some repetition between controls assigned to those sub-risks, especially within the high-level groups of Conduct risk. For example, there is a level 2 risk relating to Pre-sales service failures and another on Post-sales service failures. While these are two different risk types, they involve similar mitigation strategies and controls. Therefore, some controls have been duplicated across multiple level 2 risks. In addition, by nature, Conduct can appear in other areas such as Regulatory Compliance.

Financial Crime

In a similar way to the External and Internal Fraud sections, some of the controls under Financial Crime also refer to due diligence since these are an important part of a comprehensive suite of controls for Financial Crime risk.

Legal

Legal risk overlaps with Regulatory Compliance risk, particularly in areas where the risk arises from a failure to appropriately account for a change in laws or regulations. Controls to manage this type of risk are relevant to both risk types and were therefore included in both libraries given that failures in regulatory compliance can create significant legal issues.

Regulatory Compliance

In refining the Regulatory Compliance library, we decided to exclude any controls relating to specific regulations (e.g., Volcker). While some of these controls were included in the input libraries received from participating institutions, they were viewed as being potentially uninformative given the variation in such regulations across industries and geographies. A small number of controls mapped to Regulatory Compliance risk have some degree of overlap with other risk types such as Conduct. Therefore, in such cases, we have included overlapping risk controls in both libraries to be comprehensive.

Statutory Reporting and Tax

Given that financial reporting is subject to a significant amount of regulation and scrutiny, the Statutory Reporting and Tax risk theme is a dense control section compared to some of the other operational risks. In building out this library, we relied heavily on expert input, and we also compared and supplemented the controls based on the Committee of Sponsoring Organizations (COSO) reporting framework.

Specific risk-based observations (cont)

Third Party

In addition to the existing controls mapped to Third Party risk, the latest US interagency guidance on third party relationships was used to fill perceived gaps and cover the end-to-end third-party lifecycle (**Federal Register: Proposed Interagency Guidance on Third-Party Relationships: Risk Management**).

A small number of controls mapped to Third Party risk have some degree of overlap with other risk types such as External Fraud and Data Management. Therefore, in such cases, we have included overlapping risk controls in both libraries to ensure comprehensiveness.

Model

In the initial development of the library for this risk, there were very few controls tagged to Model risk. This is consistent with the survey results, which suggested that firms were planning to build out their libraries for Model risk.

While Model risk is not a new type of risk, increasing levels of complexity and sophistication in the type of models employed (e.g., machine learning) in recent years have led to firms paying more attention to Model risk. Here, we relied more heavily on expert input and on the Supervisory Guidance on Model Risk Management issued by the Federal Reserve to build out the library more extensively.

Information Security (incl. cyber)

Most of the Information Security controls can be mapped to more than one ORX level 2 risk. For example, a level 2 control such as "Control of information transfer" could be mapped to Data theft/ malicious manipulation of data, Data loss, and Data privacy breach/confidentiality mismanagement. Given this, we mapped each control to the "best" ORX level 2 risk (based on ORX's risk descriptions) as well as to the other ORX level 2 risks to which they are applicable.

In addition, we mapped the existing controls against the National Institute of Standards and Technology (**NIST)** framework. When no match could be found on the existing list of controls against NIST's control framework, we added additional controls to the library to fill in the gaps and ensure that the library is comprehensive.

Data Management

The Data Management library includes many controls that overlap with other risk libraries, such as Information Security, Third Party, and Business Continuity (e.g., breach management, third party data quality management, user access management). As described in the general observations, the approach taken involved reviewing the specific control descriptions and ensuring that they address Data Management risk.

Managing risk together

ORX believes many heads are better than one. We're here to bring the best minds of the international operational risk community together.

By pooling our resources and by sharing ideas, information and experiences, we can learn how best to manage, understand and measure operational risk and become less vulnerable to losses. We work closely with over 100 member firms to develop a deeper understanding of the discipline and practical tools. We set the agenda, maintain industry standards, and garner fresh insights.

ORX is owned and controlled on an equal basis by its members.

For more information about ORX, visit our website at **www.orx.org**

Report contacts

Steve Bishop
Research and Information Director, ORX
steve.bishop@orx.org

Mike Constantinou
Research Consultant, ORX
mike.constantinou@orx.org

ORX Reference Control Library pricing

ORX members	Non-member
Free	Price on request

Disclaimer: This work is the property of ORX. ORX has prepared this document with care and attention. ORX does not accept responsibility for any errors or omissions. ORX does not warrant the accuracy of the advice, statement or recommendations in this document. ORX shall not be liable for any loss, expense, damage or claim arising from this document. The content of this document does not itself constitute a contractual agreement, and ORX accepts no obligation associated with this document except as expressly agreed in writing.

Please note the ORX Reference Control Library can only be used by members under the conditions set out in Section 29 (Confidentiality) of the **ORX Articles of Association** and by non-members in accordance with the **Terms and Conditions**. For the avoidance of doubt, commercial use of the ORX Control Library by consultants or other firms for any financial gain is not permitted without express permission from ORX and will incur a charge. ©ORX 2022

O.R.X

Managing risk together

orx.org