May 2022

O.R.X

ORX Reference Control Library

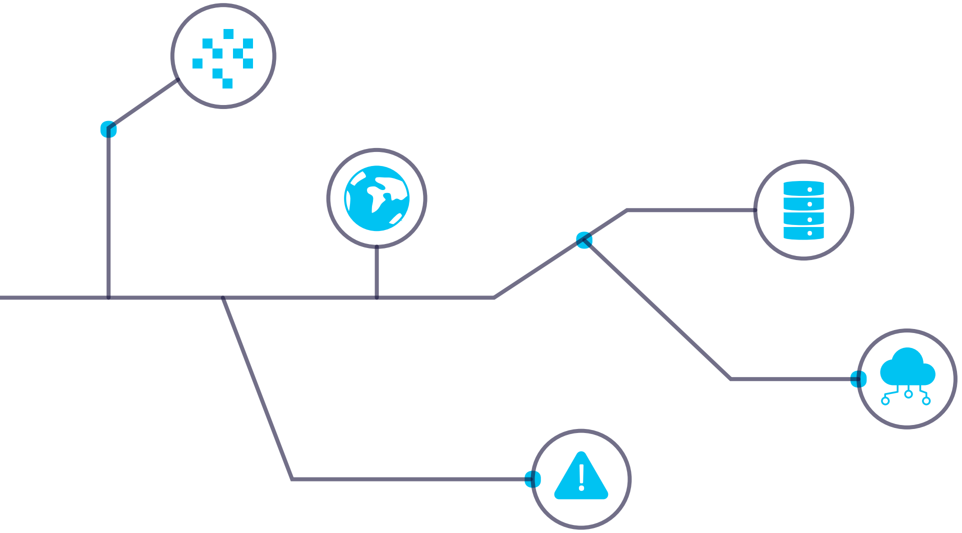
Developing an industry-leading library of controls for operational and non-financial risk

Managing risk together

orx.org

ORX, with McKinsey & Co. as a knowledge partner, has developed a Reference Control Library for operational and non-financial risk for the financial services industry.

Building on the success of the **ORX Reference Risk Taxonomy** and drawing on control data from nearly 50 banks and insurers, this is the most comprehensive global effort of its kind.



Access the ORX Reference Control Library

The ORX Reference Control Library is available to all ORX members. Visit **members.orx.org/orx-publications/orx-reference-control-library** to download the full library of over 750 controls, mapped to the ORX Reference Taxonomy.

To help you get the most from the library, we've provided a range of resources and ways to explore it. There's a downloadable spreadsheet you can use for your own analysis and a guidance document to help you understand the information and how best to use it.

We'll also shortly be releasing an interactive version which will allow you to explore the risk types and controls, help you identify linkages and delve into the different levels.

Explore the ORX Reference Control Library

Why develop the ORX Reference Control Library?

The financial services industry was already evolving at pace when coronavirus (Covid-19) both changed organisations' operating models and accelerated the race to digital.

This pace of change continues and provides both an opportunity and a need for operational and non-financial risk (ONFR) teams to step up and support the business as it transforms.

Most organisations are seeking to optimise their internal control environments to provide resilient services and to meet regulatory expectations in an efficient and cost-effective way. In recent years, control libraries have increasingly been used as an essential foundational tool to support control optimisation. They enable the standardisation and simplification of controls through setting expected control types for risks or processes, as well as streamlining control identification and assessment processes across a business.

Yet organisations looking to develop comprehensive and dynamic control libraries find that it is a particularly complex and time-consuming process. Furthermore, at an industry level, there is an overall lack of standardisation between organisations. These factors extend the time it takes for an organisation to develop a library and limit the potential to benchmark and share insights at an industry level.

Given this backdrop, ORX, with McKinsey & Co. as a knowledge partner, has developed the first ORX Reference Control Library for operational and non-financial risk in financial services.

The remainder of this document outlines the benefits of using the library, provides an overview of the library itself, explains how we went about constructing it, and describes the key observations that arose during its development.

How does the ORX Reference Control Library help?

Aligned to the ORX Reference Risk Taxonomy, the ORX Reference Control Library draws on control library data collected from nearly 50 banks and insurers (the majority of the data available from the membership).

The library provides a framework for the typical control types currently used by the industry today to mitigate each risk in the taxonomy. It can be used by organisations to:

- Review their internal control instances (or control library) against the typical control types in the reference library to support control optimisation activities
- Expedite the internal development of a control library, which can be both time consuming and complex, potentially using all or parts of the ORX Reference Library
- Gain insight into the relative importance of their controls in mitigating ONFR through future sharing and benchmarking of control information aligned to the library

We believe 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 currently used by a range of ORX members for each risk. It is informed by a wide range of financial services organisations across a variety of geographies and business lines (both banking and insurance). As a result, there will be various controls in the library that may not be applicable to every organisation.

It can be used in different ways

Given the thematic nature of some risks, it is possible to approach the library in different ways, adapting it to your business as required. Because of its origins in industry data, the library will provide a good guide to the typical controls to be considered. However, depending on your organisation's risk taxonomy, some controls may align to different risks, some may be less relevant, and, in some areas, you may wish to be more or less granular.

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 of these factors may support the need for future iterations based on enhanced member data.

The ORX Reference Control Library – what does it look like?

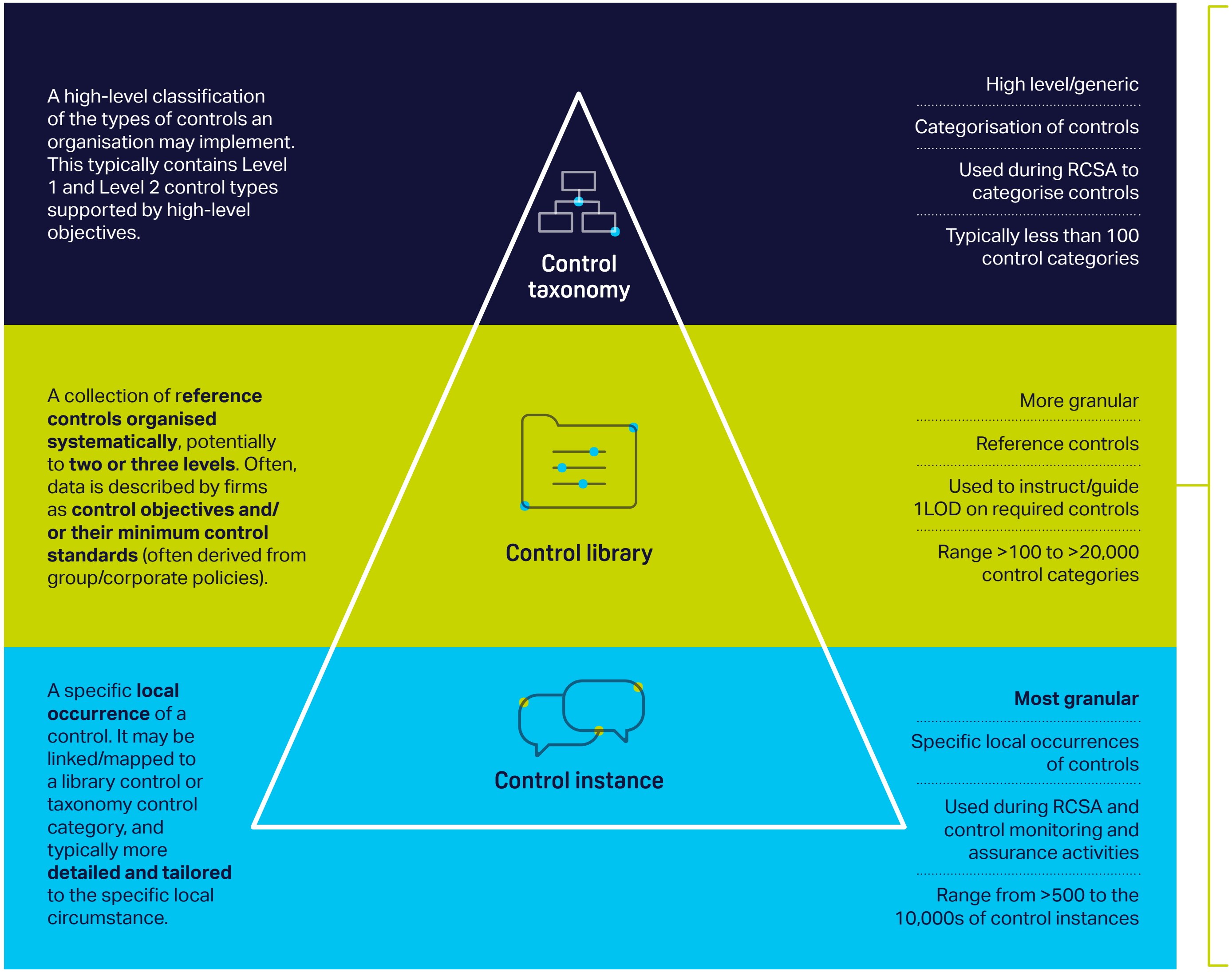
The ORX Reference Control Library in numbers:

Controls are aligned to the **16 level 1 ORX Reference Risk Taxonomy categories** and further split into **61 sub-level risk categories**

Includes **761 reference controls** (typical controls mitigating the risks)

Developed based on **~50,000 raw control taxonomy/library data entries** provided by nearly **50 of ORX's member institutions (both banks and insurers)**

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.

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).

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.

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

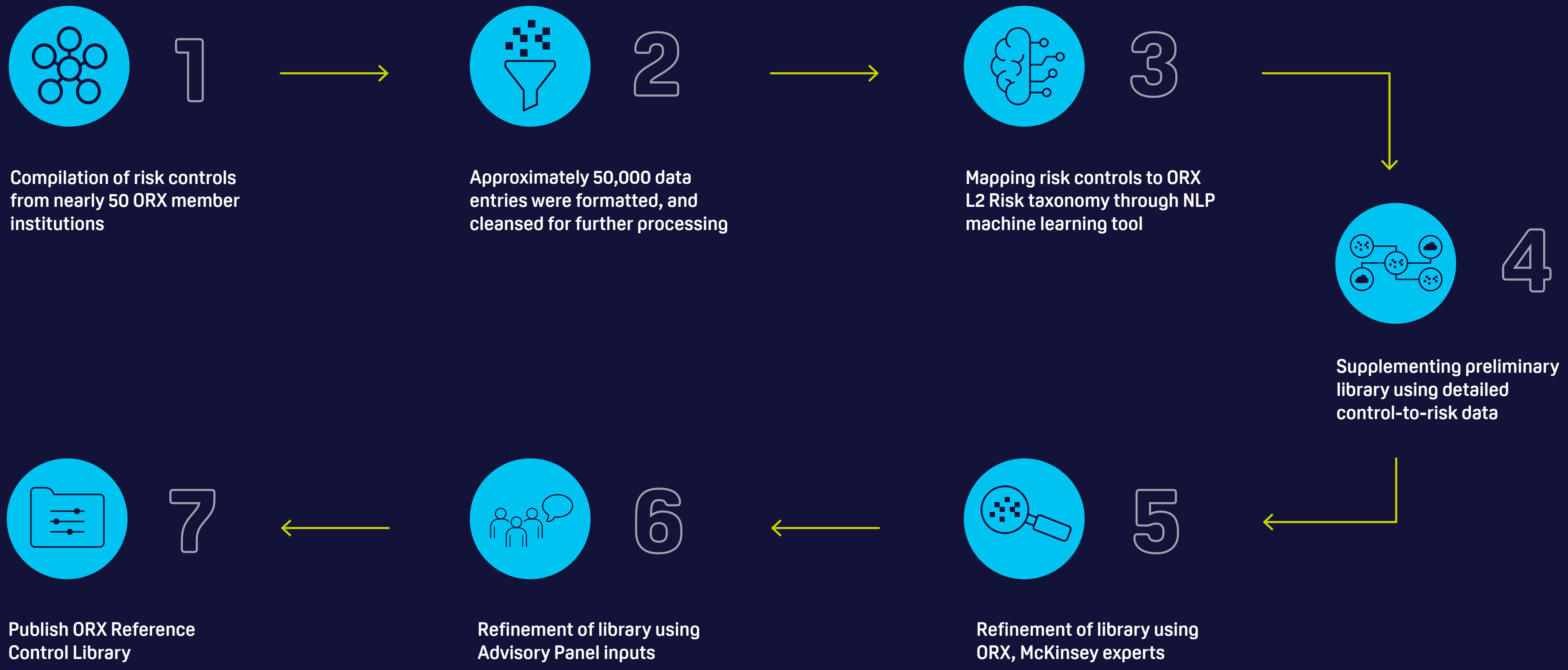
Snapshot of the library

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

Developing the ORX Reference Control Library – once again, data in the driving seat

As with the ORX Reference Risk Taxonomy, the control library is based on control taxonomy and library information from financial institutions. During 2021, we collected data from nearly 50 of our member institutions (banks and insurers).

How we developed the 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

Key observations on industry trends and practices

During the development of the ORX Reference Control Library, we were able to make a number of observations and identify a number of trends in the control taxonomy and library data collected from across the industry.

Some of these observations are also outlined in the following papers: 'ORX Reference Control Library Study – Initial Results Report' and 'ORX Controls Practices Paper – Control Optimisation, Monitoring & Testing, and Automation', both of which are available to ORX members **on the website**.

The use of control libraries is emerging as good practice, but they are challenging to develop

- Around 35% of financial organisations involved have developed a control library.
- A majority of other organisations see the potential benefits of, and have plans to develop, a control library.
- Control libraries are, however, challenging to develop and often involve both the 1LOD and 2LOD, with a majority taking 1-2 years to complete.
- There has been limited external input in the development of control libraries (with the exception of pockets of recognised standards such as COBIT for technology and NIST for cyber). As a result, practices can be questioned internally and by regulators.

As a result, practice is divergent

- Organisations have different approaches to defining control libraries. For example, 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 will not, by themselves and without other controls, prevent an adverse event from happening). The ORX Reference Control Library includes specific policies and training given the member data collected.
- The number of controls included in libraries ranges widely, from 100+ controls to 20,000+. The ORX Reference Control Library includes 761 controls, which is roughly in line with the median size of the libraries collected.
- The number of controls for each risk type in organisations' libraries also ranges widely.
  - For example, conduct risk is more established and advanced compared to some other risk types and, consequently, this is reflected in the volume of controls for this risk.
  - A small number of risk types were associated with fewer controls, such as model risk, where we have seen increasing levels of complexity and sophistication in recent years. While institutions have begun to pay more attention to this risk type, the associated control frameworks are not yet as well established as other types.

We also observed that the same or similar controls are used to mitigate multiple risk types

Another important observation is that 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 had the relevant specificities for the risk type.

This was 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. When using the ORX Reference Control Library, it is better for organisations to take a more holistic view of the risks and controls to ensure that key controls are not missed.

How to access the ORX Reference Control Library

The ORX Reference Control Library is available on the ORX member website. Members have access to:

- The full ORX Reference Control Library aligned to the ORX Reference Risk Taxonomy.
- The full guidance document providing general and specific guidance on the controls aligned to the various risk types.
- A digital visualisation of the ORX Reference Control Library through the ORX members' website (available by the end of Quarter 2 2022).

Visit the ORX Reference Control Library

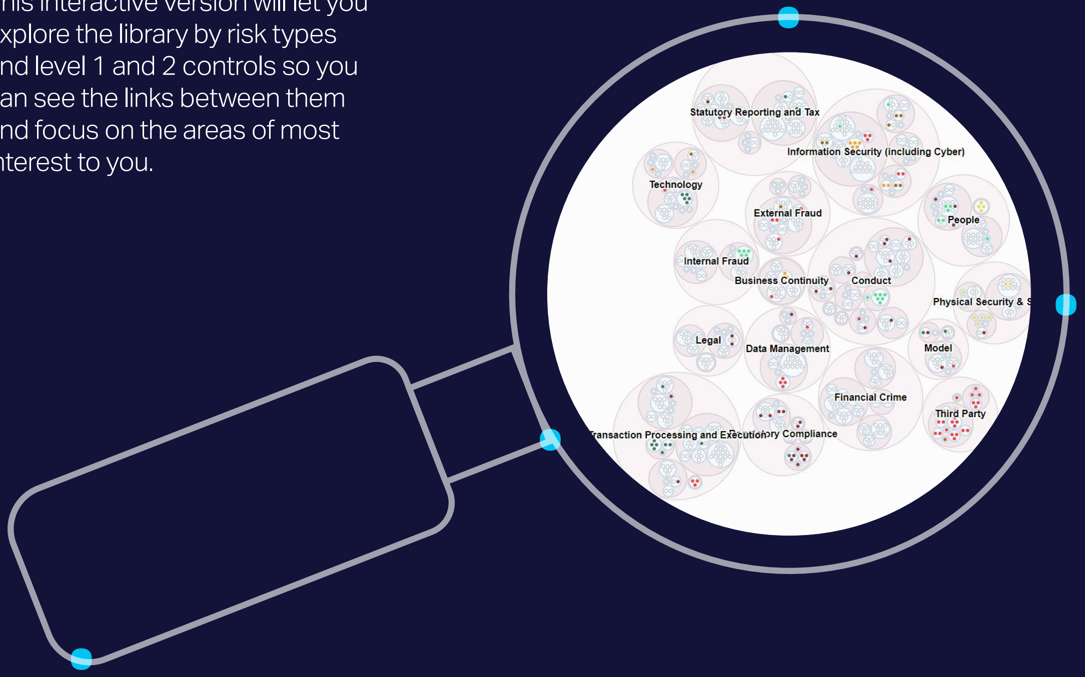
More on controls from ORX

Coming soon

ORX Reference Control Library Explorer

The ORX Reference Control Library Explorer, available to all ORX members on our website soon, will help you dig further into the detail of the ORX Reference Control Library.

This interactive version will let you explore the library by risk types and level 1 and 2 controls so you can see the links between them and focus on the areas of most interest to you.



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	£10,000

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.

O.R.X

Managing risk together

orx.org