ORX Reference Control Library Study – Initial Results Report

Leveraging the power of over 100 financial organisations to energise your operational risk management.

ORX report contacts:

Steve Bishop,
Head of Risk Management
Programmes & Insurance

Steve.Bishop@orx.org

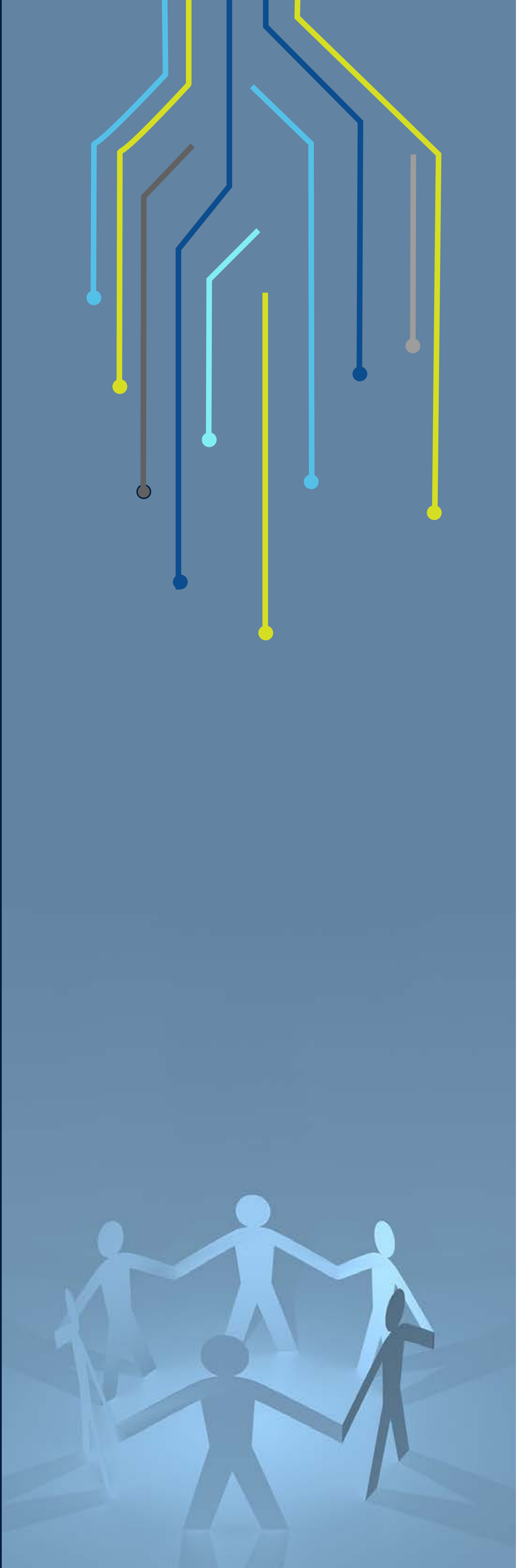
Mike Constantinou,
Consultant to ORX

Mike.Constantinou@orx.org

Follow ORX:

@ORX_Association
@ORX_Association

Visit: orx.org



Introduction

The focus on controls

The financial services industry is evolving at pace. The Covid-19 pandemic has both changed organisations' operating models and further accelerated the race to digital. Banks and insurers are changing significantly, managing multiple complex programmes and understanding how their future businesses will operate.

We stated in the recently published paper, Right time, right place, that industry change provides an opportunity for operational and non-financial risk (ONFR) to step up like never before and support the business as it goes through digital transformation. To do so will mean making ONFR resilient and enabling risk leaders to innovate how they serve the business and actively add value.

Core to this resilience is a well controlled organisation. Understanding and operating an efficient and effective control environment will enable a business to deliver change, optimise its resources and manage risks effectively, ultimately leading to the delivery of business objectives and results, as well as safeguarding stakeholders. ORX therefore firmly believes that an industry-led focus on controls and control practices is a strategic priority for the management of ONFR.

An industry-led strategic initiative

ORX is driving forward this industry focus on controls, initially progressing two key activities:

ORX Reference Control Library
Building on the success of the ORX Reference Taxonomy, and using data collected from nearly 50 members, we are working with McKinsey & Co as knowledge partners to develop an ORX Reference Control Library. This will be a set of controls organised systematically and aligned to the ORX Reference Taxonomy.

The library will reflect the most common control objectives or standards in place across the industry by risk and we aim to publish it, along with guidance, around the end of Q1 2022.

This reference library will help members to understand and benchmark their own controls against industry practice, as well as helping further their own thinking. We are also aiming for the library to support the future alignment of industry risk and control information and to help facilitate ORX information sharing and benchmarking activities.

Control practice
ORX will also provide a forum for the discussion and development of control practices, enabling members to share experience and enhance approaches.

This work has commenced with initial roundtables looking at the work to develop the ORX Reference Control Library and initial information gathered from members on control practices. Over the coming months we will explore further topics of interest, including control automation and monitoring.

The remainder of this report sets out the initial findings from the first survey on control library practices. These findings have been enriched with further key discussion points raised at the roundtables.

About this report

This report sets out the findings from our initial review of industry control practices, in particular the use of control taxonomies and libraries. It is based on responses from 63 member organisations and discussion at round tables held in October.

A direction of travel for the industry:

Although only around 35% of institutions currently have fully developed control libraries, it was clear from discussions at the roundtables that the majority of remaining institutions have a plan to develop one. It was acknowledged that it is a challenging exercise to complete, often taking significant time (1 year plus), but the benefits can be significant. Many participants said that the alignment of control expectations across the three lines of defence, improvements in control transparency and efficiency, and a better understanding of the overall organisational control environment outweighed the difficulties.

The work has highlighted that, in many cases, control libraries have been developed within institutions with limited external input (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.

It is hoped that the ORX Reference Control Library will guide the industry, providing a common industry control standard for ONFR.

Next steps:

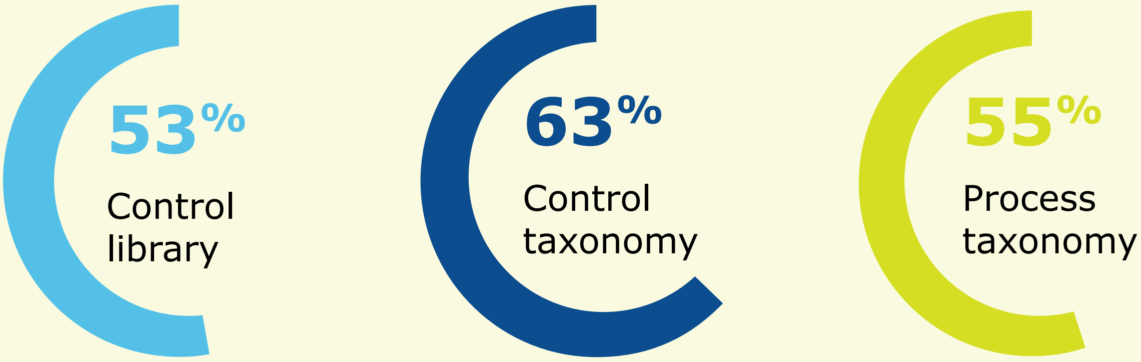
Following this initial report, ORX intends to publish the ORX Reference Control Library around the end of Q1 2022. In addition, we will hold a series of roundtables in the coming months designed to explore the control topic further. Member feedback has indicated that these will start with discussions around control automation and control monitoring.

Diversity of control definitions

As anticipated, there is a clear diversity in key definitions around controls across institutions. As a result, the review of the survey results has required thoughtful interpretation. As an example, there is a broad range of terms used within and between institutions with differing meanings, including for control, control library and control taxonomy.

For example, 53% of participants responded that they have what they consider to be a "control library", whereas by the ORX definition (provided on page 6) that percentage is actually closer to 35%.

% of respondents that have the following defined in their institution



Firms use varying language to describe their controls practice, resulting in differing interpretations of these terms.

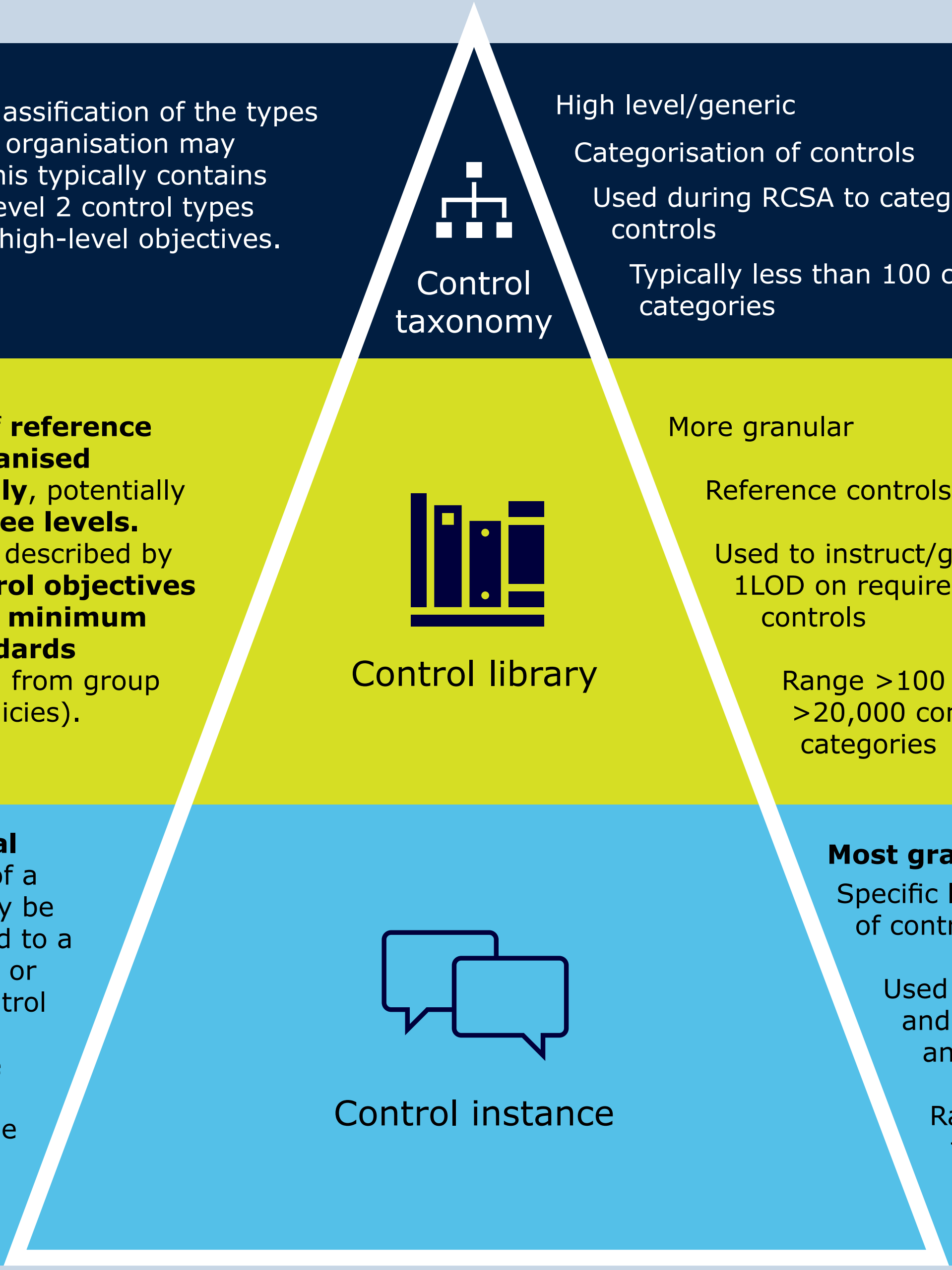
Diversity of control definitions (cont.)

We have therefore further refined the definitions ORX initially proposed to encourage consistency in understanding across the membership, in particular to provide clarity in what is being developed in the ORX Reference Control Library initiative.

The extended definitions are shown below and are further explained on page 7

Control taxonomy definition	Control library definition
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.	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).
Extension to definition Invariably used during first Line of Defence (1LOD) Risk and Control Self-assessment (RCSA) process to categorise/describe actual control instances operated. Helps the 1 and 2LOD review/challenge process, bucketing controls and helping to identify similarities/gaps in control type usage across business areas.	**Extension to definition** Used as the controls the 1LOD is expected to/could operate to mitigate a particular risk and/or business process. Often, 1LOD has a choice to adopt controls or justify/seek approval to use alternative controls. The controls would typically be assessed as part of the RCSA process. 2LOD often engage with the 1LOD to develop the control library.

Distinction between control taxonomy, library and instance



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

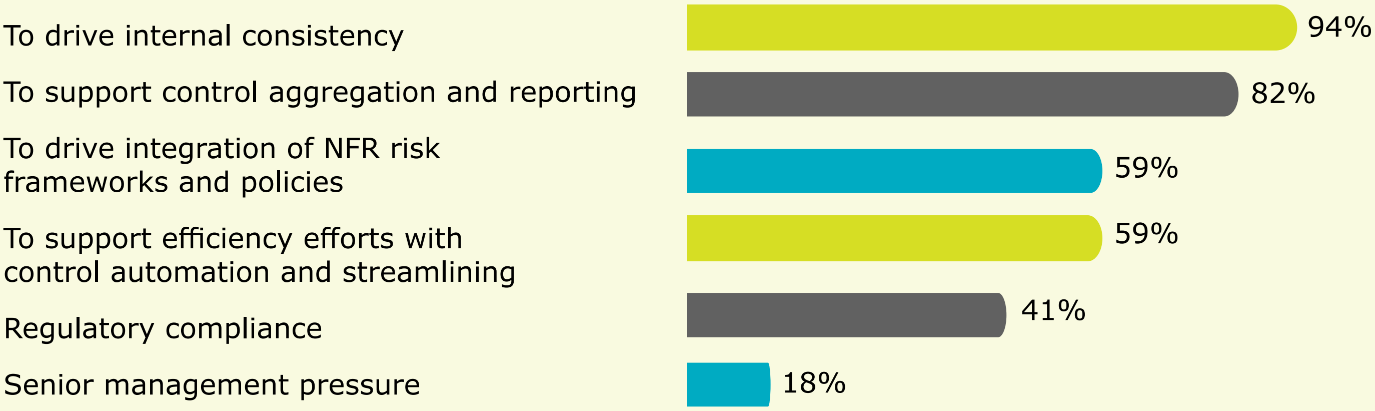
Used during RCSA and control monitoring and assurance activities

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

Key drivers and benefits of a control library

For institutions that have developed detailed control libraries (with over 100 controls), there were a number of key drivers behind this decision. The two most important reported were 'consistency in control identification and assessment' and that 'a library enhances control aggregation and reporting.'

What were the driving factor(s) behind the development of your control library? (> 100)



While the development of a control library can be challenging and a time commitment, the potential benefits are significant.

One institution remarked:

"The control library has provided structure in terms of how controls are discussed, reported and how risks are managed"

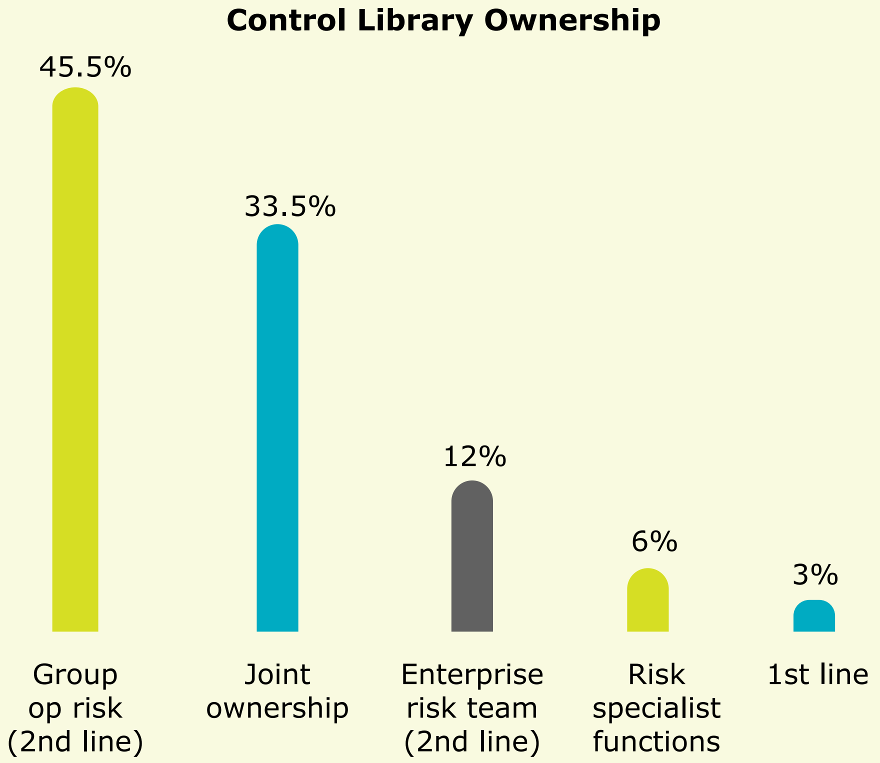
Further benefits included:

- Supporting the standardisation of controls implemented across the business, including an enhanced understanding of the minimum control standards and a removal of unnecessary/duplicative controls (particularly if controls are linked to corporate policies).
- Strengthening 1LOD ownership and 1LOD and 2LOD understanding of control requirements and controls in place.
- Simplifying control documentation and assessment requirements for the 1LOD.
- Providing an enhanced view of control effectiveness across businesses.
- Allowing effective comparison of controls and sharing of best practice.
- Facilitating greatly enhanced aggregation, analysis of control performance and reporting of risk and control information (at business and enterprise level).
- Enabling refinement of control assurance models that can then be used consistently across the 3LOD.

Approaches to control library ownership and development

The findings show that the group operational risk function acts as the control library owner in 46% of cases with joint ownership between the operational risk function and/or the 1LOD and/or risk specialist teams in 34% of cases.

There is often collaboration in the development of the control library content across the operational risk functions, risk specialist functions and the 1LOD.



Discussions at the member roundtables indicated that collaboration between the 1LOD and 2LOD can benefit both the development and use of a control library.

Members reported 1LOD and 2LOD collaboration in development is likely to:

- Improve the completeness and clarity of the controls defined
- Drive 1LOD buy-in to using the library
- Promote 1LOD understanding of the controls they are being asked to implement and assess

Approaches to control library ownership and development (cont.)

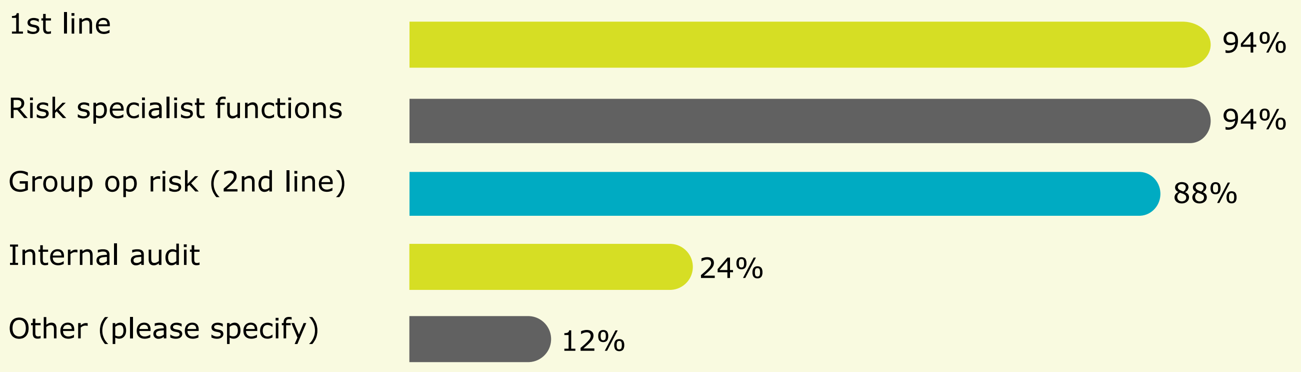
Discussions at the member roundtables indicated that collaboration between the 1LOD and 2LOD can benefit both the development and use of a control library.

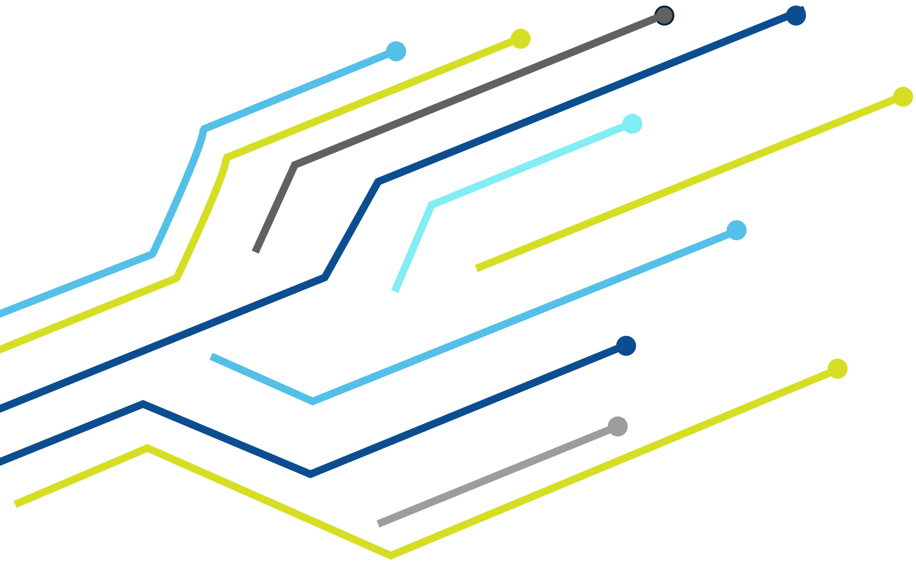
Members reported 1LOD and 2LOD collaboration in development is likely to:

- Improve the completeness and clarity of the controls defined
- Drive 1LOD buy-in to using the library
- Promote 1LOD understanding of the controls they are being asked to implement and assess

Control Library Development

Who was involved in identifying the controls in your library (> 100)





Approaches to usage

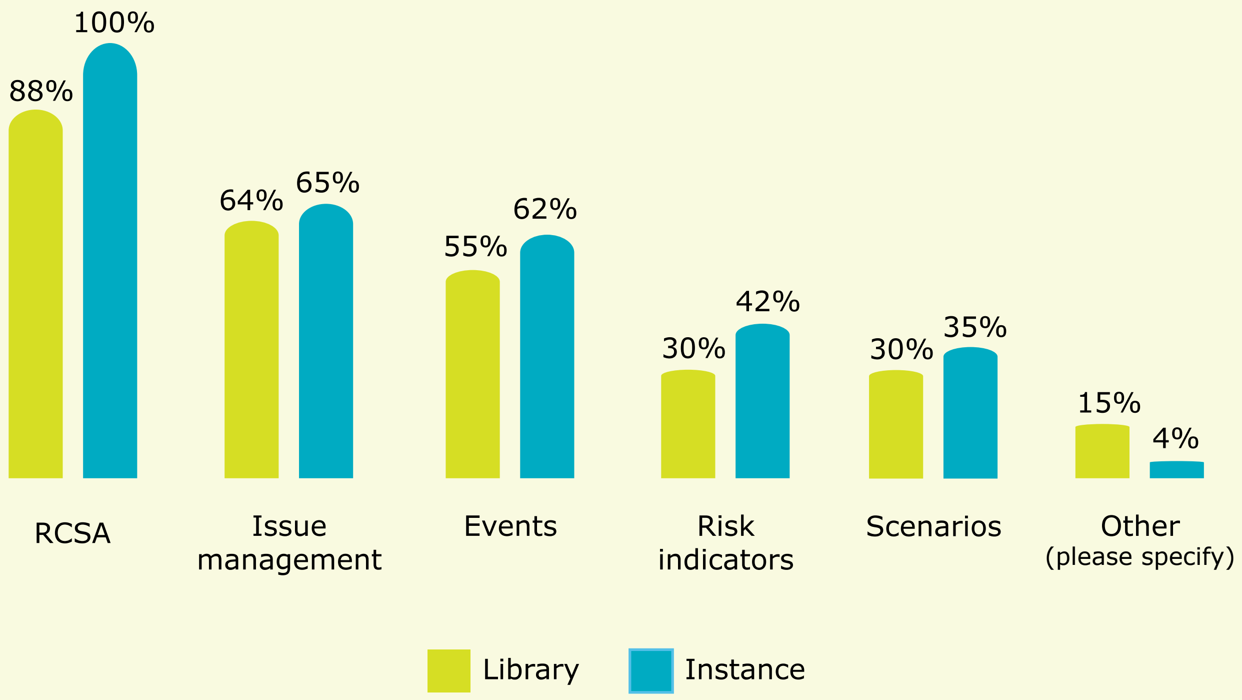
While many institutions would like their control library to be integrated and used across their operational risk framework (e.g. to link to risk events, scenarios etc.), the survey results indicated they are predominantly used as part of RCSAs.

However, when we refined this question further at the control library roundtable, to focus on controls instances, participants indicated that there is clearly a higher usage of/link to control instances in other operational risk framework elements. Discussions indicated that there is strong interest in leveraging control libraries and instances and linking these more across the risk framework, leading to a better understanding of the control environment status and effective risk management actions that should be taken.

One participant stated their aim is to have *"a control-led operational risk framework"*

Participants acknowledged that this is not easy though, e.g. given differing levels of control granularity that may need to be considered in an event vs. the RCSA. Given this, challenges and solutions for using control libraries and/or control instances across the operational risk framework elements will be further explored during the planned control library discussion groups over the coming months.

What operational risk framework components do you use your control library and instances in?



Time taken to develop control library and key challenges

It is clear from both the survey and the ensuing discussions that control libraries (with more than 100 controls) require a significant time investment, with the majority taking over 12 months to develop.

Many control libraries have been developed internally, often co-ordinated by the operational risk function. There also tends to be significant input from 2LOD risk function specialists (e.g., compliance, cyber etc.) and, in many cases, the 1LOD. There are a minority of cases where consultants have also been used to lead development.

ORX expects that the development of the Reference Control Library will help members to accelerate their thinking and help reduce the internal effort required.

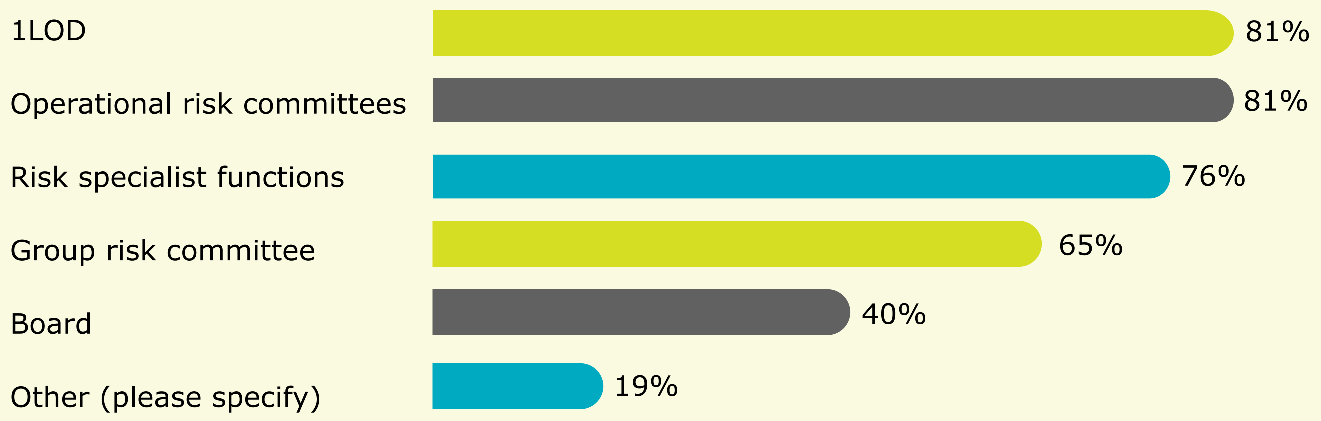
Key challenges in terms of control library development include:	Examples of solutions taken to address challenges include:
Securing 1LOD buy-in to the exercise and output	Involvement in or in a few cases ownership of content by the 1LOD
Clear articulation of the controls	Collaboration between operational risk, specialist risk functions and 1LOD
Deciding on the level of flexibility 1LOD has in deciding which controls to implement	Some control libraries focus on the control objectives (COs) and allow flexibility providing COs are met
Striking an appropriate balance between completeness and usability when deciding on granularity	Some control libraries focus on a concept of key controls
Meeting regulatory expectations particularly regarding comprehensiveness of controls	Regular dialogue with the regulator during the development phase
Effort required for ongoing maintenance of the control library, so it remains up-to-date	Periodic governance forum to agree where controls should be added or removed from the control library

Control reporting

In the survey, we also looked at how controls information is reported. Results indicate that over 80% of institutions report controls level data to 1LOD management and to operational risk committees. However, the number of institutions reporting control level information to group risk committee and to the Board drops to 65% and 40% respectively.

This level of reporting is notably less than for risk indicator information, which a recent ORX Risk Indicator and Culture Study found was reported in all cases to senior management and in over 80% of cases to the Board. Discussion suggested that this is a reflection of the granularity and scale of the control information and often a more summary level view is reported to senior committees.

Who is control assessment information reported to?



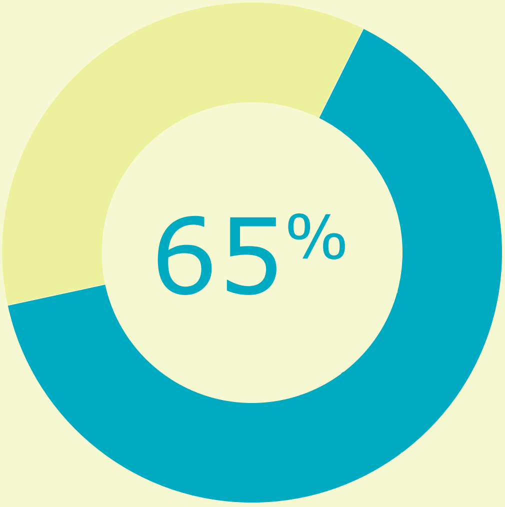
Institutions’ future plans

This initial work also examined plans for the future development of control libraries. Targeted areas include:

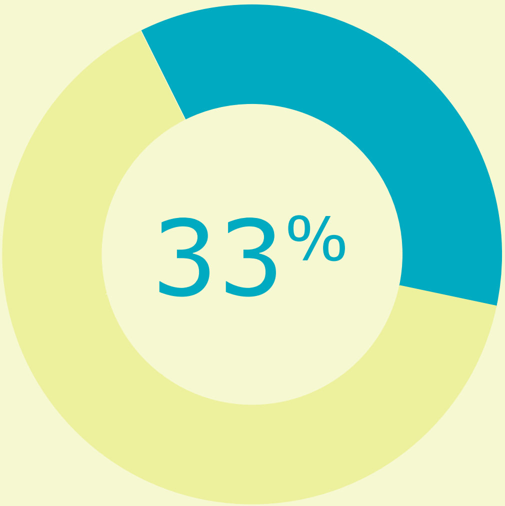
- Ensuring completeness of the control library, e.g. inclusion of missing, potentially more contemporary risk areas such as model.
- The linking of controls to processes.
- Alignment with Sox and Audit approaches.
- Enhancement of controls, particularly to make them more automated, and enhancement of control monitoring (including leveraging data).
- Consideration of the digital business model and control changes this may introduce.
- The semi-automation of the control library maintenance process.

As part of current digitalisation strategies, perhaps surprisingly, only a limited number of members reported plans to better automate existing controls, as well as introducing new controls to account for an increasingly digitalised operating environment (additional risks faced by firms, e.g. cyber).

Firms planning to enhance their Control Libraries



Firms stated their digitalisation strategy impacted their Control Library



Areas of further interest and next steps

At the October 2021 control library roundtable meetings, participants were asked about other areas of interest that might form the basis of future discussions. The areas identified are ranked here in order of preference with control automation and control monitoring and testing the most popular topics.

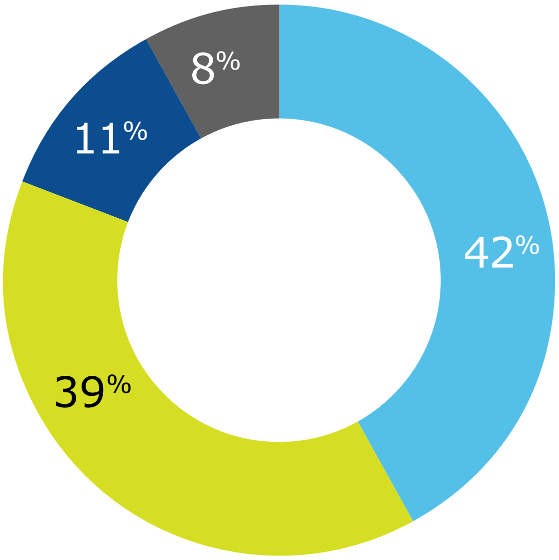
These were also two areas we asked about in the study, with results backing up the significant interest.

Rank	Area of further interest	% of firms interested
1	Control automation	77%
2	Control monitoring and testing	73%
3	Control integration across GRC	50%
4	Driving control efficiencies	50%
5	Latest control developments in digital business	45%

What are the levels of control automation?

Around four in ten institutions have automated under a third of their controls.

Control automation is stated to be a key next step with respect to controls development in the future.



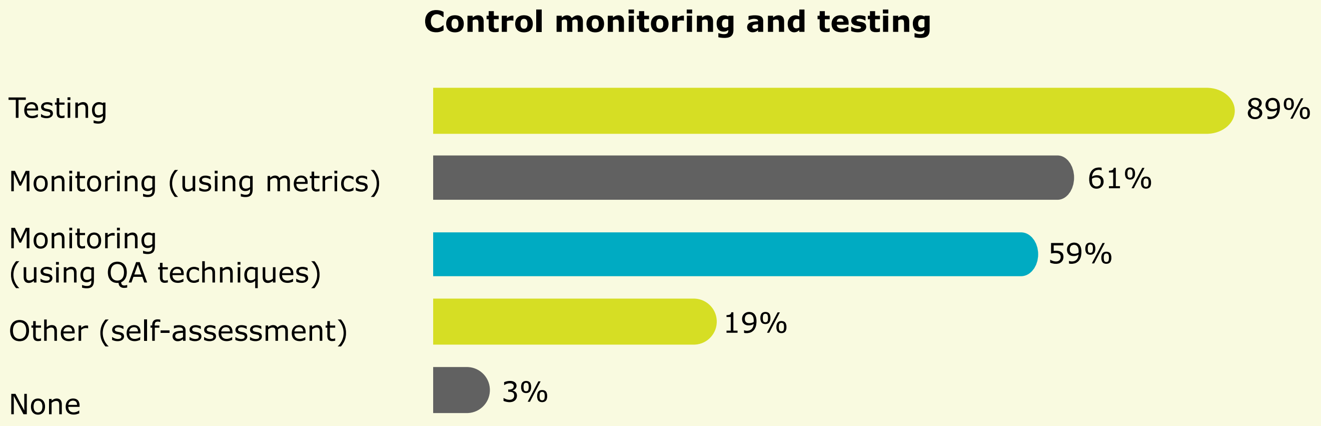
● Unknown

● 0 - 30%

● 51-80%

● 31-50%

Areas of further interest and next steps (cont.)



Results show a range of activities employed to monitor control design and effectiveness. We will explore further as part of future discussions on this topic.

ORX recognises the high level of interest in the controls topic and as a result will be running a series of deep dive discussion groups in the coming months.

These will focus on the topics identified above and will allow members to explore topics in more depth and share practice. To support this, ORX will provide a write-up of these discussions.

ORX Reference Control Library:

In addition, ORX and McKinsey & Co as knowledge partners, supported by an ORX memberadvisory panel, will continue to develop the ORX Reference Control Library. This work, in line with the methodology presented, will continue over the remainder of 2021 and Q1 2022. The intention is to publish the full Reference Control Library and guidance by end Q1 2022.

The discussion groups and the ORX Reference Control Library will be available to all members.

in @ORX_Association @ORX_Association Visit www.orx.org