ORX Controls Practices Paper – Control Optimisation, Monitoring & Testing, and Automation

Purpose

This paper sets out current industry practice, progress, and views on control optimisation, monitoring and testing, and automation. The paper draws on input from members in two dedicated topic-based roundtables, the results of roundtable polling, and survey responses gathered in 2021 as part of the ORX Reference Control Library project.

We would like to take this opportunity to thank members for their contributions during the roundtable meetings, particularly those who presented.

ORX contacts:

Steve Bishop,
Research and Information Director
research@orx.org

Mike Constantinou,
Consultant to ORX
Mike.Constantinou@orx.org

Follow ORX:

@ORX_Association
@ORX_Association

Visit: orx.org

Introduction

Most Financial Services (FS) organisations are seeking to optimise their internal controls to support resilient services, satisfy regulatory expectations, and meet the challenges of digitalisation in an efficient and cost-effective way.

However, the reality for most is that there has been a continued overall increase in the level of controls over the last three years.

The roundtable discussions revealed the following key reasons for this increase:

- A continued growth in regulatory expectations around controls for a range of risk types, including cyber, resilience, data management, and ESG.
- The need to address identified control weaknesses.
- Limited progress made in the automation of controls.
- Challenges in effectively using risk indicators as a more cost-effective method of control monitoring/assurance.

This paper summarises discussions about the nature of these challenges, provides examples of where FS organisations have made progress, and suggests ways to optimise your controls practice.

8 ways to optimise your controls practice

1. Clearly define what a control is (and is not) and be precise on the scope of your control inventory.
2. Prioritise management attention and resources onto KEY control management, ensuring this is embraced in business practice and the controls operated.
3. Identify opportunities for control automation where there is a specific business driver for automation, supported by the right skills, tools and people.
4. Consider automating your controls assurance process to drive objectivity, reduce manual effort, and report timely information.
5. Develop a Control Library to support control standardisation, rationalisation of controls and clear ownership, and where possible use industry control standards.
6. Centralise your controls governance and sharing processes to support the effective and efficient operation of shared controls.
7. Use indicators to monitor control optimisation activity.
8. Implement a combined assurance plan to ensure co-ordinated and efficient monitoring and testing of controls across the three lines of defence.

Factors driving the increase in the overall level of controls

In a roundtable poll,

71%

of FS organisations considered that the level of internal controls had increased,

with only

11%

reporting a reduction

and

11%

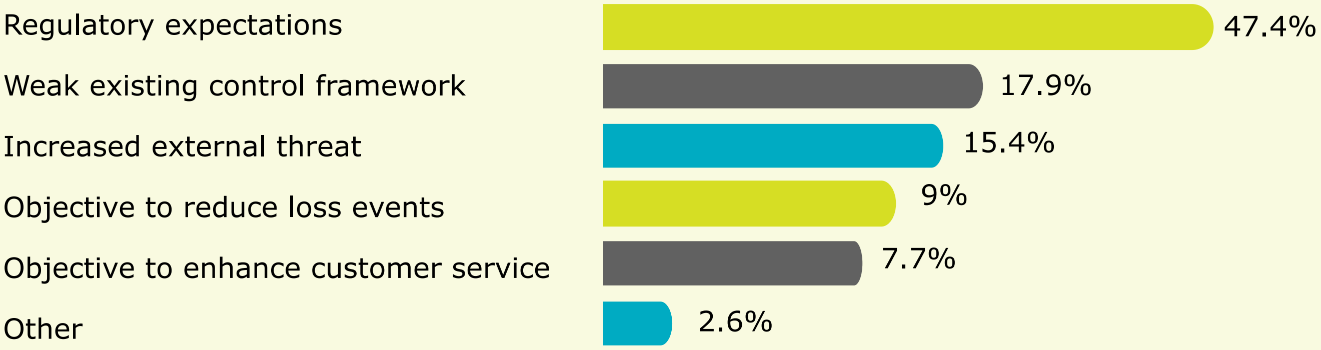
reporting that they have remained at the same level.

Almost half the FS Organisations polled responded that satisfying regulatory expectations is a key driver of the continued layering of additional controls. Subsequent discussions revealed that this was the case across most jurisdictions. Examples of increased regulation included Operational Resilience and ESG.

Remediation of weak controls (18%) and addressing increased external threat (15%), e.g. cyber-attacks, are the next highest drivers of the overall increase in controls.

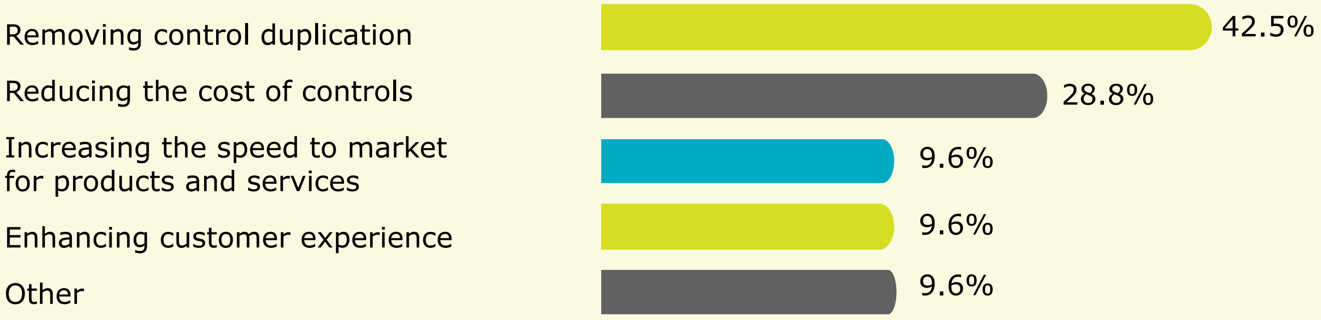
The factors driving the volume of controls, both upwards and downwards, were explored, yielding the following results:

Regulatory expectations are widely believed to be the main upward pressures on the level of controls.



Initiatives targeting the removal of control duplication are the largest downward driver of the level of controls. FS organisations that have developed Control Libraries with standardised controls have been particularly successful in removing duplicative/superfluous controls.

FS organisations report that a number of pressures are driving a reduction in the volume of controls



There are a range of practices being used to support control optimisation

Redefining a control and the focus on key controls

Definition of a control

Following a review of FS organisations' definitions of the concept of control, the ORX study 'Understanding Control Management Practices (2017)' developed a broad definition of a control as 'an activity designed to prevent or mitigate the impact and/or the likelihood of a risk.'

O.R.X

Understanding control management practices

September 2017

Managing risk together

www.orx.org

During 2022 roundtable discussions and the development of the ORX Reference Control Library, there has been continued debate over what is an appropriate definition of a control. In particular, discussion has centred around whether governance, policies, training and processes are in fact controls or simply sound risk management procedures for organisations to have in place. There are two broad ways of thinking about this:

- FS organisations that believe these are relevant to include in a control inventory and monitor along with other controls, citing examples such as sales training, which may be a regulatory requirement.
- FS organisations that believe these are not controls, or at least not key controls, and report that they have benefited from adopting a narrower definition of a control that prioritises management focus on key controls. Although not controls per se, these items are considered to be mitigants and therefore are part of a control environment.

Focus on key controls

Many FS organisations, irrespective of their definition of a control, have been focusing on refining their control inventories to 'key' or 'primary' controls.

The determination of a key control is often defined by:

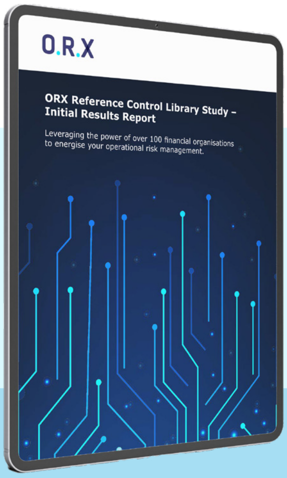
- Its linkage to the materiality of the risk(s) it is mitigating, and/or
- The Risk Function specialist who defines key controls in policy, and/or
- Its inclusion in the Control Library, which is often developed in collaboration between the 1LOD and 2LOD.

This not only reduces the overall effort involved in the Risk and Control Self-Assessment (RCSA) exercise and monitoring and assurance of controls but also frees up time to focus on the risks and controls that truly matter.

However, some FS organisations reported that even when controls are reduced in the Control Library, Policies and/or RCSA process, 1LOD management may continue to operate them. Therefore, for real control rationalisation to take place, there must be a change to the business culture and controls in use and not simply a change in the risk management system. Ensuring that this action takes place is one way in which risk teams can add value to the business.

Control automation

Control automation provides potential benefits to FS organisations – in particular, greater reliability and capacity for increased frequency of the control and at a lower cost in the longer term.

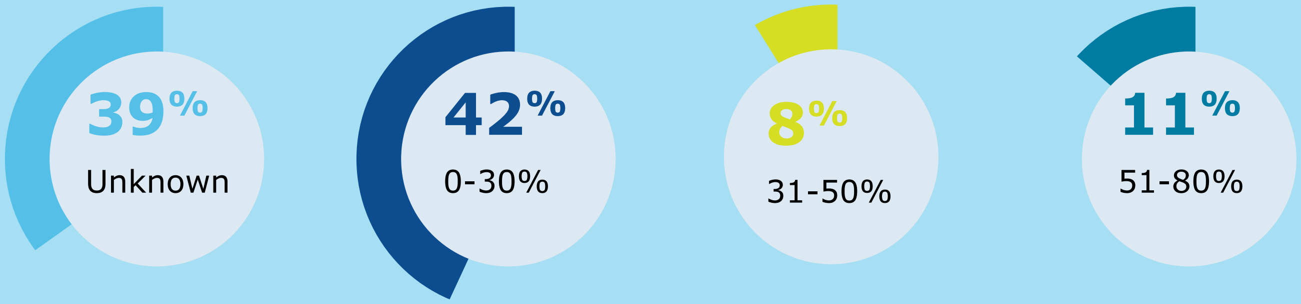


O.R.X

ORX Reference Control Library Study – Initial Results Report

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

The current level of control automation is low in most FS organisations, as revealed by the **ORX Reference Library Control Study** results shown below in which participants were asked to estimate the percentage of automated controls within their organisation.



There are a number of barriers that have limited the adoption of control automation.

ORX members shared the following key challenges:

- The cost benefits of control automation are often not realised in the short term, whereas 1LOD management have short-term profit and cost targets. Automation is often therefore not prioritised by 1LOD management.
- 1LOD can be reluctant to invest in control automation where manual controls are operating effectively or where there is anticipated future process change, e.g., due to digitalisation.
- Certain types of controls do not inherently lend themselves to automation or automating them is too complex/costly. One institution estimated that only around 40% of controls could be automated.
- Lack of standardisation across a FS organisation’s control framework.
- Shortage of internal skills and/or tools to automate.

Discussion at the ORX roundtables revealed that the key to successful control automation is the need for a business driver, the right risk people involved at the right stage, the right skills to implement automation, and the right tools to monitor the outcome of automation. For example, one institution explained that it 'piggybacks' on 1LOD process re-engineering activity since this is the ideal opportunity to automate key controls and monitoring as part of wider digitalisation efforts.

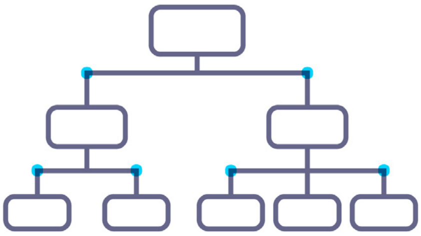
There are also variations in how FS organisations are approaching control automation.

One key approach that is being increasingly used is Bots/Robotic Process Automation (RPA) for automation of certain types of controls, and this can also be used for control monitoring and testing.

Another approach is the use of data lakes designed to centralise information and allow for the execution of automatic controls and control monitoring, although this is considered to be a slightly more challenging process.

Most firms are planning to move towards a more automated control environment

90% of FS organisations polled stated that they had plans to increase control automation.



Automation of the control testing or attestation process

Some FS organisations are automating the control testing or attestation process. One FS organisation explained that since they had experienced challenges with the speed of control automation, they were focussing their efforts instead on piloting an automated attestation process.

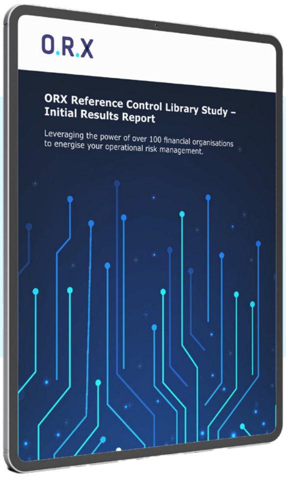
The stated benefits of automating control assurance are that it:

- Provides an objective process using, where possible, existing data to evidence control effectiveness.
- Supplies 1LOD management with more frequent information and, in some cases, also supports capacity planning.
- Reduces the manual effort around testing.
- Can be used for all types of control (automated, semi-automated or manual).

This control attestation process can be applied to any control providing there is sufficient availability of data. The process can automate control effectiveness assessments, although control design assessment still needs to be an additional manual process. In this example, a control monitoring dashboard has been linked to the GRC system.

Control libraries

In recent years, Control Libraries have increasingly been used as a tool to support control optimisation by enabling the standardisation, delayering and clear ownership of internal controls.



O.R.X

ORX Reference Control Library Study – Initial Results Report

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

Around 35% of FS organisations have developed a Control Library, as reported in the ORX reference control library – initial results report (2021)

A majority of other FS organisations see the potential benefits of doing so and have plans to develop a Control Library. Developing a Control Library is a challenging process often involving both the 1LOD and the 2LOD, with most taking 1-2 years to complete. Many participants stated 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 development of an ORX Control Library is expected to assist FS organisations to:

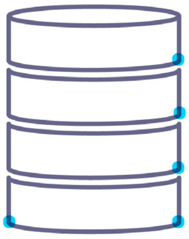
- Benchmark their internal controls and support control optimisation activities within their organisation.
- Accelerate the internal development of control libraries, which can be both time consuming and complex to develop.
- Provide insight into the relative importance of their controls in mitigating ONFR through future linkage of FS organisations' data, such as ORX Scenarios and/or Losses.

Control governance and control sharing

Centralised governance and sharing of controls are areas that many FS organisations are also increasingly focusing on to support optimisation practices.

For example, one FS organisation has established a gatekeeper function with a monthly 'change council' meeting, with all new key controls having to go through the council for approval. This was described as a necessary but onerous process.

Another FS organisation highlighted their approach based on a 'Control Marketplace'. This involves a centralised database within their Governance, Risk Management and Compliance (GRC) system that is used by control owners across the group to advertise their controls and allows business owners to select controls relevant to their business area. The control owner operates the control on behalf of multiple business areas providing regular control information to the risk owner(s). The arrangements made between risk owners and control owners are currently informal, but the process is expected to be formalised, with records of their interactions being retained and evidenced in the system.



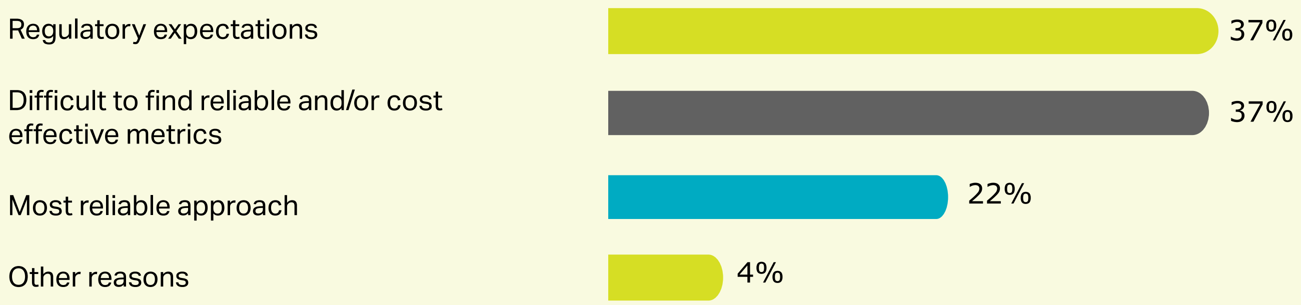
Control optimisation indicators

A number of FS organisations are using control indicators to support control optimisation. One FS organisation reported that senior management sponsor control optimisation and monitor control optimisation measures with explicit targets that are compared to external industry benchmarking information. The metrics focus on areas such as control sharing, control automation, control effectiveness, and the balance of preventative to detective controls.

Testing remains the dominant method of monitoring control effectiveness

Despite the efforts of many FS organisations to reduce their reliance on control testing, which is both manually intensive and costly, testing remains the dominant method of monitoring control effectiveness. Control testing may take the form of an interview or discussion at a workshop, particularly if this relates to design effectiveness. Testing is increasingly evidenced-based for operating effectiveness testing. A small number of FS organisations have also started to use BOTs for testing purposes where sufficient data is available and organized in a way that makes this possible.

Testing remains the most common approach used by firms for several reasons



There are three key interlinked drivers behind the continued reliance on testing:

- A regulatory expectation that testing is undertaken.
- Alternative forms of control monitoring such as the use of control indicators have proved a challenge for most FS organisations. ORX's Risk Indicators and Culture Pilot Study report provides a summary of these ongoing challenges.
- Testing is often considered by FS organisations to be the most reliable approach.

July 2021

O.R.X

Risk Indicators and Culture

A pilot study from ORX

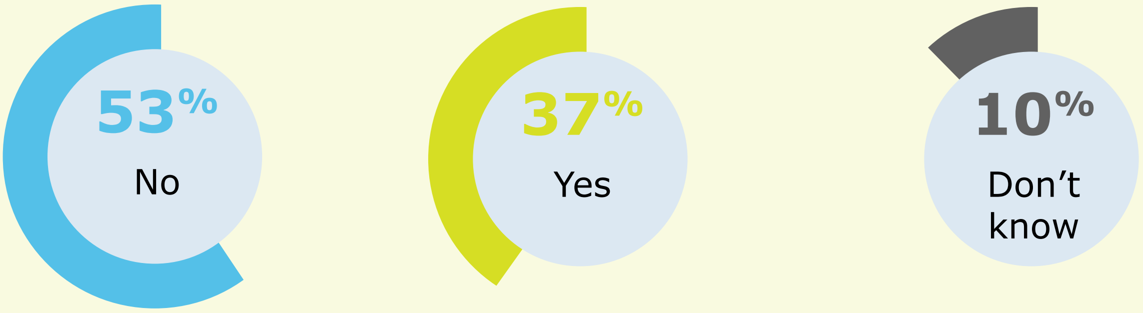
Managing risk together

orx.org

A high percentage of FS organisations have still not adopted a Combined Assurance Plan

A combined assurance plan is a good opportunity to ensure coordinated and efficient monitoring and testing of controls across the three lines of defence. Irrespective of this fact, a roundtable poll revealed, perhaps surprisingly, that a majority of FS organisations (53%) have yet to develop a combined assurance plan. In a small number of cases, FS organisations stated that their Internal Audit Function was not keen on a combined assurance approach since they believed that it may bring into question their independence from the first and second lines of defence.

Most firms have yet to develop a Combined Assurance Model across the 3 lines of defence



Future ORX activities on control practices

ORX will continue to support member benchmarking activity and discussions on the crucial subject of control practices.

ORX will be publishing an Industry Control Reference Library in Q2 2022 and will be hosting further roundtable discussions on Controls Practices during 2022.

For any enquiries on control-related activity, please contact:

Steve Bishop, Research and Information Director, **research@orx.org** , or

Mike Constantinou, Consultant to ORX, **Mike.Constantinou@orx.org**

in @ORX_Association   @ORX_Association   Visit www.orx.org