

Thought Leadership

Why Banks Should Upgrade their Controls Framework to Better Manage their Risks



Authored by:

Rick Bonhof

**Managing Consultant at
Synchron Business
Consulting**

Banks have invested heavily in rolling out Enterprise Risk Management frameworks, largely based on the 'three lines of defence' model with the notion that those who take on and benefit from risk must have accountability for the effective monitoring and control of this risk. However, increasingly, regulators are pushing for stronger corporate governance underpinned by an effective internal control framework. In this article, we'll discuss how to set up an effective control framework that mitigates risk, automates control testing, and helps organizations move toward a more intelligent real-time control model.



Authored by:

Simon Beattie

**Managing Consultant at
Synchron Business
Consulting**

Design of internal control frameworks

The Basel Committee on Banking Supervision in 1998 outlined that an effective internal control framework for financial institutions should consist of the following elements:

- Management oversight and the control culture
- Risk recognition and assessment
- Control activities and segregation of duties
- Information and communication
- Monitoring activities and correcting deficiencies

Typically, the financial institution's governing body will be responsible for

overseeing the control framework and setting the overall control objectives.

The business lines and service delivery teams form the first line of defence (1st LOD) in the control framework and carry responsibility for risk recognition and assessment and implementing control activities.

The second line of defence (2nd LOD) is formed by compliance and risk management who are monitoring that the first line of defence is carrying out its controls activities and act to correct deficiencies.

Finally, the internal audit department forms the third line of defence (3rd LOD) tasked with giving an independent view on the effectiveness of the control framework.



We recommend that firms focus on a single set of controls around a single business workflow, start small, and expand from there to build incrementally a larger controls library. This may include starting with their highest risk areas or highest volume areas to make reviews more efficient and to have a more immediate impact on downstream risk remediation.

Availability and quality of data sets

Arguably the most important driver of intelligent control testing is the availability and the quality of the data set(s) against which the control test will be run. As banks work on POCs in innovation environments they'll need to consider what data they select for the POC and then determine how they will approach key data quality challenges such as:

- Duplicate data fields
- Inconsistent data
- Missing data sets

Our recommendation is that firms allocate sufficient time and resources to define the data model used for each control test and perform a data cleansing exercise accordingly.

User friendliness

To truly empower the 1st LOD the intelligent control testing tool will need to be user friendly. Intelligent control testing will only add benefits if the user can easily setup a control test and easily interpret the result of the control tests.

This is where user experience design, mobile-first design and an understanding of building User Interfaces (UIs) that overlay on top of legacy systems can be incredibly powerful. Banks will need to consider:

- Defining the user's journey through the intelligent controls testing tool
- Translating the control results into easy to read visualisation

Conclusion

Risk management will continue to be a key focus area for financial institutions, and while risk remains a priority, these businesses will need to find ways to better manage their risk at the first line of defence, more proactively. A strong governance framework combined with technology and quality data can help these firms make significant progress to achieving more real-time control testing and enhanced enterprise risk management.

Pain points identified with control testing

For an internal control framework to be effective, the 1st LOD must be empowered to actively manage risk through effective risk identification, aggregation, mitigation and monitoring capabilities. We often find that a 1st LOD is more focused on executing the manual testing of control effectiveness and that business lines are in a constant state of mitigation, which results in a retrospective management of risk. In turn, control processes often are inefficient and applied inconsistently, which can result in increased operational risk for banks.

Common pain points that prohibit a fully-effective internal control framework include:

- Testing is manually intensive and time consuming – i.e. obtaining evidences and manually assessing the effectiveness of controls
- Subjective interpretation of control objectives and test plans leads to inconsistent results within and across lines of defence
- Testing is infrequent resulting in a backward looking internal control framework overwhelmed with remediation exercises
- 1st LOD is busier with testing and mitigation efforts rather than actively mitigating risk and improving processes
- Too much time is spent on defending control outcomes rather than interpreting and improving them

Moving toward intelligent controls testing

We believe that to achieve an efficient and effective internal control framework, financial institutions need to move toward automated and intelligent control monitoring. Technologies such as Natural Language Processing; Robotic Process Automation and Machine Learning are key enablers of this by taking away the heavy manual burden of control test execution from 1st LOD testers and providing 1st LOD with real-time information on control effectiveness and key risk indicators.

In developing the Intelligent Control Testing Accelerator, we have uncovered several important factors that need to be considered for intelligent control testing to be achieved.

Definition of controls and expected results

The first step in moving to intelligent control testing is to define clearly and unambiguously all business rules that make up a control test and the expected result for each business rule. Key considerations to consider to achieve increasingly advanced levels of automated and intelligent control testing are:

- Translating regulatory requirements into control tests and underlying business rules
- Identifying all the relevant iterations of the business rules underlying the control test
- Defining the expected results for the business rules and the overall control test