Deloitte.

Future of controls

Reimagining and modernizing the control framework for banks

Executive summary

Imagine for a moment that you have been appointed to streamline the internal control function[1] at a large global bank. As part of your assessment, you evaluate the risks and corresponding controls across the bank, by reviewing thousands of processes, systems and geographical locations. Upon a cursory inspection, you observe multiple cases of overlapping and redundant controls, and significant manual effort to test and report on the efficacy of the control environment. After your initial review, you feel frustrated—surely there must be a better way to manage the risk and control environment across the organization. There must be a way to drive better business outcomes through these risk and control functions. We hear you.

In an increasingly digital world, the risk and control environment is not keeping up with the pace of change. Controls continue to be inefficient and ineffective. Despite all the investment and increasing requirements and regulations, controls are still failing; the burden of managing, testing and reporting is increasing; and the inefficiency across the three lines of defense continues to grow.

In fact, roughly a quarter of the respondents of Deloitte's 2019 global risk management survey have stated that it's "extremely or very challenging" to effectively and efficiently manage process-level controls (including analytics and reporting). Similarly, roughly half of the respondents also indicated their institutions faced broader challenges regarding their compliance programs, specifically when enhancing systems and processes to meet new or revised regulatory requirements, and adapting the approach with respect to people, processes and technology in their internal control functions.

To ensure a robust control environment that meets financial, operational, regulatory and legal requirements, most banks have adopted the three lines of defense (3LOD) model:

- **First line of defense (1LOD) or the "front-line / business":** Responsible and accountable for appropriately assessing and effectively managing risks associated with their activities.
- **Second line of defense (2LOD) or "independent risk management":** Responsible for overseeing the bank's risk-taking activities and assessing risks and mitigation independently of the CEO and front-line units. These independent risk management groups are also responsible for designing a risk framework appropriate to the bank's size and complexity.
- **Third line of defense (3LOD) or "internal audit":** Responsible for evaluating compliance with policies, procedures and processes established by front-line units and independent risk management, as well as providing independent assurance to the board audit committee.

The regulatory tsunami of the last decade did not afford banks adequate breathing room to reassess their processes, technology and operating models, much less examine the internal control function through an innovative and strategic lens.

As we prepare for the fourth industrial revolution, we need to reimagine the risk and control environment of the future. Imagine an environment that is:

- **Highly automated with real-time control environments** allowing real-time identification of issues and rapid course correction;

[1] For the purposes of this document, the "internal control function" collectively refers to operational risk/non-financial risk management functions (second line of defense), and/or owners responsible for supervision and control execution (first line of defense).

- **Consistent, quality testing** aligned with risk appetite across the 3LOD, optimizing resource allocation and thereby allowing management to focus on driving growth; and
- **A harmonized risk and control universe** that offers clarity and efficiency.

Banks are on the brink of a new age of capability; the acceleration of digital technologies is radically changing organizations in ways that will challenge basic assumptions and operating models. The ways that organizations execute, manage and test controls can't get left behind.

The time is right for banks to reassess their risk management processes to identify long-term flexible and scalable strategic solutions that address the evolving risk and regulatory landscape. It's past time to increase the efficiency, effectiveness and coverage of risk and control programs that improve the risk posture of the bank while also curbing the costs and time spent on compliance activities.

In doing so, banks will likely need to maintain the essence of the 3LOD model, but also rethink the construction of the internal control environment to allow for streamlining—without compromising effective risk management, regulatory expectations and independence objectives.

Deloitte point of view: Three levers for reimagining and modernizing controls

While banks can start their transformation journey by focusing on any of the following three levers, banks are more likely to achieve a breakthrough impact if they engage across all dimensions holistically.

1. **Operating model redesign:** Redesign operating models, talent models and location strategies to work in a globally nimble and effective manner.
2. **Framework rationalization:** Harmonize controls and redesign the testing process to increase coverage, efficiency and effectiveness.
3. **Technology enablement:** Digitalize the internal control function by leveraging emerging technology solutions and advanced analytics.

When the three levers are applied collectively, the cumulative impact could be exponential, potentially leading to estimated cost savings or enhancement of 45–80%* for a typically large global bank.

**The estimates mentioned in the document are based on Deloitte's extensive experience of helping clients transform their internal controls. The actual percentages may vary depending on the nature of the bank's current operating model and current adoption of initiatives described in this document.*

Applying the three levers of transformation could make the internal control function:

- **Cost-efficient:** Eliminate redundancies, expand technology adoption, and improve centralized testing;
- **Insights-driven:** Provide risk intelligent information including causation and correlations between risks and events; and
- **Business enabling:** Achieve reduced friction by further integrating controls into business-as-usual (BAU) processes, consequently creating a better user experience for stakeholders across the lines of defense and enabling timely resolutions of exceptions and issues.

The journey toward achieving full-state transformation (from nascent to transformed) will be unique for each bank. While the journey may seem straightforward, based on our experience it is likely to be bumpy given the volume of processes, stakeholders and geographies that need to be considered; however, the future is upon us and the time to transform is now.

Figure #1: Illustrative internal control function—transformation maturity scale

Transformation levers	Nascent *(traditional)*	Intermediate	Advanced	Transformed *(end state)*
Operating Model Redesign	• Onshore internal controls function • Onshore testing • Distributed teams for testing	• Controls transformation governance model formalized • Majority testing onshore; a few testing activities done offshore	• Chief Controls Officer (CCO) • Combination of onshore, offshore, and managed services • Centers of excellence for specialized skills e.g., data, automation	• Predominantly offshore testing through utilities • Matured 1st line of defense influencing control design with clear control ownership, aligned with 2nd line expectations
Framework Rationalization	• Hundreds of multiple, redundant controls • Lack of formal prioritization processes and controls • Redundant and multiple testing	• Partial harmonization of controls • Common risk and controls taxonomy	• Risk-based approach to controls testing • Adoption of 'test once' approach across a few key controls	• Dynamic, continuous risk assessment • Adoption of 'test once' approach across significant number of controls
Technology Enablement	• Manual controls • Manual testing • Limited tools enablement • Ad-hoc approach to automation	• Automation of certain entity-level controls (10%) • Use of Robotic Process Automation (RPA) and data analytics tools for certain test areas • Use of technology platform for collaboration across stakeholders	• Automation of considerable entity-level controls and process-level controls across multiple areas (30-40%) • Significant use of RPA and data analytics tools across processes • Use of cognitive tools for automated analysis of unstructured data types	• Significant automation of controls (70-80%) • Continuous testing and monitoring of controls • Real-time handling of exceptions through use of cognitive tools, and predictive analytics • Predictive insights to support continuous risk sensing

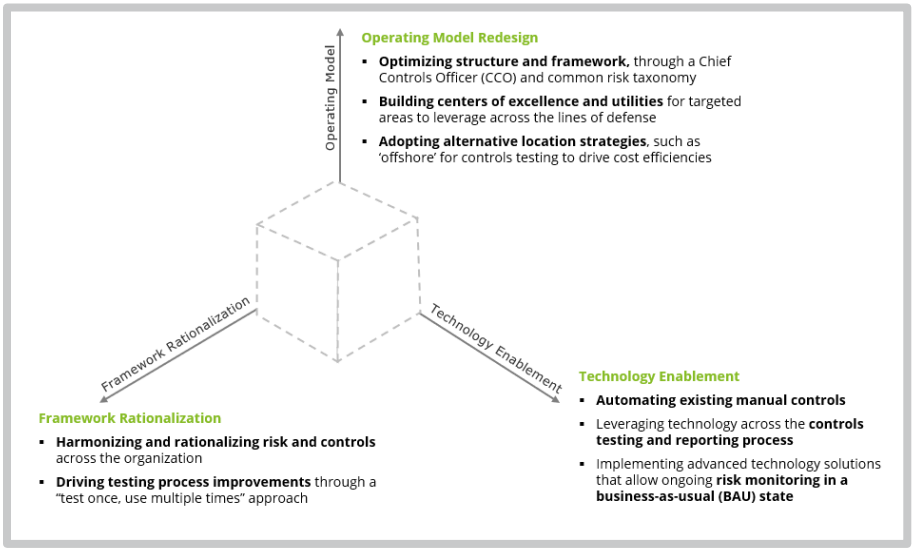
Low — Maturity of transformation — High

Deep dive into the levers of control transformation

Most discussions on the advancement of internal control functions can be deconstructed into three broad dimensions or interrelated levers.

Banks are envisioning their future internal control function to include a common language of risk and control that offers clarity; centralization of functions to drive efficiency; highly automated and real-time control environments that allow real-time identification of issues and rapid course correction; and optimal resource allocation for testing and monitoring controls that allow management to focus on driving growth. In discussions with clients, we are often asked what is the best way to get started.

Figure #2: Overview of the transformation levers



The encouraging answer, and one we passionately believe in regarding this topic, is that there is no one correct answer. The more important consideration is to overcome inertia and other very real obstacles and get started on any one of the levers—and, as success is achieved, to move rapidly onto the other dimensions. Needless to say, the more levers engaged, the higher the fulfillment of benefit and the more complete the transformation.

In the rest of this document, we explore each dimension in more detail, including providing real-life client examples of global banks that are successfully engaging these three levers.

Operating model redesign—lever one: Redesign the operating and talent models to work in a globally nimble and effective manner

The current operating model for the internal control function is proving to be ineffective in addressing the complexities of current risk and regulatory expectations and the evolving business environment.

Banks' internal control functions increasingly need talented professionals with multidisciplinary skill sets, who understand banking processes and the risk landscape and can leverage data and technology to digitalize controls and modernize the testing and monitoring process. In addition, there is constant pressure on testing and internal audit teams to reduce the costs associated with compliance, and drive efficiencies and labor arbitrage.

As banks look to transform their internal control functions, it is important to rethink the operating and talent models to allow them to operate in a nimble, efficient and effective manner. This includes:

a. Optimizing the structure and framework through a Chief Controls Officer (CCO) and a common risk taxonomy;
a. Building centers of excellence (CoE)/utilities for targeted areas to leverage across the lines of defense; and
b. Adopting alternative location strategies and building a future-ready workforce.

Leveraging CoE and offshore models could lead to an estimated cost saving of **15–30%***

**If banks already have an offshore presence, then streamlining the model may lead to 15–20% savings. The savings may be much higher in situations where banks do not have an offshore presence.*

a. Optimizing structure and framework

When exiting the 2008-09 crisis, many banks were expected to perform significant enhancements to their risk management programs. The 2LOD began to develop, often as part of initial efforts to help implement and operate these enhancements for the benefit of the enterprise. In light of heightened regulatory expectations, less questioning existed on the appropriateness of whether these efforts should be incubated in the 2LOD. In an environment where non-compliance was not an option, risk budgets were bountiful—and the pressure on management and governance committees for just someone, anyone, to get it done seemed apropos to the environment. Things have clearly changed. There is an increased pressure on the 1LOD to demonstrate the execution of their risk and control responsibility and on management to be able to demonstrate how they are confident their risks are well controlled. Much of this has necessitated the need to rereview the 3LOD model and address any potential scope creep in the mandates of the individual lines.

In the context of the pendulum of responsibility swinging back to the 1LOD, an increasing number of large financial service institutions are creating the role of a **Chief Controls Officer (CCO)**[2]. Regardless of whether this title is formally used, the person charged with the responsibility of controls is expected to:

- Concentrate the 1LOD risk and control capability and close expertise gaps that might exist in this line;
- Reassign and realign responsibility for the management of operational risk from the 2LOD to the 1LOD; and
- Bridge the interaction gap with the 2LOD.

[2] For more details, please see also our "The emergence of the chief controls officer" point of view.

To achieve this, the CCO, in coordination with the 1LOD and 2LOD, would need to:

- **Define accountabilities** to ensure it is clear which responsibilities for control are delegated, how this delegation operates, and where overall accountability lies.
- **Establish the mandate**, making clear which activities the CCO function is responsible for and what is performed elsewhere, including risk identification and appetite setting, standards setting, testing, remediation and reporting.
- **Design the operating model** to suit the mandate, taking account of resourcing; reporting lines and organizational structure; centralized or decentralized approaches; and talent, location and sourcing strategies.
- **Focus on risk** to ensure that reporting on risk exposure is not lost in the industry of control operation, testing and remediation activities.
- **Deliver efficient testing,** taking a risk-based approach and leveraging a range of testing techniques, including using emerging technologies.

In addition to leveraging a CCO, optimizing structure and framework requires organizations to enhance and update their risk taxonomies.

Enhancing and updating risk taxonomies

A risk taxonomy is a catalog or classification of risk groupings or categories that have been defined by a bank. It helps drive the comprehensive identification of risks that the bank could face, and alternately assists with the aggregation and roll-up of information when reporting to management and various risk committees. Ensuring consistency in the aggregation method, risk taxonomies assist in gauging the trending of risk, period over period, and help drive structure for multiple risk management tools such as risk and control self-assessments. Therefore, taxonomies provide a consistent language through which operational risks facing the institution can be communicated.

Traditionally, most taxonomies have been modeled from the Basel event types. With the increase in non-financial risks that institutions face—cyber risks, the increased focus on market integrity and conduct, sales practices and customer harm, emerging industry ecosystems and third-party risk—there is a clear recognition of the need to make changes to existing taxonomies, while at the same time maintaining cross-references to Basel.

Many institutions have already started down this path, adapting existing taxonomies to reflect today's operational risk environment while also maintaining a mapping to Basel event types, primarily for capital management purposes. But given how integrated taxonomies have become in operational risk management programs, any changes will affect multiple downstream processes and control procedures. Inventorying how taxonomies are used and any downstream effects is an essential part of the enhancement of operational risk management and control programs.

This document focuses on this very impact on the institution's control framework and the scoping of individual control activities. Once banks have identified the catalog of operational risks they face (i.e., the taxonomy), identifying the right controls to mitigate the occurrence or realization of those risks—and reduce the severity of impact should the risk materialize— becomes critical. Refreshing this list of risks and scoping the appropriate controls is one of the key factors to consider and the starting point for any control rationalization effort. We explore this approach in more detail in lever two of this document.

Figure #3: Illustrative representation of Deloitte's risk taxonomy framework

Risk Class	Category	Sub Category	Risk Type	Definition/Description
NON-FINANCIAL RISK	Compliance Risk	Compliance Risk	Consumer Protection	Risk of failing to comply with consumer protection statutes resulting in regulatory sanctions, reputational damage or targeting by consumer advocacy groups. Risk of failing to provide public information, pre-contractual, contractual and post-contractual information. Risk of misusage of client's personal data, failing to comply with the confidentiality regulations.
NON-FINANCIAL RISK	Compliance Risk	Compliance Risk	Conflicts of Interest	Risk to a financial institution that may result from dealings with insiders, the bank benefiting inappropriately, the bank's conflicting roles with a client or an employee's unethical conduct.
NON-FINANCIAL RISK	Compliance Risk	Compliance Risk	Privacy	Risk of non-compliance with one or more obligations regarding unauthorized access, use, disclosure, disruption, modification or destruction of personally identifiable information of a client and/or employee.
NON-FINANCIAL RISK	Compliance Risk	Compliance Risk	Market Integrity	Risk of failing to develop and administer an effective Anti-Market Abuse Program that ensures that markets operate fairly and safely in order to encourage transparency and the widest possible customer and confidence in them.
NON-FINANCIAL RISK	Conduct Risk	Products and Channels	Abusive Pricing	Risk of false, misleading, abnormal or artificial pricing, contrary to market levels
NON-FINANCIAL RISK	IT Risk	IT Risk	Inappropriate user profiling or access management	Risk of inappropriate actions, use of- or access to- information , derived from lack or incorrect access management privileges or authorization
NON-FINANCIAL RISK	People Risk	Employment Practices	Diversity & Discrimination Risk	Risk of losses arising from acts of all discrimination types
NON-FINANCIAL RISK	Process Risk	Execution, Delivery & Process Management	Trade Counterparties Risk	Risk of losses and unsettled transactions that result from incorrect, incomplete or inaccurate counterparty data used for the execution, capture or maintenance of a transaction
NON-FINANCIAL RISK	Reputational Risk	Reputational Risk	Reputational Risk	nd
NON-FINANCIAL RISK	Reputational Risk	Reputational Risk	Environmental and Social Reputational risks	Risk of direct or indirect connection to sensitive sectors, client relationships and/or transactions with a negative impact on the environment or society, which deviate from International Standards or the Code of Business Conduct and Ethics and hence influence the sustainability of the organization.
NON-FINANCIAL RISK	Strategic Risk	Business & Strategic Risk	Business Model Risk	Risk of failing to develop a business model that focuses on creating and maintaining value for shareholders
NON-FINANCIAL RISK	Strategic Risk	Business & Strategic Risk	Business & Strategic Risk	Risk of impact on earnings or capital arising from adverse business decisions, misaligned strategy or lack of responsiveness to industry trends, for example, M&A, product obsolescence, aging consumers and workforce, emerging markets, industry consolidation, energy shocks, cost inflation, consumer demand shifts etc.,
NON-FINANCIAL RISK	Third-Party Risk and Outsourcing	Third-Party Risk	Financial Viability Risk	Risk of disruption to the institution's operations due to a third party no longer being able to provide products/services as it's unable to generate profit or maintain necessary capital for supporting its ongoing operations

b. Building CoE for targeted areas to leverage across the three lines of defense

Today, global organizations are adopting newer operating models to bring efficiency in performing ongoing monitoring of internal controls. One of the most popular and effective methods adopted is setting up **CoE for testing and managing controls**. Centralizing activities common to control functions in a control CoE can help to build consistency in the performance of controls or in the assessment of effectiveness. In addition, the CoE could also be responsible for driving control transformation efforts, especially as it relates to the "technology lever" (i.e., automation, analytics and cognitive technologies).

While the benefits of CoE/utility are numerous, there are key business decisions that need to be made, including:

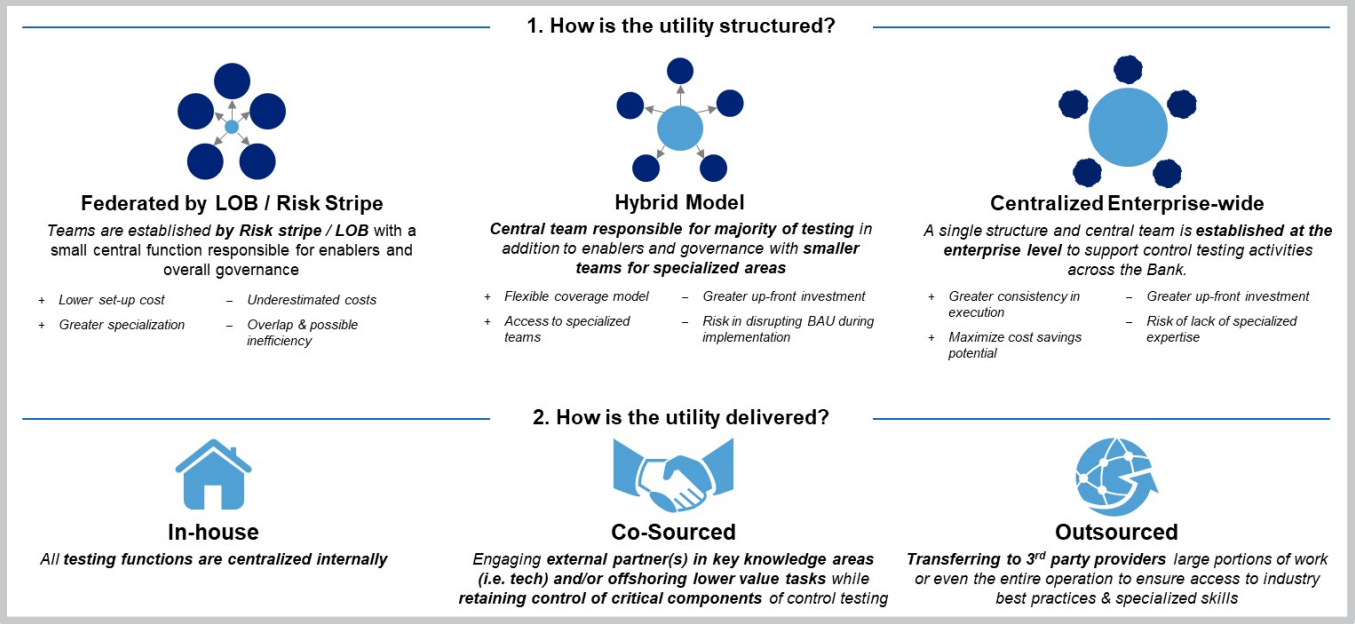
- **Mandate and governance**: Banks need to determine the mandate for the utility and how it will support and collaborate with the lines of defense and the CCO. It is important to build a service management framework and align with roles and responsibilities to be able to operate the utility seamlessly and effectively.

- **Service scope:** It is important to determine the testing scope for the utility. For example, the nature of controls that will be tested through the utility, the frequency and extent of testing, key performance indicators related to responsiveness and time taken to execute, etc.

- **Utility structure:** Traditionally, banks' utilities have been structured in a federated or hybrid model. However, a centralized utility would enable banks to achieve greater consistency in execution, eliminate redundancies, and foster collaboration and effective issue resolution across the lines of defense.

Lastly, banks could adopt alternative location strategies e.g., **offshore models** for the CoE/utility. By building the control CoE offshore, it would help banks reduce the cost of controls testing and monitoring. Banks have the option of either running the utility in-house or outsourcing to a third-party service provider.

Figure #4: Illustrative representation of a control CoE / utility



c. Adopting alternative location strategies and building a future-ready workforce

Banks often devote considerable resources to manual test controls in order to satisfy various regulatory requirements. Leveraging cost-effective location strategies, such as moving testing activities offshore, allows banks to significantly drive cost savings and allow the continuous delivery of testing across time zones.

Building a centralized offshore utility can also allow a bank to get a complete view of the risk and controls across various processes; rationalize the frequency, scope and extent of testing based on the risks; and execute the "test once, use multiple times" approach *(explained under "Framework rationalization").*

These utilities can also be leveraged to drive technology enablement and automation to make the control testing and monitoring process more efficient and effective *(explained under "Technology enablement").*

- To build a future-ready workforce in the controls utility, banks are implementing programs to cross-train and rotate employees across the testing and business functions to build "purple teams".
- Purple teams represent a combination of resources that possess a mix of business, technology, risk management and data analytic skills.
- Members of purple teams can speak the language of both business and technology, allowing them to serve as translators between both functions while focusing on making technology systems useful in a business context. This helps the utility drive technology enablement efforts.

Client spotlight:

- **Client challenge:** A large global banking client wanted to drive efficiencies in its compliance quality testing function and were keen to explore alternative strategies, including offshore models and testing utilities.
- **Deloitte solution:** Deloitte assessed the current operating model of the testing function to determine inefficiencies and gaps. Through visioning conversations with senior client stakeholders, Deloitte helped develop a two-year transformation roadmap for transferring testing offshore through a centralized testing utility. In addition to providing recommendations, Deloitte helped the bank set up its offshore-based testing utility in India for its compliance quality testing group.
- **Value generated:** Post-implementation of a two-year transformation road map, the bank's centralized testing utility allowed it to test processes across America, Europe and Asia-Pacific. This testing utility allowed the bank to minimize redundancies in testing; adopt the "test once, use multiple times" approach; enable common testing processes; and efficiently leverage new technologies such as artificial intelligence (AI) that complement centralized data management and testing.

Process redesign—lever two: Harmonize controls and redesign the testing process to make it more efficient and effective

In the last decade, when it came to internal control design, monitoring and reporting, banks reacted to the evolving regulatory landscape. They often adopted tactical solutions to meet immediate regulatory requirements. This led to issues such as:

- A patchwork of risk and control frameworks across the organization;
- A library of controls that continue to grow;
- Prescribed and inflexible test procedures that may not adequately address evolving risks;
- Test programs that lack a risk-based focus; and
- Inadequate reporting framework that lacks insights.

With the increased pressure to increase the scope and coverage of testing, contain the cost of compliance and provide insightful and timely reporting, banks have an opportunity to redesign the control processes to drive efficiency and effectiveness across the internal control function.

Key redesign phases include:

a. Harmonizing and rationalizing risk and controls across the organization; and
b. Driving testing process improvements through a "test once, use multiple times" approach.

Transforming control processes could help achieve estimated cost savings of **10–20%.**

Key activities for each redesign phase are as follows:

a. Harmonizing and rationalizing risk and controls across the organization

As new industry frameworks and regulatory requirements (e.g., SWIFT, Cloud Computing Framework and NIST) are released to address an ever-growing list of risks, many banks have responded by adding new controls to address these specific, identified requirements. This has resulted in an explosion of potentially redundant and/or duplicate controls within and across the 3LOD, as organizations try to quickly design controls that address these risks. This drives the need for organizations to review their risk and control

environments to ensure they have well-written controls that holistically address the risk to avoid duplication across regulatory requirements. Banks have an opportunity to standardize, benchmark and optimize their controls to implement a more robust control framework, align with industry best practices, and improve the efficiency of control testing.

By completing an exercise to harmonize and rationalize your controls, you could potentially decrease the amount of required testing and redundancy across the 3LODs, freeing up resources to focus on testing of known problem and/or higher risk areas.

However, adopting robust, dynamic risk assessment techniques are a precursor to harmonizing controls. This refers to an integrated risk-based program that helps identify diverse risks associated with the process or function and then prioritize based on the nature of risk. Dynamic risk assessment helps with focusing on an organization's significant business risks and is responsive to a frequently changing risk environment.

The identification and regular updating of risks is probably the biggest factor in the rationalization or harmonization of controls, including designing new controls for any new risks identified.

Harmonizing and rationalizing the control framework involves:

- Evaluating business process objectives to ensure the correct balance between risk and control is maintained. Too much control is as suboptimal as too little control.
- Establishing a common taxonomy for controls, identifying critical controls, and establishing a mechanism to ensure that controls are working effectively.
- Mapping controls to multiple regulatory requirements to reduce redundancy.

Banks need to identify controls that are repetitious or redundant, so they can be streamlined or eliminated. Harmonizing controls includes:

- **Entity-level controls:** Creating comprehensive entity-level controls by combining some existing controls.
- **Controls benchmarking:** Benchmarking control processes, definitions and their risks across the industry, as well as adding, eliminating and combining controls based on industry best practices.
- **Controls standardization:** Standardizing and rationalizing the control framework based on a top-down approach, including common control considerations to introduce better and leaner controls.
- **Risk-based controls testing:** Adopting a risk-based approach to obtain more evidence for higher risks and vary the extent and frequency of testing based on the nature and severity of risk, and risk of control failure.

For example, if we look at access controls, harmonization of controls would entail looking at parameters, such as how the control itself has changed over the year; looking at failures over the year; and attrition of individuals responsible for managing the control. This will help determine the key risks, and whether the current controls are adequate or if newer controls are required. It could also help determine the nature, extent and frequency of testing.

However, harmonization of controls is not a one-time activity. Banks need to establish a mechanism to reevaluate controls on a periodic basis based on changes to business objectives, evolving business processes, and changing risk profiles.

Client spotlight:

- **Client challenge:** A leading financial institution was looking to test the design and operating effectiveness of internal controls across lines of businesses and the global organization (US, EMEA and Asia).
- **Deloitte solution:** Deloitte obtained an understanding of the control environment, including the business process (compliance and external financial reporting) and information technology (IT) areas. The team assisted management in determining scoping and prioritization of controls through risk assessments, identification of critical control points, and development of a testing roadmap. Then, the team created automated test scripts with detailed test procedures and a testing methodology to ensure "evergreening" of work performed i.e., the scripts can be leveraged for future testing efforts.
- **Value generated:** The results of the design and operating effectiveness testing were shared with business line management and business-aligned operational risk coordinators, and a key list of issues was identified. The insights related to the remediation plan helped the client significantly enhance the existing control environment.

b. Driving testing process improvements through a "test once, use multiple times" approach

Control testing acts as an independent oversight process to help provide assurance on the effectiveness of controls and their adherence to stated policies and procedures. However, as various regulatory requirements have evolved over time, processes around control testing have resulted in redundancies and other inefficiencies. Some controls are common for multiple regulatory requirements, and the testing teams check the same controls multiple times throughout the year to satisfy different reporting requirements. To counter these inefficiencies, **banks are adopting an integrated control testing approach that allows banks to "test once and use multiple times."**

Banks are developing **integrated control repositories** that document a consolidated list of controls across different processes and functions. This helps provide better visibility to testing teams of the controls that are common for multiple regulatory requirements. Also, by using better workflow tools and dashboards, the control testing results can be updated in the repository, allowing the testing teams to leverage the results when reporting on other regulatory requirements.

In addition to being more efficient, this approach could significantly increase the experience of process owners and help reduce friction between testing teams and process owners. In other words, a fully harmonized control function that leverages a "test once, use multiple times" approach could blend key controls related to compliance, operations, regulatory and financial requirements.

In addition, banks can leverage the following techniques to drive testing process efficiencies:

- **Surveys and peer reviews:** Conducting survey walkthroughs to simplify the control owner process could lead to fewer in-person meetings, thereby reducing time and effort for the control owners. In addition, peer reviews of controls by other process owners can significantly reduce the effort required for testing, as the testing team can rely on peer review results.
- **Control self-assessments:** Leveraging samples, evidence and results from control self-assessment processes can reduce the time and expense required for testing.
- **Continuous monitoring and reporting of key-risk indicators:** Banks should consider conducting real-time and continuous monitoring of key risks to identify anomalies and trends. Dynamic risk reporting can support timely identification, measurement and reporting of risks, including risk appetite breaches and key-risk indicators that are customized to individual audiences. Leveraging a combination of emerging technologies could allow banks to achieve this in a cost-effective way *(explained under "Technology enablement").*

Client spotlight:

- **Client challenge:** A leading financial institution was looking to review the quality of more than 8,000 control instances documented in its control library, with an estimated manual effort of 26 weeks. The client wanted to identify efficient and effective methods to meet stringent regulatory deadlines.
- **Deloitte solution:** As a first step, it was important to rationalize the control framework to understand the key risks faced by the client and the corresponding controls. Deloitte leveraged its proprietary automated control library assessment tool, *Controls Intelligence*, and uploaded the control instances into the tool. Root cause analysis delivered a remediation road map and provided insight into remediation priorities. In addition, Deloitte helped identify duplicate controls that could be eliminated or streamlined. Deloitte used a risk-based approach to help the organization prioritize controls and processes for testing purposes. Deloitte helped streamline testing using lean and targeted testing procedures based on risk assessment results and risk of control failure. Deloitte determined the optimum nature, timing and extent of testing using the revised risk-based approach to reduce testing effort.
- **Value generated:** A combination of innovative methodologies and tools helped drive significant efficiencies and reduce the effort by over 60%.

Technology enablement—lever three: Digitalize the internal control function by leveraging emerging technology and analytics

Arguably one of the biggest changes to affect the financial services industry over the last five years has been the adoption of new client-facing, decision and transaction processing technologies to significantly speed up decision making. This trend has led to significant changes in the risk profile of banks; yet, at the same time, it also offers the promise of enhancing risk and control management processes.

Currently, in many organizations, the majority of controls are manual—requiring process and control owners to spend significant time and effort in monitoring and reporting on controls. There is constant pressure on the internal control functions to reduce costs, drive efficiencies and identify emerging risks in a timely manner. Banks see a growing need to leverage emerging technologies such as robotic process automation (RPA), AI, cloud, and predictive and prescriptive analytics to make the internal control function more efficient and proactive.

Driving digital transformation in the risk and control function includes the following three dimensions:

a. Automating existing manual controls;
b. Leveraging technology across the control testing and reporting process; and
c. Implementing advanced technology solutions that allow ongoing risk monitoring in a BAU state.

Before we dive deeper into the application of emerging technologies, it is helpful to analyze some of the guiding digital principles when assessing adoption and usage:

- **Frictionless user experience:** Delivering a secure and customized user experience; easy access to data; and mobile and cloud-enabled to scale.
- **Agile:** Real-time or near real-time risk posture; and rapid response capabilities to risk events.
- **Automation and analytics:** Controls that are automated or provide a digital trail for analytics; shared data and analytics across lines of defense; and risk correlation, large scale analytics across channels and customers.
- **Intelligent:** Proactive risk sensing; and foresight and insights into emerging risks.
- **Actionable:** Alerts and timely escalation of issues to stakeholders; and leveraging risk portal and self-service.

Leveraging a combination of technology enablers could drive estimated cost savings of **20–30%.**

a. Automating existing manual controls

Digitalized processes and controls are either fully automated and/or create a digital trail regardless of how they are executed (i.e., manual or automated).

Currently, a significant number of controls at large global banks are manual. There is a huge potential to reduce the cost of testing by designing automated controls that, if done correctly, would allow testing teams to focus on the design of automated controls rather than costly, manual and sample-based testing.

Digitalizing controls can help banks leverage actionable risk data across the 3LOD, as well as enable smart monitoring as an enterprise capability to effectively identify, monitor and report risks in real-time. As business units/process owners get near real-time visibility into risks, they are better equipped to rapidly respond to risk events.

Banks can leverage a combination of new (e.g., RPA, AI, cognitive, and big data analytics) and established technologies (e.g., workflow tools and governance risk and compliance [GRC] systems) to enable digitalization.

Given the scale and complexity of the control environment, it is important to prioritize the right controls for automation. Banks should consider adopting the following step-by-step approach:

- **Prioritize controls** based on the risk assessment results, degree of standardization and repetition, volume, etc.
- **Select the method of automation** e.g., RPA, GRC, cognitive intelligence, etc.
- **Source the data required for digitalization** to facilitate automated monitoring.
- **Identify KPIs** for selected process and controls, and to measure the effectiveness of digitization.

Client spotlight:

- **Client challenge:** A global investment bank wanted to enhance the effectiveness of its internal control function, including enhancing first-line ownership, control rationalization and leveraging technology to make controls “preventative”.
- **Deloitte solution:** The Deloitte team helped the client redesign and optimize the end-to-end process as a precursor to leveraging technology and automation. The team prioritized a regulatory area with a significant error rate and issues and used pilot experience to expand across topics, products, businesses and geography. For the prioritized area, the team leveraged automation and technology to uplift preventative controls into the process, which helped reduce time and effort for second-line testing. The team also enabled the client to create a CoE to lead automation and business change management efforts.
- **Value generated:** The solution enabled the client to standardize its risk and control framework through a centralized rules repository, evaluate transactions in real-time, and leverage preventative and smart detective controls to identify and remediate issues in a timely manner.

b. Leveraging technology across the control testing and reporting process

Once key process-level controls are digitalized, it is easier to automate the testing of these controls. Banks should consider making strategic investments across the testing lifecycle, in areas such as data management, automated testing, and workflow and collaboration tools to drive efficiencies.

- **Workflow management:** Workflow management and collaboration platforms could help provide instant visibility to stakeholders across the lines of defense, thereby fostering collaboration. *Banks could leverage workflow and business process management tools, such as Pega, Appian and Workiva.*
- **Data management:** Data management tools can help extract population data from organizations' Enterprise Resource Planning (ERP) systems and the storage and preparation of data (standardization, removing anomalies, etc.) This data can then be visualized to identify outliers for further investigation. *Banks could leverage data cataloging and wrangling tools, such as Informatica, Collibra and Trifecta to address their data management needs.*
- **Automated insight generation:** The aggregated, cleansed data could be fed into an analytics engine to identify hidden risks and patterns through 100% population testing. As a result, internal control functions will likely need to spend fewer hours testing and can instead focus their time and effort in analyzing exceptions. *Automated machine learning (AutoML) vendors, such as DataRobot, H20.ai and Tensorflow are a few of the leading tools in this space.*
- **Automated reporting:** Banks could leverage RPA and natural language generation (NLG) to automate the creation of testing and exception reports. *NLG vendors, such as Narrative Science/Quill and Arria could be leveraged to automate the generation of testing reports, including the creation of control narratives and descriptions of possible exception items.*
- **Data visualization and dashboarding:** Coupling automation and cognitive technologies with advanced visualization tools (*such as Tableau or Microsoft PowerBI)*, dashboards, and conversational interfaces (i.e., chatbots) could allow banks to visualize data and identify outliers for further investigation, while delivering a seamless experience to key stakeholders across the lines of defense.

Client spotlight:

- **Client challenge:** A global bank struggled to address the risk of segregation of duties within its wire disbursement process.
- **Deloitte solution:** Using Deloitte's *Digital Testing and Controls Automation (DTCA)* approach, Deloitte was able to analyze numerous security profiles and transactions. This uncovered critical segregation of duty violations that would likely have gone undetected due to the complex nature of the bank's IT environment. In one instance, the same individual had the ability to update payee information and process disbursements, creating the potential for fraud.
- **Value generated:** Analyzing security profiles is now a continuous process that alerts the bank of future violations in real-time.

c. Implementing advanced solutions that allow ongoing risk monitoring in a BAU state

In addition, banks can implement solutions that can help with the ongoing monitoring of the risk and regulatory landscape and keep track of multiple control frameworks and requirements. Leveraging predictive risk intelligence and the use of advanced analytics for pattern recognition, as well as correlation and causal analysis, can give the internal control function a head start with identifying the buildup of potential risk and the need for remedial action. Some examples include:

- **Regulatory horizon scanning:** Banks can leverage horizon scanning tools that can scan the regulatory landscape for new regulations, or amendments to existing regulations, and help identify

new requirements that banks may have to comply with. *Vendors such as Corlytics, Cube and Compliance.ai are exploring this space.*

- **Ongoing risk sensing and predictive analytics:** Beyond regulations, banks can use broad-based risk sensing tools to identify emerging risks in the ecosystem (e.g., supplier, customer, geopolitical and social media). Banks can establish predictive analysis capabilities to support risk sensing through the identification of previously unknown patterns, correlations and causation. GRC platforms can continue to play an important role when insightful metrics—aligned with specific risk exposures and use cases—are collected and leveraged for predictive analytic models. This information becomes an available node of intelligence for broader enterprise-level insights across various themes, as well as to inform risk assessments and mitigation strategies.

Several leading global banks have embarked upon the journey to digitalize their risk and control functions across the three technology enablement dimensions by implementing dedicated accelerators and incubators, developing innovation programs, and partnering with vendors.

- Gartner, Forrester, and other leading analysts have identified *MetricStream, ServiceNow, Bwise, ACL/Rsam Galvanize, RSA Archer and LogicManager* as key risk management vendors.
- In addition, the RiskTech startup ecosystem (i.e., startups that leverage emerging technologies to address risk-related issues) is evolving rapidly.
- While established vendors offer a more holistic solution, the RiskTech startups are more on point solutions for specific needs across the lifecycle.

Banks have an opportunity to leverage a combination of these established vendors and/or startups in their internal control functions.

Note: *Deloitte does not endorse any of the vendors mentioned in this document. The list is based on a preliminary assessment of analyst reports published by Gartner and Forrester in 2018 and 2019 and additional independent, preliminary secondary research.*

Client spotlight:

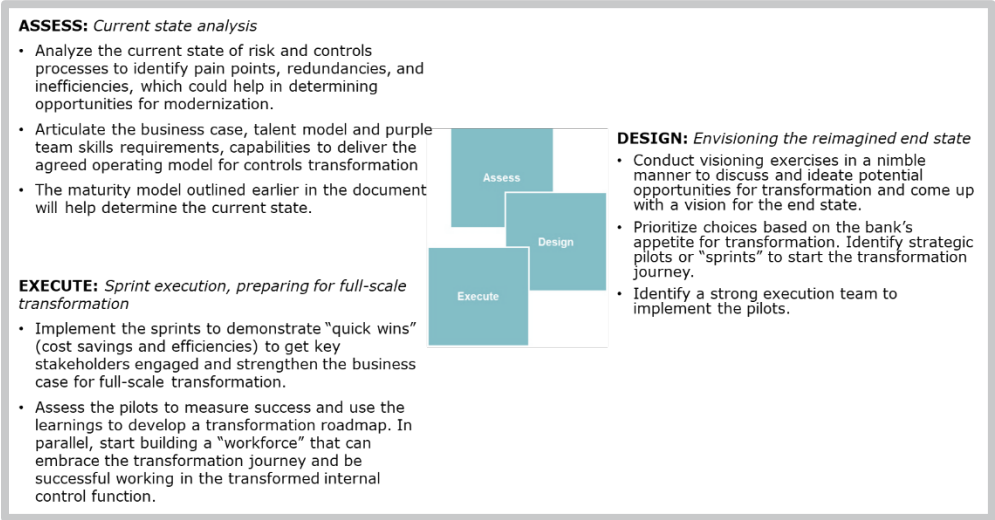
- **Client challenge:** A large financial services institution was under pressure to meet compliance and operational risk testing requirements, including coverage and execution. The client lacked the resources, capacity, technical knowledge and time to address all the requirements of its compliance and operational risk testing plan. Assistance was required across the testing lifecycle, including the design, execution, data requirements, and test operating model and strategy.
- **Deloitte solution:** Deloitte provided resources through different delivery models to assist the client with various needs, including co-sourcing for execution and remediation of existing testing; subject matter expertise for specific regulatory requirements; and traditional project structures for the design and execution of new tests and test strategy. Deloitte also used innovative solutions, leveraging robotics and automation to drive efficiencies and deliver strategic testing insights.
- **Value generated:** The client was able to meet ongoing regulatory requirements and provide compliance and operational risk testing coverage for their businesses. In addition, the client gained exposure to an innovative testing approach that leveraged a combination of alternative delivery models and technology.

Plotting the way forward—how can banks get started?

The path toward control transformation is a continuum with increasing value. **There is no "one size fits all" approach and the journey towards transformation is unique to each bank. Banks can start their transformation journey from any of the three transformation levers and then move outwards to**

leverage the other levers. When the three levers are applied collectively, the cumulative impact is expected to lead to significant cost savings and efficiencies.

Figure #5: High-level approach to help banks get started:



The future is here—the future is now! Are you ready?

Contact us to discuss how the ideas presented in this document can apply to your organization, and how you can begin your journey to transform your internal control function.

Global contacts

Naru Navele

Partner, Deloitte & Touche LLP

+1 470 434 2002

nnavele@deloitte.com

Nitish Idnani

Principal, Deloitte & Touche LLP

+1 212 436 2894

nidnani@deloitte.com

Madhu Gopinath

Principal, Deloitte & Touche LLP

+1 713 982 2319

mgopinath@deloitte.com

Cherian Thomas

Managing Director, Deloitte & Touche LLP

+1 678 299 7310

chethomas@deloitte.com

Kimberly Turgeon

Partner, Deloitte & Touche LLP

+1 416 643 8376

kturgeon@deloitte.ca

Ninad Bhangle

Specialist Master, Deloitte & Touche LLP

+1 678 299 9854

nbhangle@deloitte.com

Special thanks to the following subject matter experts for this publication:

James H Caldwell, Partner, Deloitte & Touche LLP**; Stuart Rubin**, Managing Director, Deloitte & Touche LLP; **Gowri Zoolagud,** Managing Director, Deloitte & Touche LLP; **Kalyan Rajendra Prasad,** Managing Director, Deloitte & Touche LLP; **Manoj Bhale,** Managing Director, Deloitte & Touche LLP; **Anil Atmuri,** Senior Manager, Deloitte & Touche LLP; **Matthew Tilner**, Senior Manager, Deloitte & Touche LLP; **Vipul Sehgal**, Senior Manager, Deloitte & Touche LLP; **Yang Chu**, Senior Manager, Deloitte & Touche LLP; **Abhishek Deshpande**, Senior Manager, Deloitte & Touche LLP; **Meghna Panwar**, Senior Manager, Deloitte & Touche LLP; **Shreya Shrivastava**, Manager, Deloitte & Touche LLP; **Khyati Kabra**, Manager, Deloitte & Touche LLP

Luxembourg contacts

Laurent Berliner

Partner, EMEA FSI Risk Advisory Leader

+352 45145 2328

lberliner@deloitte.lu

Roland Bastin

Partner, Risk Advisory

+352 45145 2213

rbastin@deloitte.lu

Martin Flaunet

Partner, IFRS Leader

+352 45145 2334

mflaunet@deloitte.lu

Irina Hedea

Partner, Risk Advisory

+352 45145 2944

ighedea@deloitte.lu

Stephane Hurtaud

Partner, Risk Advisory

+352 45145 4434

shurtaud@deloitte.lu

Jean Philippe Peters

Partner, Risk Advisory Leader

+352 45145 2276

jppeters@deloitte.lu

Jerome Sosnowski

Partner, Risk Advisory

+352 45145 4353

jsosnowski@deloitte.lu

Eric Centi

Partner, Financial Services Tax

+352 45145 2162

ecenti@deloitte.lu

Pascal Martino

Partner, Banking Leader

+352 45145 2119

pamartino@deloitte.lu

Arnaud Willems

Partner, Operations Excellence & Human Capital

+352 45145 3309

awillems@deloitte.lu

Endnotes and references

1. **Deloitte UK, "The emergence of the chief controls officer," May 2018:** https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-mission-control-in-financial-services.pdf
2. **Deloitte, "The future of controls | Radical change: confidence, intelligence, performance," November 2019:** https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-future-of-controls.pdf
3. **Deloitte, "The Future of IT internal controls—Automation: A game changer," January 2018:** https://www2.deloitte.com/in/en/pages/risk/articles/the-future-of-it-internal-controls.html
4. **Deloitte Center for Regulatory Strategies, "Reimagining the first line of defense's role in bank regulatory compliance: Digitalizing processes and controls to drive profitability and efficiency," January 2018:** https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-regulatory-reimagining-the-first-line-of-defenses-role-in-bank-regulatory-complaince.pdf
5. **Deloitte Luxembourg, "Three Lines of Defense: Time to rethink and reframe the model," July 2017:** https://www2.deloitte.com/lu/en/pages/risk/articles/three-lines-defense-luxembourg.html
6. **Deloitte, "Digital testing and controls automation: A transformative approach to automating your control environment," 2019:** https://www2.deloitte.com/us/en/pages/advisory/articles/digital-testing-approach.html
7. **Deloitte, "Beyond the hype: Global Digital Risk Survey 2019," 2019:** https://www2.deloitte.com/content/dam/Deloitte/es/Documents/riesgos/deloitte-digital-risk-survey.pdf
8. **Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Guidance on Internal Control: Internal Control—Integrated Framework," 2013:** https://www.coso.org/Pages/ic.aspx
9. **Gartner, "Magic Quadrant for Integrated Risk Management Solutions," July 2019:** https://www.gartner.com/en/documents/3947432/magic-quadrant-for-integrated-risk-management-solutions
10. **Deloitte, "Global Risk Management Survey," 2019**: https://www2.deloitte.com/bg/en/pages/finance/articles/global-risk-management-survey-2019.html
11. **Deloitte, "The people dimension of analytics," March 2017:** https://www2.deloitte.com/ca/en/pages/deloitte-analytics/articles/people-dimension-of-analytics.html
12. **Deloitte, "The future of operational risk management: Evolving data architectures," January 2019:** https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/predictive-analytics-in-the-operational-risk-framework.pdf

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.