Infosys®
Navigate your next

VIEWPOINT

RATIONALIZING CONTROL SYSTEMS TO MITIGATE RISK

Banks are at a crossroad. They must balance regulatory compliance while keeping costs in check. Using a control structure based on an agile risk management framework banks can achieve both objectives.

Infosys® | Knowledge Institute

Lax controls cost banks money. A lot of money. An astounding $20 billion was paid out by banks in the three years between 2012 and 2015, according to Bloomberg. And this was only for lax money laundering controls.[1] If total fines are considered, banks have paid out $321 billion in less than a decade leading up to 2016.[2] And money is not all they lose. Bank brands face a loss of reputation and of senior management, as heads roll through resignations after each compliance failure.

From the collapse of Barings Bank in the 1990s[3] to the "2010 Flash Crash" that dragged the Dow Jones Industrial Average down 9%,[4] the inability of banks to manage risks or criminality has had catastrophic impacts on institutions and the industry as a whole. Governments and regulators across the U.S. and Europe introduced numerous regulations and bodies that aimed to increase capital requirements, restrict bonuses paid to bankers, protect consumers and strengthen regulatory powers. Some of these include the Dodd–Frank Wall Street Reform and Consumer Protection Act, the Consumer Financial Protection Bureau, the European Banking Authority, the Housing and Economic Recovery Act, the European Securities and Markets Authority, and the European Insurance and Occupational Pensions Authority.

Control systems are designed to help financial institutions comply with regulations. Banks have adopted control systems that help track banking practices such as auditing standards, regulations and operations. Efficient control systems allow banks to operate at ease and act swiftly. When set up effectively, these systems help avoid erroneous activities, fraudulent transactions and banking irregularities. They act as a vigilant watchdog of the bank, helping foresee probable issues that could impact the bank and prevent or minimize any future losses. Lack of effective control systems exposes banks to risks and poses threats to their success.

Control systems hold banks back

But in many cases, control systems have gotten out of hand. They have become too complicated and onerous, often overlap, and are very expensive to manage. The past few decades have seen banks build multiple control systems to shore up their integrity. Within each bank's divisions — investment banking, retail banking, commercial banking — various control systems were created that were considered appropriate at the time but were no more than bandages for a bullet wound. These systems operate in silos and generally don't communicate with each other. Quite often, these control systems compete with each other and negate the objective of building risk-proof businesses and institutions. While certain risks are well understood, risks emerging from unorganized control systems are misunderstood and wrongly acted upon by the industry.

Within a bank, each business unit tends to treat control systems differently to suit their current requirement; some units consider their control systems strong, while others may consider the same control systems as an impediment that slows down their processes to deliver services or make informed business decisions. Existing control systems suffer from a host of other issues, including:

- **Duplication of risk and control.** Correlation, intersection and duplication of controls occur because of multiple, overlapping and conflicting lines of reporting and responsibility.
- **Bottom-up approach to control systems.** Control systems are treated equally regardless of the underlying risk profile. This leads to an inflated and inefficient structure that slows down an organization's decision-making ability.
- **Mapping.** Controls are often not designed at the optimum level and are not adequately documented. Furthermore, control systems versioning becomes slow as additional documentation is required, and it is difficult to obtain consensus from all users for the updates.
- **Review.** There is an absence of a continuous process to design and review control structures. Auditing control systems to reflect emerging business changes or issues is limited. Often, this knowledge resides within individuals, while organizations don't have a fair understanding of these systems, their usage and the impact of any breach.
- **Lack of standardization.** Control systems are not standardized. Many of them are developed on an ongoing basis, and the process through which they are deployed needs a second look.
- **Exposure to fraud consequent to control weaknesses.** Internal operations, people or external activities may compromise the effectiveness of control systems. Multiple ways of maintaining control systems can jeopardize how they are leveraged to manage risks.

While control systems are generally well defined for business-critical processes, trivial matters are often overlooked. For instance, providing an employee or external contractor with access to an application can result in a breach of security or increase the probability of internal fraud. This increases the importance of why each control system or procedure must be analyzed and understood to arrive at a robust framework and policies to govern controls.

One might think that multiple control systems increase a bank's robustness and enhance security. And yet,

multiple banks seem to continue to falter. In 2019, the European Union fined five large banks €1.07 billion for rigging the foreign exchange market between 2007 and 2013.[5] Back in 2012, the LIBOR scandal brought out the dark underbelly of large trading houses and resulted in banks paying over $9 billion in fines.[6]

According to United Nations estimates, the amount of money laundered globally in a year is between 2% and 5% of global GDP, or $800 billion to $2 trillion.[7] This is forcing banks to rethink their strategy on control systems. Rather than focusing on multiple control systems that operate in silos, they are looking at building a network of control systems that communicate with each other. Ultimately, the risk office needs to use control systems to gain an end-to-end holistic view of activities. This by its nature is a complicated and ever-evolving environment to map. However, "less" is increasingly considered as the new "more" in control systems design.

Rationalizing control systems…

Banks are rethinking how control systems can be redefined and rationalized. Their siloed approach to control systems does not provide an end-to-end view. Rationalization can help achieve that. It is a process of continuous improvement that analyzes existing controls and aligns the control structure with risk to improve efficiency and strategic effectiveness. All controls are not equal — some are more strategically important, while others mitigate significant risks. Controls must be analyzed and prioritized based on their objective, the level of granularity needed to provide assurance levels and the impact in case of their failure.

Control systems rationalization involves understanding how organizations are historically structured, how they continue to be structured and whether organizations can respond to day-to-day changes. This provides an understanding of how processes are laid out and helps organizations get attuned to the changing scenarios.

The risk office can be provided with an intelligent digital dashboard to allow them to have a holistic view of the entire gamut of control systems. This helps manage more with less, with a smaller team managing organization-wide control systems. A centralized control repository helps build a robust and agile organization that responds to changes much faster and in a linear fashion.

…through a dynamic framework

A control systems framework can be structured through a matrix of risks and impacts, as indicated in Figure 1. Different services need to be rated

Figure 1. Control systems framework – risks and impacts

Domain	Key services	Internal control system risk				External control system risk			
		People		Technology		People		Technology	
		Risk	Impact	Risk	Impact	Risk	Impact	Risk	Impact
Investment Banking	Research and sales	◐	●	◐	●	○	●	◐	●
	Trade execution	●	●	●	●	○	●	●	●
	M&A	●	◐	○	◐	○	◐	◐	○
	Asset servicing	◐	○	◐	◐	○	○	◐	○
	Underwriting and Syndication	◐	○	◐	○	○	◐	◐	◐
	Risk management and Corporate advisory	●	●	●	●	○	●	●	●
Wealth Management and Private Banking	Portfolio construction	◐	○	◐	○	○	○	◐	○
	Asset allocation	◐	●	◐	●	○	◐	○	◐
	Trade execution	●	●	●	●	○	●	◐	●
	Asset servicing	◐	○	◐	○	○	●	◐	●
	Tax management and Compliance	○	○	○	○	○	○	○	○
	Custody and Trust services	◐	●	◐	●	○	●	◐	●

○ Low ◐ Medium ● High

Note: Impact ratings are illustrative
Source: Infosys Limited

on their risks and impact levels by people and IT within and outside of the enterprise. Services that are generally considered high risk-high impact are those that pose a threat to the front office, those that support M&A and those that support accounting and portfolio strategy executions. For example, information leaked on M&A could be highly impactful as it could affect the reputation of the firm, have legal and compliance repercussions, and influence pre-merger discussions. Trading applications also hold sensitive client information. Securing them and having a well-thought-out control procedure and infrastructure are critical.

The framework is not sacrosanct. Control systems are always changing and are complicated by nature. Banks need to simplify them yet keep them flexible. Different activities carry different risk levels with different impacts at different points in time. Ratings can vary depending on how the cluster of applications is grouped in an enterprise and the tasks those applications perform. The framework provides a base to deal with risks in financial services.

The industry must assess their business towers, supporting applications and infrastructure to form an integrated plan of building advanced warning and risk-mitigating control systems.

Benefits of rationalization

Adopting control optimization can lead to significant benefits of an integrated compliance framework that improves the risk and control environment:

- Simplification and standardization of controls can lead to lower costs and improved operational efficiencies.
- Risk-based approaches result in enhanced effective and efficient risk assessment processes and better-aligned risk coverage through identification of key controls.
- Control automation and automation testing bring in efficiencies and lower the cost of compliance.
- Removal of control duplication brings in efficiency for testing and monitoring controls and higher reliance on the testing process.

According to Dr. Ashok Hegde, vice president at Infosys, "Control systems rationalization can result in 15% to 17% overall cost savings." He estimates that this would also reduce regulatory-related fines by 70% to 80%, as well as improve the brand of the organization as less time is spent in front of the regulator.

Six steps to success

Rationalizing control systems is a complex process that can take anywhere between nine and 14 months to complete end-to-end, according to Dr. Hegde. Indeed, the first four to five months are spent simply on documenting all the control systems and mapping their relationships out. Dr. Hegde outlines six steps to help banks rationalize their control systems:

Figure 2. Steps to help banks rationalize control systems

Step 1

Understand and view all processes. Assess or map control systems and document the whole process.

Step 2

Identify conflicting genres. Any conflicting controls are identified and rectified. This enables the organization to become more secure and improve efficiency.

Step 3

Identify complementary genres, where control systems supplement each other. This helps avoid unnecessary processes and makes the processes more robust.

Step 4

Club or consolidate control systems. Create a centralized dashboard of the control systems that can be managed on a day-to-day basis.

Step 5

Build a digital dashboard that provides insights into how control systems can be leveraged to mitigate risks and improve business agility.

Step 6

Set up governance. This includes a governance body for periodic review. The chief risk officer should oversee the governance function.

Source: Infosys Limited

Quicker, faster, stronger

Rationalizing control systems makes banks agile and helps them respond to changes more quickly. They can transform both from a cost perspective and a revenue perspective as this increases their capacity to take higher orders. Control systems should not be limited to identifying threats but should also recommend preventive measures. With the use of artificial intelligence and machine learning, many uncommon threats can be detected and reported in real time. While the financial services industry still has a long way to go, a new beginning has been made. With a more integrated and rationalized set of control systems, hopefully the financial crises of the past can be prevented in the future.

References

1. "Stung by Big Fines, Big Banks Beef Up Money-Laundering Controls," Bloomberg, April 4, 2019, https://www.bloomberg.com/news/articles/2019-04-04/global-banks-beef-up-money-laundering-controls-as-fines-sting
2. "World's Biggest Banks Fined $321 Billion Since Financial Crisis," Bloomberg, March 2, 2017, https://www.bloomberg.com/news/articles/2017-03-02/world-s-biggest-banks-fined-321-billion-since-financial-crisis
3. "Barings collapse at 20: How rogue trader Nick Leeson broke the bank," The Guardian, February 24, 2015, https://www.theguardian.com/business/from-the-archive-blog/2015/feb/24/nick-leeson-barings-bank-1995-20-archive
4. "The Human Touch in AI-Aided Trading," Infosys Knowledge Institute, June 2019, https://www.infosys.com/about/knowledge-institute/insights/ai-aided-trading.html
5. "EU fines Barclays, Citi, JP Morgan, MUFG and RBS $1.2 bln for FX rigging," Reuters, May 16, 2019, https://in.reuters.com/article/eu-antitrust-banks/eu-fines-barclays-citi-jp-morgan-mufg-and-rbs-1-2-bln-for-fx-rigging-idINKCN1SM16B
6. "Understanding the Libor Scandal," Council on Foreign Relations, October 12, 2016, https://www.cfr.org/backgrounder/understanding-libor-scandal
7. "Money-Laundering and Globalization," United Nations Office on Drugs and Crime (UNODC), https://www.unodc.org/unodc/en/money-laundering/globalization.html

Authors

Dr. Ashok Hegde
Vice President – Financial Services, Domain Consulting Group
Ashok_H@infosys.com

Samad Masood
Infosys Knowledge Institute
Samad.Masood@infosys.com

Aliya Patricia Rebello
Senior Consultant – Financial Services, Domain Consulting Group
Aliya_Rebello@infosys.com

Sharan Bathija
Infosys Knowledge Institute
Sharan_BP@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next