Compliance and Risk Management Transformation Part II: Making It Happen

By David Samuels
This article is co-authored by Brent Crider and Paul Kalamaras

Note: This is the second in a two-part series on transforming compliance and risk management to meet the pressing demands of today's financial services environment. In Part I, "Compliance and Risk Management Program Transformation: Why the Wait?" we provided an overview of drivers, obstacles, and strategies. Here we delve into tactics.

Banks are reluctant to embrace transformation. When will they finally effect the operational and digital transformation of their compliance and risk management programs? These are tough but fair questions, since the Institute of International Finance's (IIF's) global survey of bank CROs recently showed about half of them still defining transformation strategies.

As collaborators in compliance and risk management transformations at several banks, we recently wrote an article sharing our analysis of why banks need to go faster. In this piece, we share the solutions that have worked for us, by setting out the success factors, key questions, and essential ingredients for operational and digital transformation.

To repeat our top takeaway from the first article: No transformation, no growth. Financial services companies cannot keep increasing compliance and risk management staffing and costs to cover each new product, service, geographic expansion, acquisition, or regulatory mandate. The situation has become so unmanageable and costly that it hinders growth. Such is the fate of old-school, manual compliance and risk management operations.

On the other hand, operational and digital transformation elevates compliance to a higher quality, consistency, efficiency, effectiveness, scalability, repeatability, and regulatory integrity—enabling instead of slowing growth. Here's how to make it happen …

Success Factors: Timing and Leadership

Timing Is Everything

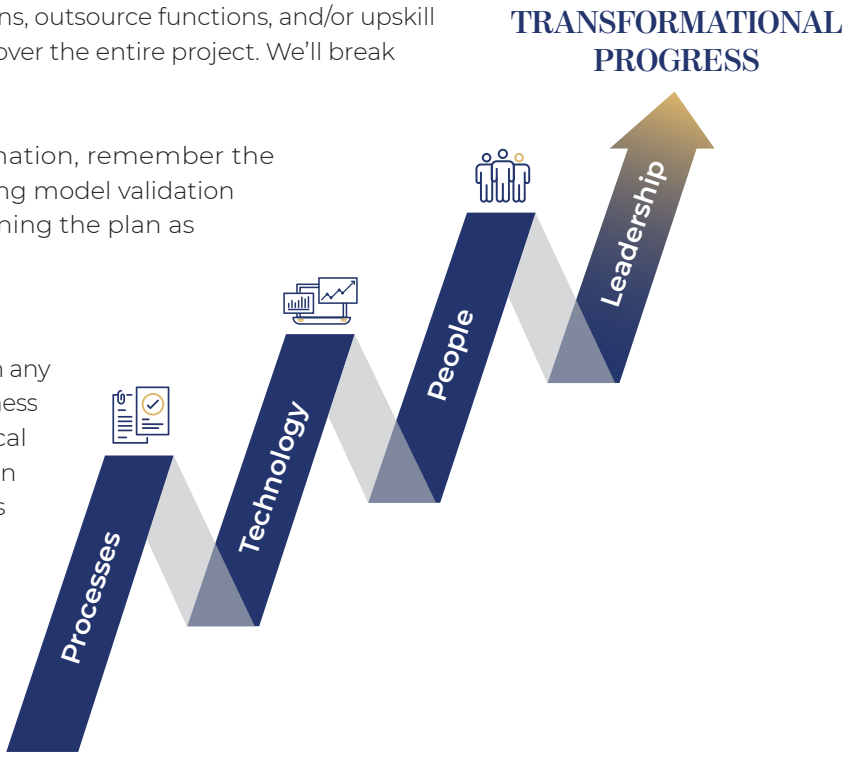
The time for transformation is now. Many of the biggest banks and leanest fintechs have already raised the bar by streamlining and automating their compliance and risk management. From a strictly competitive point of view, the risk of waiting any longer is too high.

Timing is also of the essence in the design of your transformation plan. One of the first essential questions to ask when modernizing your programs is how fast? There are two schools of thought: One says to "go big or go home," while the other calls for phasing in transformation. Each approach has its pros and cons.

For instance, a phased approach may be more palatable to the board and top executives who have to buy into the plan and help implement it company-wide. After all, transformation is hard work for everyone involved. But phasing can have unintended consequences. Cost benefits can take too long to materialize, for instance. With

nothing gained, the biggest risk is that "transformation fatigue" sets in as each new phase is introduced—ultimately derailing the plan. Alternatively, going big delivers cost and other advantages faster, while shortening the painful disruption that comes with any transformation.

Our advice is to go big if you can, but phase in if you must. Try to limit the number of phases and their duration, though. Think about phasing in the processes, technology, and people aspects of the plan. That is, streamline processes first, then upgrade technology to automate and analyze data, and then address the question of whether to eliminate staff positions, outsource functions, and/or upskill your people. And maintain a governance group over the entire project. We'll break down this structure later in the article.



Whether going big or phasing in transformation, remember the importance of setting milestones and conducting model validation at regular intervals. This sets you up to keep tuning the plan as needed and pivot when issues emerge.

Leadership Earns Buy-In

Transformation plans can face many obstacles in any organization, from a silo mentality in different business units to board-level wariness about technological risk to regulators' apprehensions. As our discussion of timing above points out, getting their buy-in is essential to the success of your transformation plan. Forging company-wide collaboration and regulatory partnership takes strong leadership on the part of CROs and CCOs—an attribute for which there is no secret sauce, but one that can be bolstered by taking the following steps:

- **Getting Regulatory Buy-In**

"The expectation is that regulatory change will grow in both volume and pace, yet the resources available to firms to manage that change will, at best, remain the same," according to a recent Thomson Reuters report. This is the context for any discussion of transformation with regulators. Because, as the report added: "Unless firms have the means to comply with them, regulations are just the evidence in an enforcement case."

Work closely with your regulators to get them on board with your transformation plan. Be transparent with them. Schedule regular meetings; we'd advise monthly. Describe how automated data collection and reporting can help banks comply more consistently and accurately with changing regulations. Share your transformation plan with regulators to avoid surprises, and use diagrams that clearly illustrate what you're doing. Don't neglect to describe the solid internal governance structure you've instituted. The goal is to build a more effective and scalable regulatory compliance program.

- **Getting Internal Buy-In**

We can best summarize how to get internal buy-in in three words: the business case. Of the many benefits of digital and operational transformation, key bank stakeholders are sure to focus most intently on cost takeout. In this regard, we've helped banks increase compliance and risk management productivity up to 50% by redesigning workflows, eliminating unnecessary steps, and implementing productivity tools.

With your business case in hand, establish close working relationships with IT, HR, legal, and other stakeholders—including them in weekly governance meetings. Use the same kinds of graphic presentations that you're employing with regulators to present your business case to your senior executives and the board. Your case can be further strengthened by working with external advisors on benchmarking against industry best practices and other types of analysis that require a broader view of the financial sector.

When discussing the business case, though, don't lose sight of this basic requirement: Cost-takeout cannot come at the risk of noncompliance. Any digital and operational transformation of compliance and risk management needs to take place within a culture in which all stakeholders prioritize compliance.

> "At the end of the day, you have no choice. In order to grow a business, you have to meet your regulatory obligations."—BRENT CRIDER

Key Questions: Eliminate, Automate, Outsource, or Staff?

To effect a transformation, four fundamental questions need to be posed across all areas of compliance and risk management:

- ***What to eliminate.*** Begin your transformation by eliminating redundancy and ill-conceived processes for quick wins.
- ***What to automate.*** Look at what remains, and streamline those processes with new technologies for efficiency, effectiveness, quality, and scalability.
- ***What to outsource.*** Consider using third-party, managed services to perform low-value-added processes, for cost containment and access to best practices.
- ***What to staff.*** Plan to retain and where necessary expand staffing, not only in higher-value roles such as analytics but also to oversee any outsourced processes.

Essential Ingredients: People, Processes, and Technology

Acting on your answers in the four areas listed above brings us to the classic triad of people, processes, and technology. As you move forward, you should be keenly aware of the intersections among the three, and address them in the following order:

Processes

Don't try to automate from scratch, because you may end up digitizing unnecessary, redundant, or otherwise flawed workflows. Instead, start by analyzing the accumulation of policies, procedures, and processes that have built up in your compliance and risk management functions over the years. Eliminate the unnecessary, streamline those that are essential, and only then proceed to automate, integrate, and/or upgrade with analytical capabilities.

> **"In one case, the BSA department had created a Frankenstein-level mishmash of policies, procedures, and processes based on several years of changing regulatory mandates. Our first step was to assess and to rewrite our documented workflows and procedures before beginning the transformation."**—PAUL KALAMARAS

Technology

Examples of the technologies you might then employ could include:

- Robotic process automation, to improve the accuracy and efficiency, including reducing time spent on redundant processes, of data input;
- Integration of data, gathered from multiple systems and displayed on unified dashboards; and
- Analytics, including machine learning and artificial intelligence (AI/ML), to recognize patterns in areas such as fraud detection to recognize patterns in areas such as fraud detection, mining large amounts of data and generating summaries, or conducting adverse media and internet research in a highly efficient manner.

People

Only after designing the new processes and their enabling technology should you look at the people on the compliance and risk management team. Consider eliminating positions that don't add value, whether because they involve manual, redundant processes or because their roles don't add unique value and might be better performed by third-party, managed services. Compliance outsourcing is on the rise, in the face of industrywide issues such as cost constraints and skills shortages, according to Thomson Reuters' global survey. Specifically, 38% of financial services compliance functions reported having outsourced at least some of their operations in 2023, up from 30% in 2022.

Staff restructuring comes with several provisos, though. For example, compliance leaders should look to upskill staff in low-value roles and, where possible, provide opportunities for alternative employment. Higher-level positions will also need to be added to ensure the compliance and efficiency of outsourced processes (upskilling opportunity?). Remembering that your organization is responsible for any non-compliance on the part of your managed service provider, plan to have solid third-party risk management in place for vetting, contracting, and monitoring them.

How to Get Started

Begin by asking yourself, what are the indicators that your compliance and risk management programs could benefit from transformation? The answer could come from several exercises—for example, benchmarking against best practices in the industry, identifying potential savings, mapping the potential regulatory implications of your bank's long-term strategy, or forecasting the next few years on the ever-changing regulatory landscape.

Then, map potential benefits to your goals, considering compliance first but also efficiency, effectiveness, quality, scale, and return on investment. Your business case and transformation plan should flow from there.

Transformations are big—there's nothing small about them. But our experience has taught us that the rewards can be commensurate with the effort. And the steps we've laid out here have proved effective in digital and operational transformations like the one you're contemplating right now.

This article was co-authored by:

Brent Crider

Brent Crider, Doctor of Executive Leadership, is a risk and compliance professional. Most recently he served as the Chief Compliance Officer at MoonPay. He previously served in multiple C-suite roles and has 35 years' experience in public and private institutions leading program enhancements. Brent's experiences range from creating organizations to improving and strengthening existing corporations to exceed performance standards. Dr. Crider retired from active duty in the U.S. Air Force after serving 20 years. He was a senior intelligence officer and served as the Director of the National Security Agency group at the U.S. Special Operations Command and spanning four continents. He is a Certified Anti-Money Laundering Specialist and holds advanced degrees in Economics and National Security and Strategic Studies.

Paul Kalamaras

Paul Kalamaras is a current community bank board member and the former Senior Executive Vice President and Chief Risk Officer at Investors Bank, a $25 billion asset commercial bank where he was responsible for the overall risk management of the company, including the credit, compliance, information security, BSA/AML, and enterprise risk functions and was a member of the bank's Executive Committee. Previously, he served in a number of executive leadership positions in middle market, retail, and business banking lines of business in several regional and community banking organizations.

Author

David Samuels

David Samuels, Treliant's Chief Executive Officer and a Senior Advisor to Vistria, the company's primary shareholder, is responsible for setting and executing the firm's long-term strategy and creating value for stakeholders. David is a respected financial services and fintech expert with over 30 years of experience. He has spent extensive time in Asia, Europe, and the Americas assisting financial institutions of all sizes with risk management, compliance, and operational efficiency matters, including applying intelligent workflows, outsourcing, and artificial intelligence to drive scale and optimization. **dsamuels@treliant.com**