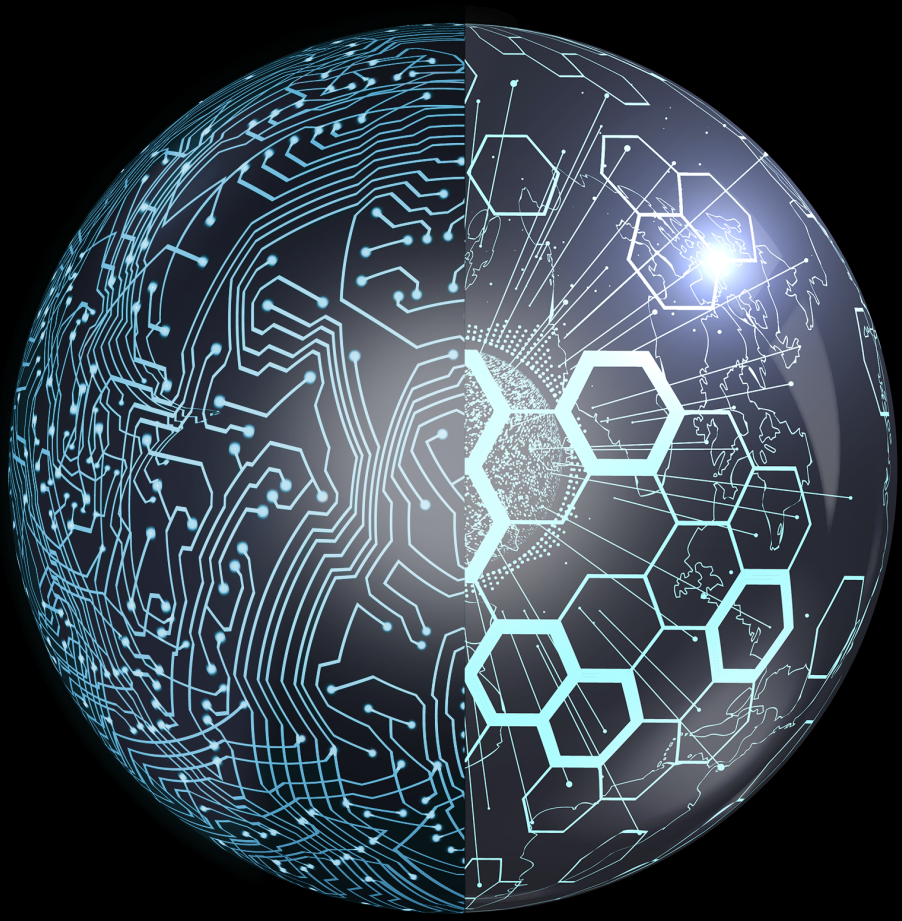
Deloitte.



Digital transformation for the risk and compliance functions

5 questions about the digital transformation for the risk and compliance functions

An interview with **Shuba Balasubramanian,** Principal, Deloitte Transactions and Business Analytics LLP

What is digital transformation? Marketplace definitions approach the question from a few angles. Is it deploying digital technology to improve efficiency and reach customers at every touchpoint? Is it a strategic reimagining of the business? Is it the end state of an organization with digital in its DNA?

Whatever way it is described, digital transformation is taking place throughout many organizations. However the process is slow going for many compliance and internal audit groups, groups that often are not part of the conversation. Identifying the barriers that compliance and internal audit face regarding digital transformation and understanding how to potentially overcome them can help these functions share in the operational benefits of technology innovation and join the digital sea change in how organizations operate.

Why are risk and compliance functions the last to find out about digital transformation?

Organizational leaders often see digital transformation as a path to grow the business, streamline operations, and strengthen customer relationships. Sales, supply chain, R&D, and other functions that directly impact profit and loss are deeply engaged in capturing transformation's return on investment (ROI). As a result, compliance and internal audit are often the last ones to hear about it.

Compounding the problem, compliance and internal audit groups may not yet grasp the speed and scope of digitization underway in the organization. Or, if they are attuned, they may feel more threatened than excited by technology's potential to change their work, or even replace them.

The lack of a direct communication line to the information technology (IT) organization can be another hurdle in compliance and internal audit transformation. As a result, compliance and internal audit are unable to capture IT mindshare as they pursue transformation, while technology developers risk overlooking potential vulnerabilities. Finally, the compliance and internal audit roles often involve checking other peoples' work and actions. Chilly receptions from other enterprise functions may come as no surprise.

What are enterprise risks of leaving risk and compliance functions out?

As organizations broaden their digital footprint with connected devices and other emerging technologies, their risk profiles change, both through more points of potential vulnerability and the increased threat of new cyberattacks. A lack of continuity and consistency among security initiatives in the enterprise can worsen these exposures. Absent the involvement of effective compliance and internal audit programs, hidden threats—some potentially dire—can remain undetected.

It is also possible that other closely aligned functions are homing in on digital transformation. The chief legal officer and chief integrity officer roles in particular might need to travel on somewhat parallel tracks with compliance and internal audit. Separate, disconnected initiatives can create unnecessary duplications, costs, and even additional vulnerabilities.

In the same vein, another risk to consider is financial. Should compliance or internal audit take the initiative to stand up a digital transformation program on its own, unnecessary expense may start to accrue if the technology resources needed for digital transformation already exist elsewhere in the enterprise.

What do risk and compliance functions risk by deferring digital transformation?

The short answer is potential obsolescence. When robotic process automation (RPA) can handle exponentially more transactions than humans, it follows that RPA may be leveraged to provide compliance and internal audit checks and balances. The bots have not taken over yet, but more companies are deploying them every year. Compliance and internal audit may have a closing window to move from traditional to digital models themselves. In the interim, inadequate digital capabilities could further weaken relationships between compliance, internal audit, and the rest of the business.

How can risk and compliance functions jumpstart their digital transformation?

First, don't feel overwhelmed. As noted earlier, compliance and internal audit may be able to benefit from transformation work already underway in the organization. Efforts to break down silos can start with strengthening communication and ties between the two groups themselves. For example, compliance can learn from internal audit's involvement in the governance, risk, and assurance aspects of enterprise resource planning (ERP) implementations, as well as the proliferation of internal audit-conducted RPA pilots.

Looking to the broader organization, some early bridge building to the CIO and the IT organization is imperative; nothing typically happens without their buy-in. In the longer term, if CIOs better understand the role of technology in compliance and internal audit, they will be more likely to keep such groups in the loop. Communication, as appropriate, with the chief audit executive, audit committee members, and financial executives is also a priority to help embed the business case for digital transformation of compliance and internal audit.

The digital transformation journey can begin with small pilots, perhaps focused on areas that require heavy manual rework. These trials can help compliance and internal audit learn how digital fits into their operations, as well as test drive the infrastructure.

What are some of the challenges risk and compliance functions can expect to face in the transformation process?

Lack of resources, both funding and skills, and accessibility to information are crucial issues. The continued view of compliance and internal audit organizations as "cost centers" rather than "strategic business partners" may prevail in some instances, causing delays in getting started. For example, compliance and internal audit need to keep up with what the business is doing in order to guard against and detect fraud and corruption. Yet the function is often challenged to obtain vendor, employee, and transaction data readily available to other functions, such as finance, accounting, procurement, and supply chain.

One development that is helping overcome this transformation barrier is the creation of integrated data layers (data lakes and the like) that enable various functions to draw data from different systems and repositories. Compliance, internal audit, and even the legal group could tap into this information just as other business units would do. For example, just as supply chain as a business unit explores pricing and sourcing options, compliance can analyze the data for evidence of price manipulation between vendors and buyers, an alarm bell of potential collusion. Such monitoring can also be extended to other threats, including controls weaknesses and potential fraudulent activities in payables, capital projects, travel and entertainment, and other areas.

Other problems may be averted by routinely bringing compliance and internal audit to the table for planning of analytics and RPA deployments. For example, the same data sets that are scanned for predictive analysis related to the maintenance of equipment can potentially provide insights into safety profiles, workers compensation fraud claims, safety incidents, contractual violations, double billing—the list goes on.

Finally, compliance and internal audit should view their hiring practices in a new light. Traditional accounting and auditing skills may still be needed, but backgrounds in business analytics and digital technologies will be of increasing importance.

My take

The days of utilizing only traditional methods to conduct internal audits, compliance testing, risk assessments, and investigations and oversight are ending. As digital technologies take on a larger role in the way organizations conduct their business, compliance and internal audit have no choice but to join in the transformation. It is essential to their evolution, and a vital component of an effective enterprise risk management framework.

For more information, contact:

Shuba Balasubramanian
Principal | Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
+1 212 840 1509
subalasubramian@deloitte.com