Deloitte.

An intelligent approach to unlocking value in service delivery transformation
Focus on risk from the start

A proactive approach can go a long way toward mitigating many of the risks associated with service delivery transformation before they proliferate and become costly to the organization.

Risk management functions[1] do not typically have a seat at the table as service delivery transformation (SDT) decisions are made. Instead, risk management for SDT is frequently handled in an ad-hoc manner, with an emphasis placed on risks that become apparent *after* the strategy has been defined and the transition is underway. In our view, we feel this approach needs to change. Dedicated risk management functions should be involved in developing the strategy for the transformation, providing governance over program execution and addressing risks related to current and future operations — right from the very beginning. This is a fundamental shift in mindset, and progressive organizations will want to waste little time in making it. Risks in the global market have become more volatile than ever. SDT requires discipline and focused attention so that unforeseen complications do not derail the transformation effort, costing the enterprise greatly in terms of regulatory noncompliance, lost value, operational failures and reputational damage.

Areas of escalating risk

A new, more-structured way to address the risks of transitioning to a service organization is quickly becoming an imperative as risks to the program, as well as those stemming from it, rise to new levels. Some common areas of escalating risk include:

- **Regulatory noncompliance** — An increasingly complex global regulatory landscape makes operating in new locations challenging. Laws and regulations in a particular country may be more or less restrictive than those currently applicable to the organization — and they are continually evolving. Cultural factors, particularly in emerging markets, can significantly affect how corporate policies are interpreted and applied in practice. For example, "pay-to-play" is culturally acceptable in China and in certain Latin American countries; however, laws and regulations including the Foreign Corrupt Practices Act and the U.K. Bribery Act explicitly forbid such practices, and the implications of inadvertently violating these statutes are severe. Thus, a detailed understanding of the legal and regulatory environment — both where it is and where it is going — is helpful, if not essential, when planning the SDT.
- **Reduced value capture** — One of the most common objectives of SDT is to lower operating costs. Cost-savings estimates are inherently uncertain, so it is imperative that models — including data and

[1] Risk management functions vary by organization. Common examples include Program Risk Management, Internal Audit, Compliance, IT Risk Management, Security, Privacy, and Third Party Risk Management.

assumptions used — are accurate and complete. Has the organization properly considered tax implications for the locations in which the shared service center might operate? Has labor arbitrage been correctly calculated, considering factors such as skill-set availability, training and local labor requirements? Equally important, how are these considerations expected to change over time? If certain variables are excluded or poor data is used to drive the decision-making process, the resulting financial repercussions can erode the transformation's value.

- Operational challenges — Decreased service quality is a common pain point in SDT. If the service organization supports internal business partners, poor service handoffs can cause internal friction, or worse, operational gridlock. If the service organization interfaces with outside customers, the company's reputation may be at stake. Understanding service risks early in the planning process and actively working to counter them throughout the transformation can mean the difference between consistent service levels and temporary, or even longer-lasting, declines.
- Security and privacy concerns — Operating in new locations, or with new technologies, exposes the organization to risks concerning data security and privacy. Therefore, it is critical to understand the types of data being handled and any cross-border data flows, as well as location-specific laws and regulations and the legal ramifications of a breach. For example, if personal data or health information will be collected, it may be subject to certain laws and regulations such as the European Union (E.U.) Data Protection Directive or U.S. federal and state laws. If intellectual property or tradecraft is being handled, it is important to be aware that many countries, including Brazil, Russia, China and India, do not afford strong legal protections for such information. In these instances, and particularly if new technologies and interfaces are to be installed, the organization will want to establish able safeguards to address these risks.

Although each area of risk has the potential to affect each organization differently, the overall implication is that today's complicated risk environment, if not managed effectively, can threaten the viability of the transformation and the realization of shareholder value. For many business executives and service organization leaders, navigating these multi-faceted risks will require a whole new perspective on risk management as it relates to SDT.

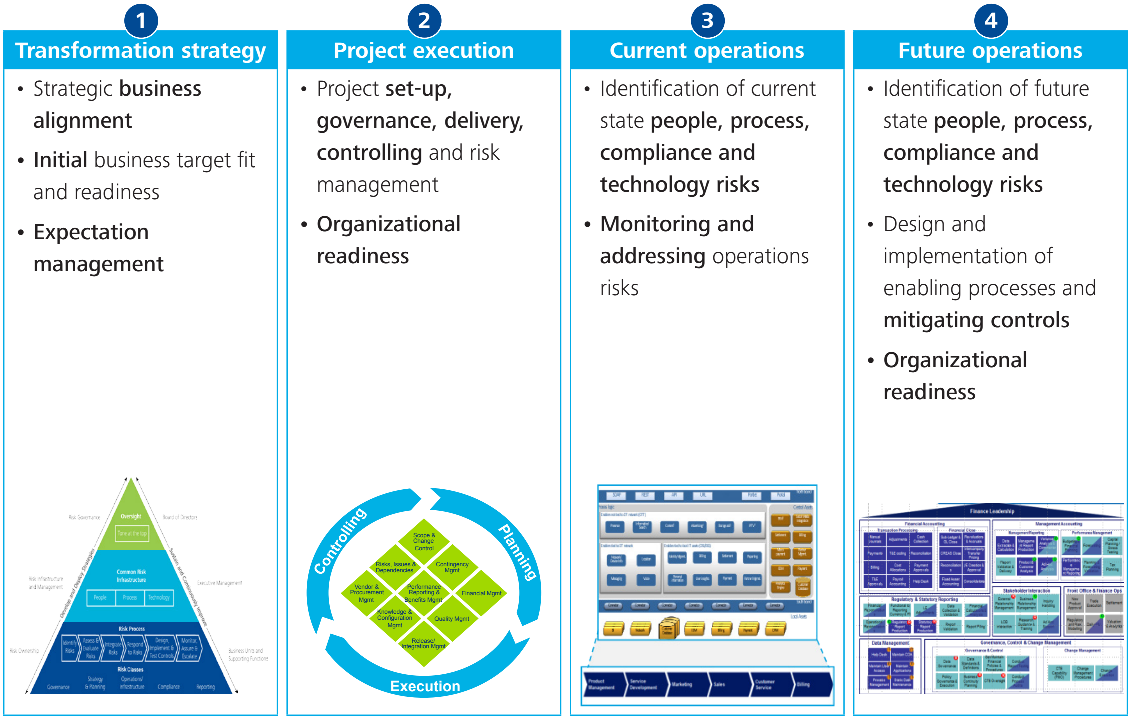
A new perspective is needed because the previous mindset was typically reactive: Decisions were made, the transformation was rolled out, and when the results were assessed, it was often discovered that financial and operational value was less than anticipated. Furthermore, when compliance functions or internal audit groups performed assessments, it was sometimes found that the new shared service organization had compliance gaps, and associated internal controls did not always align to the company's expectations about control and risk management.

In comparison, a proactive mindset is needed today: This new stance demands that a dedicated risk management workstream be defined and included as part of the program from the outset in an effort to identify and mitigate risks before they create a domino effect, rippling throughout the program and the enterprise. Furthermore, this workstream typically should be carried out by a dedicated risk management function (i.e., an individual or team), who can work alongside other program teams, such as finance restructuring, relocation and IT-enablement. If a service delivery transformation doesn't have a dedicated risk management function, program sponsors should engage one, either by drawing upon internal resources, or by sourcing them externally. For instance, a risk management team may include representation from compliance, internal audit, enterprise risk management, IT security, purchasing governance, etc. Its composition will depend on how the organization is structured, but the main idea is to have a cross-functional risk voice present from program inception.

The risk management workstream and the four risk dimensions

Once the risk management team is assembled, the question becomes: What will it do? Simply put, the charge of the risk management function within the new risk-management mindset is to proactively consider risks to the transformation as well as those resulting *from* the transformation. Deloitte's risk management methodology groups these risks into four dimensions: transformation strategy, project execution, current operating model and future operating model.

The four transformation risk management dimensions



1 Transformation strategy

- Strategic **business alignment**
- **Initial** business target fit and readiness
- **Expectation management**

2 Project execution

- Project **set-up, governance, delivery, controlling** and risk management
- **Organizational readiness**

3 Current operations

- Identification of current state **people, process, compliance and technology risks**
- **Monitoring and addressing** operations risks

4 Future operations

- Identification of future state **people, process, compliance and technology risks**
- Design and implementation of enabling processes and **mitigating controls**
- **Organizational readiness**

For each of these dimensions, the risk management team should have input into the following:

- **Transformation strategy** — This dimension examines the risks associated with transitioning a particular function to a service organization. It takes into account the risk appetite of the organization considering the full portfolio of programs currently in-flight and planned for the near future. In aggregate, these programs could increase the risk associated with the transformation. It also includes whether the decision to migrate a specific function aligns with the company's macro strategy, and if so, whether the function is ready to be moved. For instance, if the company's macro-strategy is growth by acquisition, then it might not make sense to harmonize certain areas, such as legal, which may have different requirements among country locations and operating units. However, other functions, such as accounts payable (AP) or human resources, may align with the growth-by-acquisition strategy depending on the degree of control desired. Forcing an inappropriate function

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

to be moved to a service organization could impede execution of the company's macro-strategy, as well as jeopardize the achievements of the transformation program. In other words, regardless of the specific strategies involved, the idea is to assess risks at a strategic level before decisions are made.

If a function is deemed to be in alignment with the company's overall objectives, the risk management team should then focus on evaluating its readiness to be migrated to a service organization environment. For instance, the AP function may be appropriate for shared services, but if it has recently undergone a major systems implementation, then it may not be ready. Timing should also be considered. For instance, if the company is about to make a strategic acquisition, resource constraints could pose a significant risk to the SDT. While these influential factors may seem obvious, they often go unnoticed. In order for them to become apparent, the organization should step back and test the proposed plans through a risk management lens.

- **Project execution** — The scope of this dimension encompasses identifying, tracking and reporting the risks to the transformation program after a company has decided to move a function to a service organization model. Importantly, while this dimension is more tactical in nature, it goes well beyond the purview of the Project Management Office (PMO).

  Many companies and external providers already have methodologies for understanding the risks associated with the execution of project tasks; nonetheless, risk indicators are often overlooked due to preoccupation with intense daily demands. That's why a dedicated risk management function, which is independent of day-to-day managerial oversight of the transformation program, is typically needed to identify, track, prioritize, monitor and escalate important program risks. Benchmarking SDT risks to the risk profiles of similar, large transformational initiatives is an important tool in this process. A clear line of communication to executive management is also key. In order to be effective, the risk management function should consider being able to communicate the appearance of "yellow warning lights" to executive leadership in a manner that is not filtered, biased or watered down.

- **Current operations** — The purview of this dimension is to identify the risks to the current operating model posed by the transformation, including impacts upon people, process and technology. What do these impacts look like? Day-to-day operations can be adversely affected as employees shift their focus to transformation activities. This can manifest as missed compliance or financial reporting metrics, customer or vendor dissatisfaction, or poor performance against other important measures. Increasingly, a risk management workstream, along with the added level of scrutiny and governance it provides, is needed to make sure employees don't "take their eyes off the ball" as the transition progresses because they're too focused on the future.
- **Future operations** — This dimension focuses on identifying the people, process, compliance and technology risks associated with the future state. As a result of the transformation, the company will appear fundamentally different. Accordingly, the risk management workstream should include process modeling of what the future state will look like. Once the risk management function has a firm understanding of the future state, it can then think about the risks associated with the new service organization environment across multiple dimensions. Examples include:
  - Financial statement risk — Is the organization prepared to capture all of the information it needs to comply with new reporting requirements?
  - Technology risk — How will the organization's systems and interfaces change, and what are the implications to system security?
  - Operational risk — How will the organization assure that processes are well-integrated and service levels are maintained?
  - Resource risk — How will the organization train, manage and incentivize its people to promote performance and retention?
  - Regulatory/Compliance risk — Is the organization prepared to meet compliance requirements and maintain a cost-effective compliance program?
  - Value risk — How will the service delivery organization be governed to meet cost-reduction targets now and in the future?

The main objective across all four of these dimensions is to figure out where the risks are and then to design mitigation strategies. Importantly, it is neither possible to eliminate all of the risks, nor is it necessary to overspend on addressing them. Instead, it's about identifying, understanding, managing and mitigating them in a cost-effective way.

Proactive is practical

The norm in service delivery transformation today is to deal with risks as they arise during the course of the program. Deloitte's experience suggests that few companies have a holistic understanding of risks across the four transformational dimensions, and fewer still take proactive steps, such as defining a risk management workstream or engaging risk management functions to manage risks starting at program inception. This situation is fast becoming untenable. A reactive, piecemeal approach is increasingly becoming inadequate as the stakes associated with strategic misalignment, operational failures, cost overruns, security and privacy concerns and regulatory non-compliance increase. Shared services leaders, however, do not have to wait for large budgets to be allocated in order to proactively address the risks to and from their programs. A fundamental shift in mindset can go a long way toward mitigating many of the risks associated with service delivery transformation before they proliferate and become costly to the organization. The first step in making this shift is to engage an individual or team to think about risk in a more-structured way prior to embarking on the journey.

Contacts

David Hodgson
Partner
Deloitte & Touche LLP
+1 973 602 6869
dhodgson@deloitte.com

John Conrad
Senior Manager
Deloitte & Touche LLP
+1 215 246 2383
jconrad@deloitte.com

Bryan Calvet
Senior Manager
Deloitte & Touche LLP
+1 215 405 7664
bcalvet@deloitte.com

Susan Hogan
Principal
Deloitte Consulting LLP
+1 404 631 2166
shogan@deloitte.com

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.