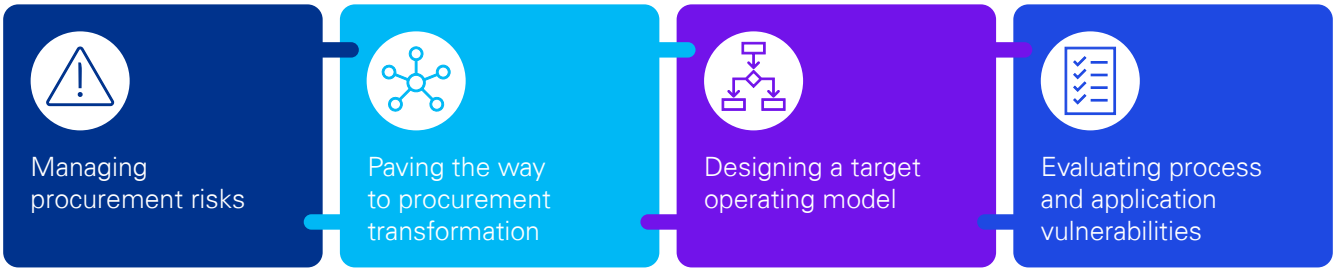
Harnessing the power of procurement transformation to enable stakeholder trust

KPMG Application Risk webcast insights

Comprehensive internal controls can help procurement organizations have a balanced performance process, develop strategic relationships, and drive operational efficiencies.

Our August 24 Application Risk webcast focused on managing risk and compliance in the procurement function and designing a target operating model for a procurement technology's security and controls framework.

The panelists addressed the following topics:



Managing procurement risks

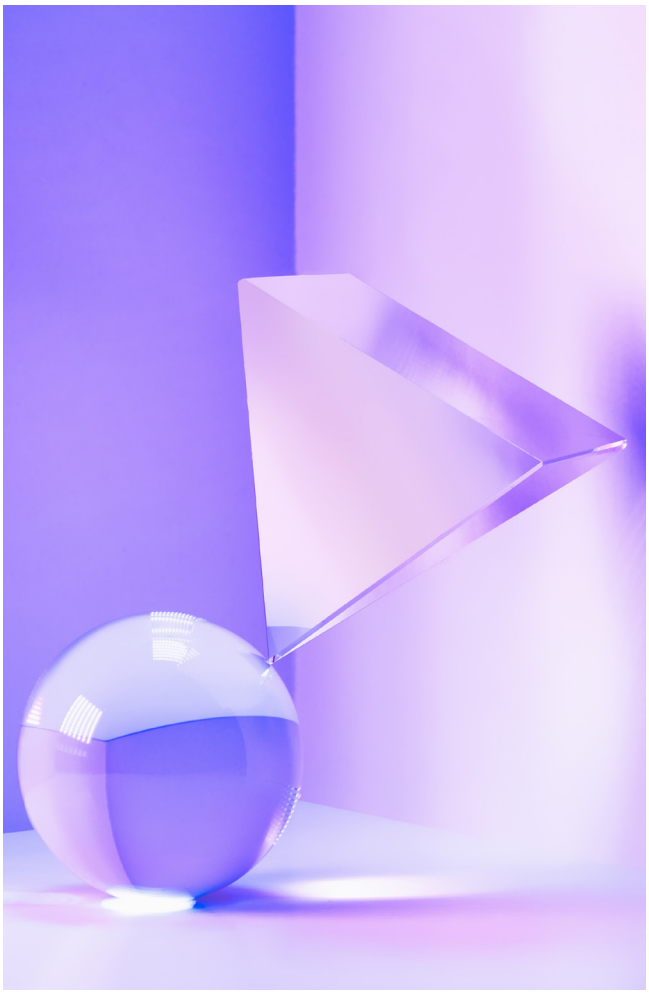
The role of the procurement function is changing—from simply managing costs to one of adding value, managing security, and building more strategic relationships. Well-defined procurement processes and applications can help businesses manage their supply chain and associated risks more efficiently while ensuring an optimal bottom line. With increasing geopolitical instability and unprecedented disruptions, organizations are seeking to reimagine their procurement function to act as a strategic lever to enhance resilience and to better respond to shifting market dynamics.

However, like any other business function, procurement is not immune to fraud and corrupt practices, posing significant risks to the financial and reputational health of firms. Mitigating the following operational risks is crucial to optimizing the function and driving value:

- Inaccurate internal needs assessment can lead to inadequate budgeting—resulting in either a significant overspend or underspend—paralyzing an organization's ability to move forward efficiently
- Intentionally defrauding an organization or the government with counterfeit invoices or manipulated bid documents

- Implementing technologies without having the right controls and security checks in place around segregation of duties and authorization and access to information, which can lead to cyber attacks
- Lack of overarching controls across business processes, such as budgetary versus actual controls, or lack of materiality can lead to disastrous financial consequences and compromised process integrity
- Other risks, including conflict of interest, inaccurate forecasting, manual processes, theft, and unethical sourcing, can potentially lead to significant losses for businesses.

It is imperative for leaders to understand these procurement risks to flag and mitigate them in time. With mounting pressure on procurement organizations to do more with less, there is an increased urgency for procurement to fundamentally evolve from a transactional back-office function into an agile, forward-looking function, which is data and technology driven and focused on maximizing process efficiency and quality, ensuring compliance and responsible spending, and bolstering stakeholder trust.



Paving the way to procurement transformation

Information technology business transformation can help rethink the procurement function, allowing it to take on greater strategic responsibilities and shift its reputation from cost-cutting to customer-centric and business-enabling.

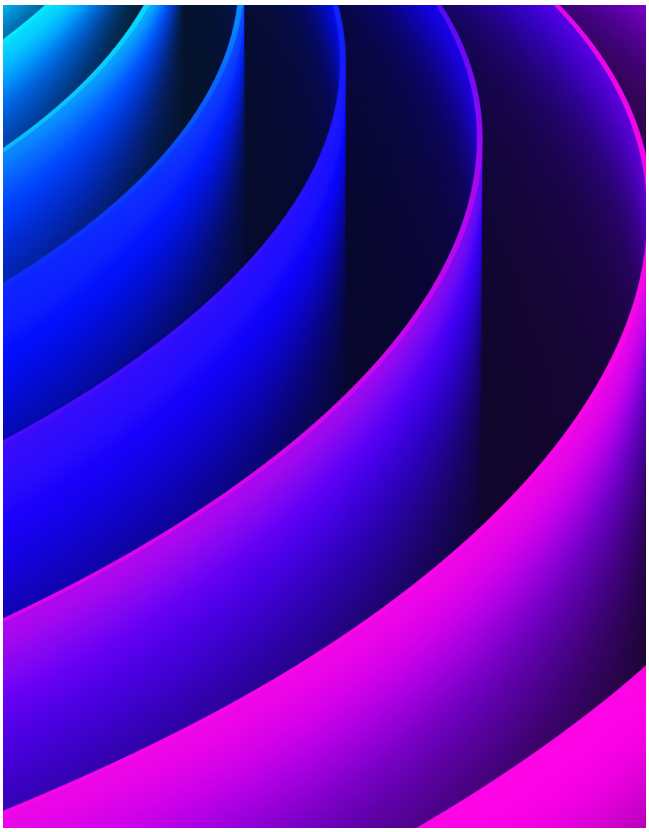
Procurement transformation initiatives effectively realize their business case goals when the application risk and compliance workstreams are keenly focused on deploying solutions that balance user enablement with the need to protect transactions and data while complying with all industry and regulatory requirements. This fundamental shift will require a reimagined operating model based on three key pillars:

- Roles: It is crucial to have clear accountability for security roles that highlights the privileges for a role to manage user authorization and drives ownership and collaboration. Ineffective role lifecycle management often leads to data corruption, making it difficult to detect and prevent fraud. Separation of duties is important from a risk perspective as it ensures oversight and prevents one person from taking responsibility for conflicting tasks.
- Controls: As organizations continue to innovate and evolve, internal controls should be designed and embedded at the earliest stages of the transformation lifecycle. Automated controls can help businesses streamline their procurement processes and uncover the reasons behind aberrations to proactively address control gaps through data-driven vigilance. To begin, organizations must assess their current state and desired future state, identify associated risks, and determine the technology required to support the process. IT controls such as IT application controls and IT general controls can enable businesses to manage operational risks, comply with regulations, and ascertain integrity and accuracy of information. Continuous controls testing must be embedded in the transformation lifecycle and is crucial to help prevent irregularities and confirm the effectiveness of internal controls.
- Change governance: To be successful in the transformation journey, effective change management is just as crucial as roles and controls—one that's versatile, interactive, and constantly testing. A well-managed change governance process ensures that all stakeholders are in the loop from the start regarding what needs

to be accomplished. With companies increasingly migrating to cloud, application updates are rapid, unlike the legacy systems. Change governance helps closely monitor these changes to test and respond to them and validate if they are aligned with business priorities.

Designing a target operating model

- To remain safe in a cloud-centric environment, organizations need to apply security controls across all their applications. It is crucial to apply a cross-application view of on-premises and cloud application security and controls. A modern cloud-based application integrates the following layers into a single, cohesive program:
  - End-point security protocols that help detect and prevent malicious attacks
  - Network security that consists of cloud security protocols
  - Authentication mechanisms such as multifactor authentication that help ensure only authorized users gain access to it
  - Application security that consists of defining roles, designing and testing controls, and building governance models with applications to strengthen security
  - Data security that focuses on securing data going into and out of an application, or potentially getting stored externally
  - Finally taking a holistic approach to monitoring and response processes.
- In order to create a risk mitigation program for a single application, it is important to have a Target Operating Model (TOM) closely integrated with the functional processes, people, technology, and an underlying governance framework, providing direction for cross-functional teams to collaborate and secure the application.
- As organizations build their TOM and define their compliance and controls program, it is crucial to understand the shared responsibility model. It dictates the security obligations of cloud providers and users to ensure ownership and accountability. While the onus for security is shared between the provider and customer, the distribution of responsibilities varies depending on cloud models such as SaaS, PaaS, and IaaS.
- From a SOC 1 reporting standpoint, it is important to understand what controls are effective within the service organization and how these controls can be supplemented. SOC 1 reports examine the financial risks and internal controls specified by a service provider. There is a dedicated section in the report that discusses the requirements for establishing the controls framework from a user organization. Hence, it is critical for IT and management to understand the control required to design an informed and effective controls framework. Often, cloud applications are too reliant on service providers to manage configuration changes that drive how automation works within your enterprise resource planning systems. It is important for process owners to identify these changes and review modifications to application functionality.
- External auditors are rapidly evolving their audit methodologies to address the unique cloud application requirements. While different firms have similar goals associated with Public Company Accounting Oversight Board standards, the individual audit teams tend to prioritize their application-specific scope to support their client-specific audit approach and methodology. Implementing automated controls at the start of the transformation journey makes the auditor discussion easier for procurement organizations.



Evaluating process and application vulnerabilities

Transformation assurance is an essential component of effective governance, providing forward-looking insights on existing issues and emerging risks that support the program's delivery of expected business outcomes:

- Prior to migrating to cloud applications, organizations should evaluate their processes and vulnerabilities and develop an assurance plan that is both periodic and aligned with application changes.
- Software development lifecycles, IT controls, authorizations, and change governance must be reviewed on a periodic basis along with the ability to manage changes holistically across environments.

Closing comments

A transformed procurement function can manage risk, enable businesses to be agile, and make informed business decisions, elevating the procurement function from an administrative function to trusted partner. While digital technologies can enable a stronger procurement capability, smarter procurement processes enabled by a robust controls environment can help businesses realize value, enhance the bottom line, and make businesses more resilient to future business disruptions.

Learn more:
visit.kpmg.us/RiskAssurance

Contact us

Laeeq Ahmed
Solutions Leader,
Application Security and Controls
KPMG LLP
T: 818-227-6032
E: laeeqahmed@kpmg.com

Niranjan Haridass
Managing Director,
GRC Technology
KPMG LLP
T: 267-256-1683
E: nharidass@kpmg.com

Alina Steenerson
Director,
GRC Technology
KPMG LLP
T: 612-305-5010
E: asteenerson@kpmg.com

Kevin Laird
Director,
GRC Technology
KPMG LLP
T: 310-663-5386
E: kwlaird@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia