KPMG

Identifying risk in your application portfolio

September 29, 2022

The traditional view of risk management is undergoing a transformation of its own, with leading companies increasingly seeking a forward-looking risk intelligence approach that more accurately quantifies potential threats, allowing businesses to better prioritize, fund, and allocate mitigation resources.

The webcast highlights the risks across the expanding applications landscape and ways to effectively balance the divergent task of leveraging modern applications to empower business users, while simultaneously protecting sensitive data and transactions.

The panelists addressed the following topics:

Understanding the evolving digital landscape

Digital innovation is driving new growth. With the ever-expanding digital landscape and advancing technologies, leaders are seeing an accelerated need for point-in-time solutions, different access mechanisms, and data centers in the cloud, making the risk landscape more dynamic.

Technology has grown in leaps and bounds over the last few decades—from legacy systems to the digital era—largely led by the transition to cloud, mobile, and the rise of data, which further accelerated the growth of artificial intelligence (AI), internet of things (IoT), and now remote working. Diverse options bring with them risk perspectives that organizations may not have considered before.

What is changing?

- As a result of the expanding application landscape, organizations are rapidly moving toward modernizing and improving their application environment. Business management software was traditionally reliant on single a vendor. Today, more and more companies are adopting best-of-breed cloud applications to handle their business-critical operations, including financials, customer relations, and human capital management.

- Leaders are focused on establishing a well-integrated data ecosystem, by driving front-, middle- and back-office transformation. The worldwide spending on enterprise application software is expected to grow 7.5 percent, while demand for a remote workforce remains strong.
- Technology vendors are offering wide-ranging solutions to fix business-driven financial processes to be more effective and keep track of cyber incidents. Although the digital ecosystem can enable better application and cybersecurity, it is equally critical to prioritize the information required and validate if the system is the right fit for your organization's application portfolio.
- While technology is undoubtedly fundamental to an organization's growth strategy, it can be challenging to manage risks and compliance as you grow your application portfolio. An integrated application ecosystem is key to synchronizing data in real time and enable effective security controls.

Outcomes of digital transformation

From strategy to tech enablement to cultural change, digital transformation helps firms take a holistic view of how processes, platforms, and behaviors across the front-, middle-, and back-offices need to evolve—and offers clear methodologies for executing that transformation. Implementing a robust technology strategy can effectively support business imperatives including increasing customer centricity, improving efficiencies and agility, enabling automation, and modernizing to gain a competitive edge. Here are some of the ways technology strategy and transformation is helping companies define value and innovation:

Collaboration and messaging: Instant messaging has changed the landscape of interactions between people sitting across the globe.

Automated processes: Automation has replaced manual, repetitive, and recurring tasks to enhance efficiency and reduce errors.

Global search: Users are able to conduct internet-wide searches to find what they need quickly.

Integration calendars: User applications can be automatically synced with future calls and meetings using an integration calendar.

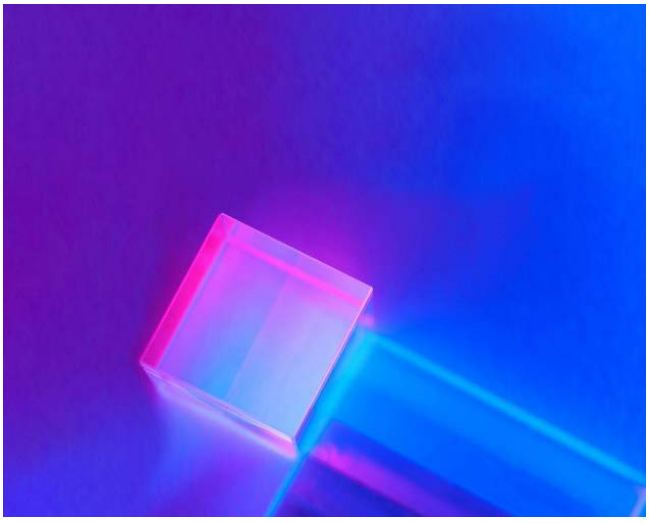
Fit-for-purpose/process-driven dynamic applications: A fit-for-purpose framework gives organizations the ability to know where to spend their time and resources.

Cloud information repositories: Digital repositories eliminate the need for on-prem data centers, offering anytime, anywhere access to data, enhanced visibility, and improved security.

Orchestrated workflow: Workflow orchestration helps organizations automate and scale their business processes to ensure productivity and manageability.

Cloud office applications: Cloud-based digital platforms improve collaborative working and enhance productivity while reducing costs.

In the new reality, consumer experience thrives on digital transformation—while encompassing all touchpoints, both physical and digital—enabling actionable intelligence, and offering ease of use and faster fulfillment. Today, it is no longer sufficient for risk professionals to monitor or mitigate risks, but rather to streamline risk processes. Control relevance is one of the key outcomes of digital transformation. Leaders must leverage the expansion of the technology and risk landscape to continuously evaluate how they conduct control tests. This will enable them to seize opportunities to optimize while reducing the cost of compliance.



Application portfolio risk and compliance considerations

Technology is undoubtedly a powerful engine of business growth. The irony is that the same innovations have also dramatically expanded the risk landscape, with everything from increased customer data exposure to a growing reliance on third-party, cloud-based service partners.

Large organizations today have a portfolio of custom software applications they use to run their businesses but struggle to keep up with the volume of security work that is involved. The following considerations can help companies understand their application portfolio and build a tailored plan to streamline risks:

- Ensuring the employees have necessary tools to accomplish their work
- Monitoring your spending on enterprise applications, particularly from a risk perspective
- Understanding the shard responsibility model
- Navigating evolving the regulatory landscape and ensuring compliance
- Identifying the risks associated with your application portfolio
- Closing the digital transformation gap with the right resources to manage your application portfolio

Understanding your application inventory journey

Business process enablement: The product-led approach of many organizations prevents them from maximizing application investments. Digital investments must always be business led and technology enabled at the core. Technology deployment—whether implementing automation, ERP and cloud, RPA, or data and analytics—needs to meet critical business requirements and must be tied to an actual business function, such as core finance processes or service delivery models, to determine how to derive return on investments and ultimately, create value.

Application inventory: Take careful inventory of the current technology landscape to ensure there is a consistent enterprise technology taxonomy and framework to build from as well as a clear view of all assets and any related controls.

Digital user experience: User experience is a key determinant of technology implementation and acceptance. Many companies fail to align and evaluate their application portfolio appropriately to optimally enable their employees. Prioritizing investments in people is critical for unlocking new capabilities, followed by the technology lens. It is important to train people to address change and to empower them to operate the systems efficiently.

Analyzing costs: As organizations evolve and expand their use of applications, it becomes challenging to keep track of the long list of applications and their purpose. Knowing your application inventory will help you determine where you can consolidate and where you can reduce control testing and evaluate the associated compliance costs.

Understanding the shared responsibility model

As organizations build their Target Operating Model (TOM) and define their compliance and controls program, it is equally important to understand the shared responsibility model. It dictates the security obligations of cloud providers and users to ensure ownership and accountability. For every application in your portfolio, you should determine what your responsibility is based on this model. While the onus for security
is shared between the provider and customer, the distribution of responsibilities varies depending on cloud models such as on-premises, SaaS, PaaS, and IaaS. Moreover, with PCAOB demanding firms evaluate their source codes for application controls, it is critical to ensure that change governance models align with the shared responsibility model.

Application risk and compliance considerations

- Auditors are getting better at assessing the evolving digital landscape and are expanding the list of "in scope" applications (IT General Controls, Separation of Dutys, and application controls). Hence, having open and routine conversations with your specific external auditors is critical. While the different firms have similar goals (often associated with PCAOB standards), the individual audit teams tend to prioritize their application-specific scope to support a client-specific audit approach and methodology. Key areas of focus include process controls, change governance, IT application controls, SOC 1 and 2, access controls, and SODs

- Often, cloud applications are too reliant on service providers to manage configuration changes that drive how automation works within your ERP systems. It is critical for IT and management to understand the controls required as a user to design an informed and effective controls framework from a SOC 1 and 2 reporting standpoint.
- Front-, middle-, and back-office applications are priority targets for fraudsters and cybercriminals (Denial of Service, ransomware, and data theft).
- To be successful in the transformation journey, effective change management is just as crucial as roles and controls—one that's verbose, interactive, and constantly tested. 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 the cloud, application updates are quick, unlike with legacy systems. Change governance helps closely monitor these changes to test and respond to them and validate that they do not affect the effectiveness of controls framework.
- IT controls such as IT application controls (ITACs) and IT general controls (ITGCs) can enable businesses to manage operational risks, comply with regulations, and ascertain the 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.

Cross-application considerations

To remain safe in a cloud-centric environment, organizations need to coordinate across multiple cloud applications. Business, technology, and risk and compliance teams need to retool the fundamental elements of their cross-application security & controls program to better support the risk presented by the increasing use of cloud applications. Some of the key cross-application risk considerations are:

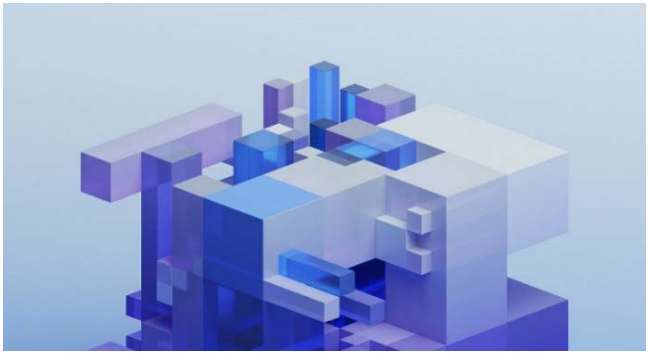
- Information doesn't stay on one platform, it travels from one application to another.
- As organization's application portfolios become more complex, it becomes more challenging to manage user access.
- It becomes increasingly challenging to have the talent and knowledge to manage risk across your application portfolio.

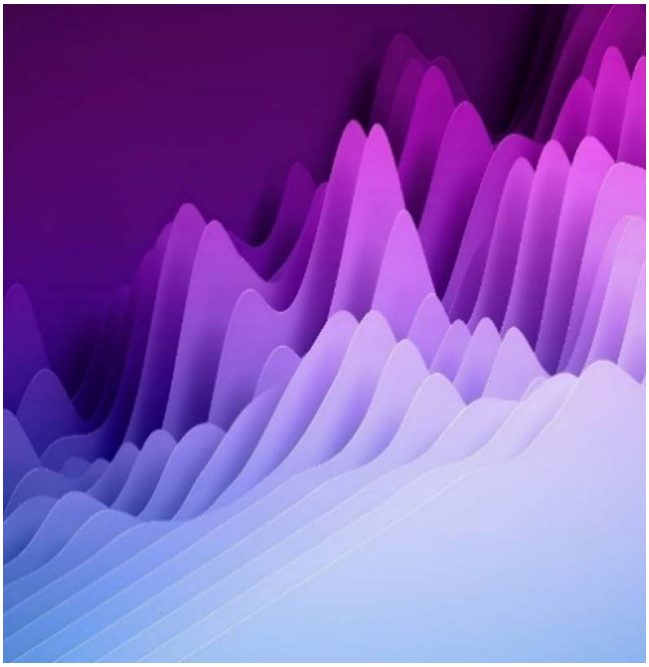
As organizations traverse applications, they need to build security controls program and compliance program across those applications. Separation and segregation of duties (SODs) are, in fact, one of the biggest considerations for application security. It ensures that a single person or entity does not have all the authorizations to do a complete end-to-end financial transaction process. Implementing technology with the right controls and security checks in place around SODs and access to information is key to mitigating cyber risks.

Best Practices for application portfolio management

Companies must evaluate their application inventory and perform regular risk assessments to understand risk and evaluate opportunities for optimization.

- **Risk evaluation:** To begin, organizations must assess their current state and desired future state and identify risks associated with compliance requirements within their application portfolio.
- **Controls effectiveness:** Migrating to a new application involves understanding which controls are affected, whether you have appropriate controls in place to mitigate risk, and whether there is a possibility of reducing manual controls.
- **Implementing security:** Certifying periodic access and provisioning access to a future system are two major security considerations companies often neglect. IT controls, authorizations, and change governance must be reviewed on a periodic basis along with the ability to manage changes holistically across environments.





Learn more:
visit.kpmg.us/RiskAssurance

Closing comments

Applications with robust security frameworks identify and mitigate application-level vulnerabilities proactively, thereby increasing the application's overall security posture through timely remediation procedures. It is critical that organizations perform regular assessments to ascertain the likelihood or impact of a risk caused by threat and vulnerability exposure across each application. Some applications may need more scrutiny than others because they may carry higher levels of risk exposure relative to other applications within the business. While the ever-expanding digital landscape can unlock capabilities, secured application portfolio enabled by effective controls can help businesses realize value and make them more resilient to future technology disruptions.

Contact us

Christian Leva
Managing Director,
Application Security and Controls
KPMG LLP
T: 214-840-2000
E: cleva@kpmg.com

Tristana Flores
Senior Associate,
Advisory Business Development
KPMG LLP
T: 720-573-7000
E: tristanaflores@kpmg.com

Brian Jensen
Managing Director,
GRC Technology
KPMG LLP
T: 817-946-9552
E: brianjensen@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