How controls integration has been impacted by transformation and digitization

Nine keys to enhancing the controls integration process

As businesses plunge full speed ahead into the age of digital transformation, journeys to the cloud and automated testing with bots, maintaining technological integrity and control over data, IT and operational security has become more challenging than ever.

While this transformation unquestionably offers huge benefits in terms of efficiency and productivity, it also creates potential security risks that can open a company up to crushing financial, reputational and regulatory exposure.

A recent KPMG webcast took a deep dive into how companies, regardless of market or industry, have evolved to this point and, more importantly, how they can maintain a secure controls integration environment even as they continue to transform and digitize their IT systems and operations.

Key takeaways from webinar

- Need for greater collaboration among process owners.
- There is greater reliance on cloud providers and other third-parties.
- Increased levels of monitoring are needed to manage risk and controls.
- Strong governance needed to monitor for changes to third-party applications (and their impact on business and controls integration).
- Third-party governance is an integrated function encompassed by risk and controls.
- Testing app and programming updates by third parties is essential. Don't be lulled into a false sense of security.

More apps, more cloud, more third parties

In the 20 years since Sarbanes-Oxley (SOX) was enacted to shore up corporate financial record keeping and reporting, we've witnessed huge changes in the technology landscape and its resulting impact on business operations and data security. The corresponding governance requirements likewise have grown much more complex, with many business's IT operations moving outside of the business four walls (on prem) and into the "cloud," and involving a multitude of third parties and specialized applications, including:

- Suppliers
- Applications hosted on the cloud
- Third-party logistics systems
- ERPs (enterprise resource planning) hosted on an IAAS (infrastructure as a service) cloud
- Vendor invoicing portals
- Payment brokers
- SAAS (software as a service) cash reconciliation tools

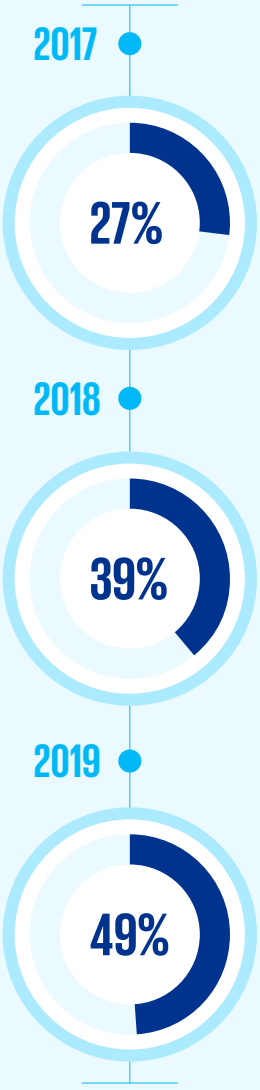
KPMG Insight

You need to evolve and automate processes. When we asked an accounting department worker why he was doing a manual journal entry log, he responded that "10 years ago we had a problem and the auditors told us to do it this way."

Businesses have found that operating in the cloud offers many advantages and allows them to easily and seamlessly incorporate the best-of-breed applications into their IT landscape. But these developments have, in turn, drastically changed the risk landscape. By putting systems and data in the cloud instead of housing them on premises and having them managed by people a company knows and trusts, businesses are putting controls in the hands of third parties who now manage the organization's data in the cloud. It has also led to a steady rise in findings of material weaknesses due to IT software, security, and access issues (see chart below), and this trend is expected to continue at an even faster rate.

Why you need to get controls right

There's an increasing trend of material weaknesses attributable to IT software, security and access issues, which all are part and parcel of increasing digitization.



Source: KPMG Material Weakness Survey, published 2020

So, while controls integration has always been important, it's now become even more critical. And with so many different players now involved in the digitization and transformation of business processes, controls integration isn't just an IT or internal audit issue anymore. It's even more important now that your controls framework is being considered, evolved, and implemented throughout the lifecycle of your transformation program.

What regulators are looking for

When regulators and external auditors examine a company's controls, the key areas of focus generally include:

- Process controls
- Cloud IT general controls (ITGC) to ensure integrity of data and processes on the cloud
- Change management controls that minimize disruptions to IT services while making upgrades
- System and organizational controls (SOC) 1 and 2
- Logging and monitoring
- Completeness and accuracy of reports
- Separation of duties (SOD)
- Access controls.

KPMG Insight

Even a simple change/upgrade made to a database can have an unanticipated change in an underlying formula, resulting in a drastic impact in financial results and month or quarter end.

Of these areas, SOD and access control remain paramount, although process control is becoming increasingly important as so many applications are now hosted on the cloud. Keep in mind that even when you're in a cloud that's being managed by a third party, at the end of the day, the data and apps still belong to your organization. You need to be aware of and understand what controls the third-party has in place.

Third-party vendors may be managing your systems and can make changes directly to your apps. You need to have adequate change management controls and a very robust logging and monitoring to ensure that an app change in one area doesn't have adverse impact on other systems.

For example, many vendors will "push" changes to you periodically without giving you the option to skip them. This change may bring with them increased risks since you may not have time to review and test them before they take effect.

Keep in mind that a change to, for example, a billing app may have unexpected consequences in the inner workings of a payment app, or inadvertently open up access to individuals who shouldn't be allowed access certain data. So signing off on the change without testing it can lead to compliance and other issues. You need to have a process in place to test updates and not simply rely on the third-party.

Who's responsible for controls integration? It takes a village

In the past, IT drove these types of digital transformation projects, or the business asked IT to drive an upgrade project. But controls integration is not solely an IT issue anymore. Because technology places an increasingly integral role in all aspects of a business—from sales to marketing to operations to finance as well as legal and compliance, essentially all departments need to be stakeholders in this process, including:

- Financial business support team
- HR business support team
- Internal audit
- App security manager
- IT security support
- Cyber security support
- External auditors.

Because technology is inextricably intertwined with the business and its operations, it requires everybody working together to scrutinize the control framework and making sure that any changes or updates designed to impact one area don't have adverse consequences in another. Questions should be asked and apps and changes to programs as part of the projects tested before they go live. This allows you to address these issues before instead of after a deficiency is found.

Nine keys to enhancing your controls integration process

The panelists offered several suggestions to help companies strengthen their controls integration process. Many organizations are already doing some of them; most aren't doing all.

Consider security and controls together. For example, if you're looking at implementing or evolving your SOD process, you need to have the appropriate IT and business partners working hand in hand to establish an effective process.

Streamline your security and controls process: Eliminate redundant controls. Too many organizations set up their security processes in silos. But these controls really need to operate in coordination with each other to be effective.

Focus on what's key and not everything. Prioritize your top five to ten most critical business transactions and ensure that apps, programs and underlying systems that impact them are tested regularly.

Involve all key stakeholders: Technology systems are deeply embedded into an organization's overall process chain. There's not one touch point with the business; you need to have conversations across multiple business units. In addition, there likely are a multitude of apps involving different vendors who should be included or at least considered in control integration conversations.

Automate controls testing and monitoring: Increasing controls automation while reducing manual controls tends to improve efficiency and reduce human error. But as you build out your controls framework and focus on continuous control monitoring, you also need to enhance the way you test your controls and move towards automating your testing to gain efficiencies.

Monitor the bots: More organizations are using bots in the performance and execution of their controls. But this can't be a "get it and forget it" situation. As with automation, you need to monitor and spot check the bots' activities to make sure they're performing their tasks appropriately.

Consider giving external auditors a seat at the table

When preparing for an external audit, internal audit needs to have a seat at the controls integration table; along with compliance, internal audit walk along with you and help you get ready for this process. But you may also want to extend an invitation to external auditors as well so they can get comfortable with your set-up before going live.

Go through some of the high-risk areas with them, and make sure that they're comfortable with your approach. You may find that they'll let you know if there are things on their radar that may impact you, or it there are new focus areas to be mindful of.

You may get push-back that external auditors will slow you down or cause problems, but that's taking a short-sighted view. It's not about getting in trouble; it's about having a partner at the table to help ensure that you're doing the right things at the right time with the right people.

Adopt exception-based monitoring and preventive controls: This is another type of automated system where you establish upfront controls and then continuously monitor what's happening. This process looks for and calls out exceptions or aberrations in key risk areas, and does so quickly.

Test third-party updates: Don't be lulled into a false sense of security when a third-party vendor makes an update to an app that you use for a particular purpose. You have to test it out to make sure the update doesn't have unintended consequences on other programs your company runs. Your company still has the ultimate responsibility of reviewing third-party SOC reports and confirming and documenting that you found their controls to be working properly and effectively.

Stay alert to M&A control issues: When companies are acquired or merge with another entity, you need to ensure that their control environments are in sync and operating effectively. One company's system may be in the cloud, the other on the premises. Or they have apps and programming that don't "talk" to each other. This will require a significant, well-thought-out and coordinated effort from all key stakeholders to create and implement an integrated controls system, and then document their efforts.

Final thoughts: Controls integration is complex but critical

Controls integration covers a wide expanse of territory. It encompasses business process controls, application controls, technology controls, cyber and data security, cloud and third-party app vendors, and much more. And when companies undertake transformation and digitization initiatives, a large part of the complexity in getting controls integration right arises because technology is intertwined in nearly all parts of a business: sales, operations, finance, compliance, HR, audit and so on.

Companies need to be more aware and sensitive to this issue, keep lines of communications open between all relevant stakeholders and act in coordination with these parties when designing and implementing a controls integration framework.

Learn more:

Watch our webcast replay

Visit our Risk Assurance Library for more insights

Connect with us

For more information about trends in controls integration, contact one of our professional below:

Jonas Eberle
Managing Director
GRC Technology Services
T: 212-954-6351
E: jeberle@kpmg.com

Kasturi Maitra
Director
GRC Technology Services KPMG
T: 415-963-8139
E: kasturimaitra@kpmg.com

Scott Palzkill
Managing Director
Application Security and Controls
T: 303-296-2323
E: spalzkill@kpmg.com

Kasey Nash
Director
Application Security and Controls
T: 214-840-2507
E: kaseynash@kpmg.com

Learn more insights at: read.kpmg.us/GRC

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