KPMG

SOD 3.0: Next-generation separation of duties for the modern ERP

New innovations require technology-driven SOD compliance and monitoring

FASTPATH

kpmg.com

Introduction

For many years, the taxpayers of Dixon, Illinois, believed a significant portion of their hard-earned dollars were funding necessary capital improvements in their bucolic midwestern town. In fact, the city's comptroller funneled $53 million into a secret bank account she then used to purchase 400 horses for breeding and show, multiple properties and vehicles, and a host of other personal and luxury items.[1]

How did one small-city official commit one of the largest municipal frauds in American history, undetected, over two decades? The same way corporations fall victim to similar crimes every day—deficient or nonexistent separation of duties (SOD) leading to unchecked behavior.

And that risk has only increased over the last several years with the introduction of new technologies, including software-as-a-service (SaaS) platforms. Once responsible for single on-premise enterprise resource planning (ERP), organizations now must manage hybrid cloud and on-premise deployments from multiple vendors, spanning the front, middle, and back office.

The inability to properly manage SOD across all functions not only increases potential risk, but also contributes to a universal rise in material weaknesses related to operational and financial compliance. Ultimately, company leaders who fail to inspire trust in their stakeholders can't fully achieve the regulatory and strategic objectives that support business growth.

To help companies evaluate and address their SOD issues, here we suggest the four pillars upon which to build a persistent SOD framework—one that continues to protect the organization long after it's put into place by adapting to changing business needs—and the steps they can take to achieve their goal and build stakeholder trust.

1 The United States Attorney's Office, Northern District of Illinois. "Former Dixon Comptroller Rita Crundwell Sentenced To Nearly 20 Years In Federal Prison For $53.7 Million Theft From City." February 14, 2013. Kartemquin Films. "All The Queen's Horses" documentary. 2017.

Increasing complexity, increasing risk

Multiple ERPs and enterprise applications from myriad vendors. Regular cloud-based software updates. Shifting employee and department responsibilities. Changing regulations and standards. All of these common factors complicate risk management and enterprise-wide controls.

Nearly two decades have passed since the Sarbanes-Oxley (SOX) Act Section 404, Management Assessment of Internal Controls, mandated SOD as an assurance that no one individual has the physical and system access to control all phases of business process or transaction. However, SOD risk and failures remain a massive issue.

Innovation, for better and for worse

In the last five years, many companies have moved from one large ERP platform to multiple vendors and a mix of cloud and on-premise deployments. In this hybrid application landscape, companies can pick and choose among best-of-breed offerings, building an enterprise technology platform that meets their specific needs.

However, even with the same vendor, buyers face challenges from cross-application risk in addition to multiple security models. Given the ease of acquiring cloud-based applications, business leaders are often adding new solutions without involving information technology (IT), which typically is more familiar with cloud security and compliance requirements.

More applications means more workflows, automation, and integration points, as well as more sets of mitigating or compensating controls that have to work together. And, after initial implementation, companies also must manage the cascading impacts of mandatory software updates in addition to the introduction of enterprise applications into the landscape.

Finally, COVID-19 has turned remote work from an exception in many industries to the rule. Technology security risk is higher from an increasingly mobile workforce, including on the vendor side. Additionally, a number of companies realized they can do as much or more with a smaller workforce, concentrating responsibilities and eliminating some natural separation of responsibilities.

Overwhelmed by the complexity, many organizations are doing the bare minimum to ensure SOD controls on an entity-wide basis.

The particular SOD challenges of companies expanding through M&A

Increasing merger and acquisition (M&A) activity could be a positive development for a recovering market—but at the same time, a potential driver of SOD failures.

Federal Reserve action reduced the cost of capital particularly for larger firms in 2020, and a continued low-rate environment should help support M&A transaction volume into 2021.* However, as the deal market begins to pick up and organizations combine, we're likely to see more SOD issues as well.

Companies that grow through M&A must combine technologies, often in short order, leading to potential SOD complexities and deficiencies.

"We have grown a lot through acquisitions and we have a global presence, so we are operating many different systems," said one vice president of technology at a public company. "It gets challenging trying to synthesize a single source of truth for what and where conflicts are."

In many M&A situations, issues also arise when staffs are consolidated and responsibilities shift. "It becomes more difficult to keep track of roles, and people are coming and going or they move departments and you find out that they still have access to things they shouldn't and it's not a good look in front of the audit committee," according to a vice president of risk management.

Tools can help stem some of the resulting issues, but without automation and a persistent and forward-looking target operating model (TOM), SOD monitoring and compliance can be ineffective, inefficient, and inconsistent. One company put several systems into place, according to an internal auditor, "but we still need people to review the reports, and we also still have about 20 percent of the business units doing this manually, which complicates the overall picture."

* KPMG Economics. "The Darkest Hour is Just Before Dawn: Challenges remain before vaccinations can save the day." December 17, 2020.

SOD-related material weaknesses remain high

SOD during the audit process

Unfortunately, it's quite common for audits to uncover material weaknesses related to SOD.

While SOX requires publicly traded companies to document and certify SOD controls, 27 percent of companies disclosed material weaknesses related to SOD in 2019, according to a KPMG study. That percentage has held relatively steady over the last few years.

Meanwhile, almost one-third of IPOs disclosed material weaknesses related to SOD in their S-1 filings in 2019, up from 19 percent in 2017. The most common root cause was a lack of resources knowledgeable about SOD and review procedures. What's happening?

Makeshift solutions

Many companies are trying to manage SOD monitoring and compliance manually, often with solutions cobbled together in house, and are struggling to achieve efficiency and a higher level of risk management.

Automation is the answer, but many organizations don't know how or where to begin synchronizing SODs across applications. While approximately 70 percent of companies use software for SOD controls monitoring , different solutions have different issues.

Many of the latest technologies also are coming from brand-new players, expanding the company vendor list—and complexity and third-party risk along with it. These issues are compounded for companies expanding to new geographies and product lines, and those responding to changing regulations; the fixes they put in place may not be scalable.

32% of audit material weaknesses were related to SOD for IPO companies. In public companies, SOD accounted for **27%** of disclosed material weaknesses.[2]

30% of companies monitor SOD controls manually, relying on traditional desktop applications such as Excel, Word, and email.[3]

Someone else's problem

In our work we have seen a number of organizations rely heavily on IT systems and applications to cover SOD requirements. However, platforms are no longer homogeneous; it's hard keep SOD "clean."

SOD compliance may be in place for one or several systems, but not all. In other instances, there may be multiple compliance programs for specific systems, without coordination. It's also wrong to assume that the cloud provider will take care of SOD, when in fact the individual or organization making transactions is the responsible party.

Companies are left to figure out how to manage SOD in multiple platforms to avoid risk exposure. ERPs as originally implemented can't handle the complexity, nor can they be customized easily or quickly. And, as auditors increase their scrutiny of SOD, including greater detail on roles and processes, it's harder for companies to answer all of those questions in a timely manner without an enterprise-wide, sustainable SOD framework.

To preserve the trust of stakeholders and unleash potential in this evolving landscape, a new way of looking at SOD becomes necessary.

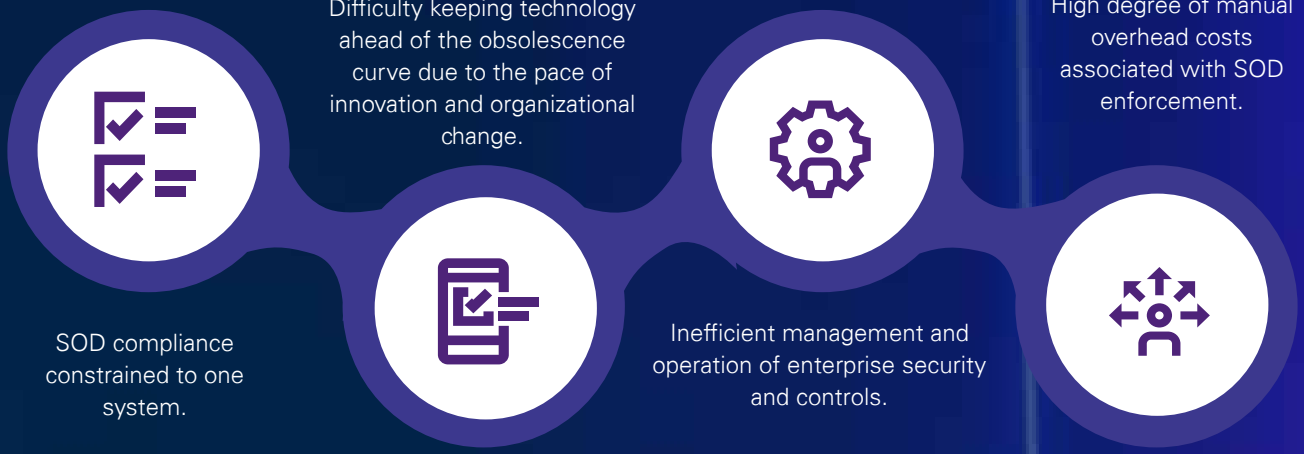
2 KPMG 2020 IPO material weakness study; and Trends in material weaknesses, Non-IPO Companies, KPMG 2020 Study. August 2020.

3 Fastpath customer research. Includes all public firms, government entities, regulated private industries above 100 FTEs, and other private industries above 500 FTEs.

Redefining SOD programs and outcomes

Technology advances require organizations to update their SOD frameworks and develop a new view of what an effective SOD program should look like—the target operating model.

Today's SOD: Limited and challenged



SOD 3.0: Automated and persistent

People

A secure and dynamic shared responsibility model

- SOD compliance embedded across the three lines of defense: business operations, oversight functions, and internal audit
- End users limited to provisioned access required to fulfill job responsibilities
- An ownership framework including approvers, owners (role, content, risk, ruleset, etc.) and sign-off
- Continuous training and development to help employees keep up with the pace of innovation and evolving regulatory requirements

Process

Ongoing compliance, monitoring, and resolution that adapts to changing business needs

- User lifecycle management includes SOD principles
- Security that matches business processes and requirements
- Prevention and detection of SOD issues in real time
- Analytics-based monitoring to quantify any exposure associated with SOD violations
- Data validation to help ensure reporting free of false positives and false negatives

The four pillars of the SOD 3.0 target operating model

A persistent SOD framework requires a strong foundation.

Technology

A single platform enabling an aggregated view of risks and monitoring across multiple enterprise applications

- SOD tool that integrates across entire application landscape—front-, middle-, and back-office
- Centralized repository for data and access to analytics
- Technical integration with any identity management, solution, and integration with the organization's governance, risk management and compliance (GRC) strategy
- Automatic updates to SOD monitoring software reflecting the most current standards and government regulations

Governance

Defined standards, robust reporting, and regulatory support

- Support for internal and external audit
- Continuous alignment with internal controls and application security owners
- Generation of reports on demand to monitor key performance and risk indicators
- Ongoing release management
- Training and organizational change management
- Ruleset management and continuous improvement

Get started. Get clean. Stay clean.

While companies are in different stages in their evolution toward establishing technology-driven separation of duties across the entire organization, there are key steps to developing and maintaining a modern SOD program. KPMG and Fastpath can help.

KPMG and Fastpath

KPMG and Fastpath combined their strengths in accounting, audit and technology to help public and private companies transform their SOD monitoring and compliance for today's challenges.

KPMG has a dedicated team of professionals focused on SOD assessments and assisting with the implementation of Fastpath software solutions. The two companies also have a working relationship to enhance products and assist each other on client engagements.

Together, we take companies through the process of evaluating their needs, implementing strategies and technology, and continuously improving their SOD program.

The Trusted imperative
When you earn and deserve the trust of all your stakeholders, you create a platform for responsible growth, confident decision-making, bolder innovation, and sustainable advances in performance and efficiency. This is the KPMG Trusted imperative, and it defines a new and dynamic approach to risk and regulation for a digital era. KPMG concentrates deep skills in risk and regulation, advanced digital solutions, and well-established change experience in one powerful and global capability. We can help you build trust with everyone who has a stake in your business, from customers, employees, and suppliers to regulators, shareholders, and the communities in which you operate.

Five steps to SOD 3.0

Vision
KPMG works side by side with organizations to assess their needs and goals and develop a high-level SOD target operating model aligned with topline corporate strategy. With the help of the Fastpath Assure® suite of security auditing tools, the process begins with a maturity assessment and planning across the four pillars of people, process, technology, and governance.

Validate
Based on a thorough risk assessment and prioritization, we validate the solution design by finalizing the TOM and developing a roadmap for implementation that includes a final solution design. Applications are prioritized based on highest risk, and we develop functional and technical designs to illustrate how Fastpath will help enable the enterprise-wide SOD program.

Construct
The Fastpath platform is then configured for specific company needs and tested, including functionality that allows organizations to monitor access controls and enterprise access risk across the wide-ranging lifecycle of business transactions. Our accelerators include proprietary SOD and sensitive access rule sets that span across 20-plus ERPs and applications. KPMG and Fastpath also have developed and continue to identify industry-specific rule sets, allowing tailored access controls for unique sector needs.

Deploy
Once the technology solution is developed and tested, integration with the TOM brings a sustainable SOD program to life. With a framework and technology in place, companies benefit from true cross-application SOD monitoring capabilities across a mixture of cloud and on-premise applications, including a wide array of major ERP packages and cloud-based solutions.

Evolve
A persistent SOD platform must change with company needs and receive ongoing support. We work with companies to help ensure that once the Fastpath solution goes live, organizations have the processes in place to continually improve and adapt. Additionally, we can help organizations scale up or down with a SaaS-based solution, allowing flexibility and speed to adapt as the threat landscape changes.

Together, KPMG and Fastpath help companies to not only define and achieve separation of duties today, but also maintain an efficient and effective SOD framework that can weather regulatory, technology and other changes to come.

Contact us

About KPMG

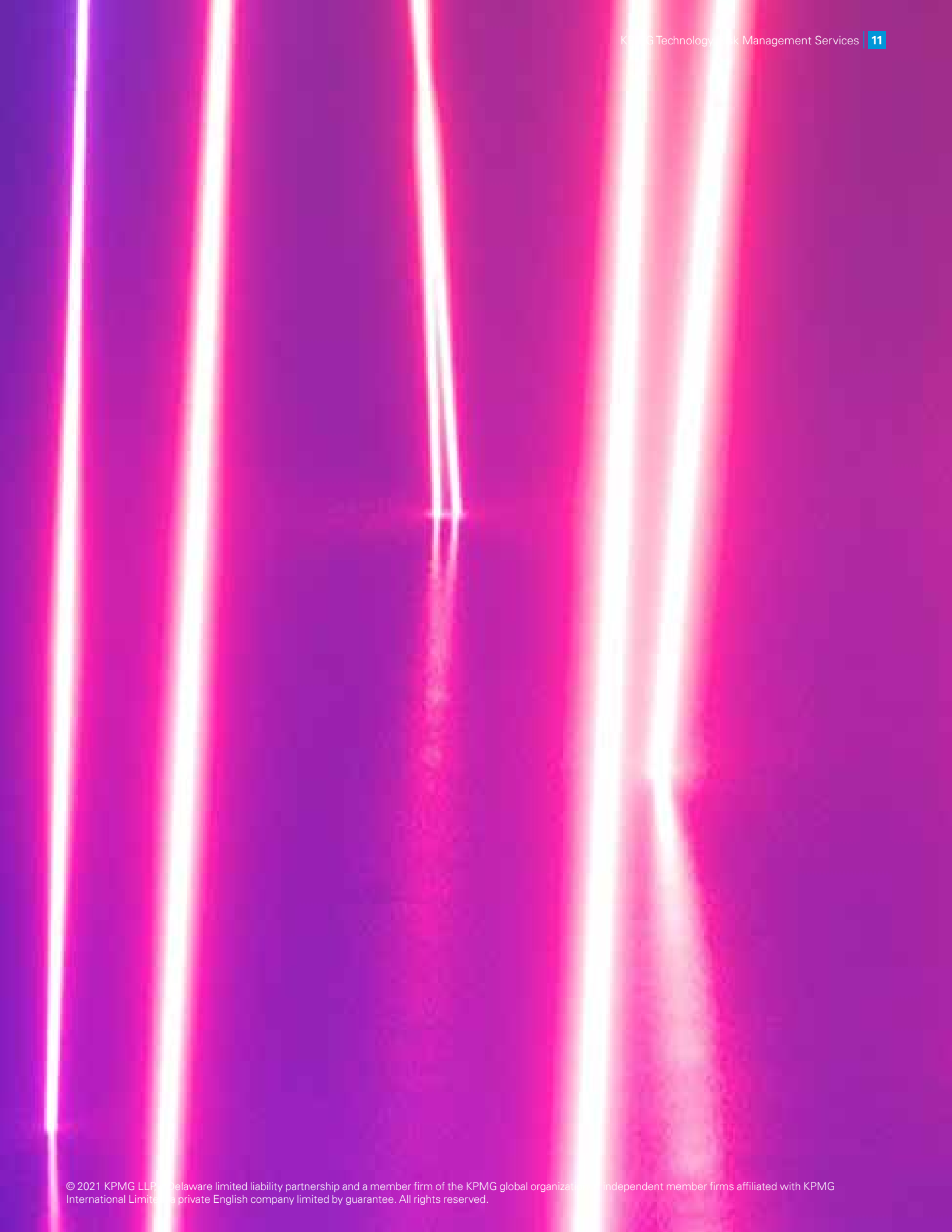
KPMG has advised companies how to design and implement effective application security for more than two decades, including helping them put processes and tools in place to manage and streamline SOD programs. Our dedicated GRC technology specialists bring together various skills in the security and controls landscape to help technology, risk management, compliance, and internal audit teams understand application security risks, and how to manage the impact those risks can have on the business. The professionals who are trained in our application security and SOD solution have a wide range of industry, functional, and regulatory compliance experience to assist companies with their unique needs. For more information, visit **read.kpmg.us/GRC**

About Fastpath

With over 1,000 customers in over 30 countries, Fastpath supports public and private global enterprises of all sizes with an award-winning security access, separation of duties monitoring, and compliance platform. The Fastpath Assure suite of tools provides an innovative new class of intelligence to monitor access controls and enterprise access risk. Solutions address audit, identity, and separation of duties by user, role, and privilege down to the lowest levels of access. Fastpath customers gain actionable intelligence about their access risk in today's dynamic business environment. For more information, visit **gofastpath.com**

Mick McGarry
Principal
GRC Technology Services
KPMG LLP
hmcgarry@kpmg.com
214-578-2225

Aidan Parisian
VP Customer Strategy
Fastpath Solutions
aidan@gofastpath.com



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

Designed by **CREATE** | CRT134954 April 2021