Rebooting security by design: Collaborate, automate, and verify everything

Shifting security left does not have to come at the expense of innovation, speed, or compliance

kpmg.com

Security and compliance do not have to be development speed bumps

Many companies are amid an increasingly complex balancing act in which they must at once consider development speed, protect against security threats, and meet audit and compliance requirements. Ultimately, it’s an exercise in both creating and preserving value. We believe that our coordinated framework—powered by automation, integrated tooling, and cross-functional collaboration—represents the operating model of the future.

This structure is the key underpinning of the evolution from DevOps to Governed Secure DevOps, where security shifts left, but not at the expense of governance or, most importantly, delivery speed. The result is a highly efficient continuous integration/continuous delivery (CI/CD) pipeline along which high-quality code is built, testing is conducted, and new or updated applications are safely deployed.

Before we move further, it’s crucial to clarify exactly who we’re speaking to. There are three audiences here: the collective information technology (IT) delivery and support organizations (IT Engineering), information security (InfoSec), and technology risk (Tech Risk). We’re focused on preventing issues such as data breaches, cyber events, application outages, and unauthorized releases—as well as the resulting financial and reputational costs, and the process breakdowns that lead to these incidents—while not inhibiting innovation, security, or agility. The strategy and response around preventing future events falls under the collective purview of these groups.

For these groups to work together efficiently, the foundation must be built on centralized tooling that enables automation and integration, as well as a concerted “shift left” of operational, security, and audit considerations. Further, an employee-centric, human-capital-focused model, and the relevant cross-functional processes, will go a long way toward minimizing security gaps, audit complexity, development delays, outages, and other operational issues. This approach provides software organizations with a new and repeatable way to build, protect, and deliver their products and services.

The goal is for these groups to think deeply about whether they are prepared to develop, build, and deploy securely, expeditiously, and at scale. To get there, the question for every professional who contributes to the success, or failure, of the systems development lifecycle (SDLC) is not simply, “Are you ready?” but “Are you ready to work together?”

DevOps security and compliance challenges across the enterprise

IT Engineering

- Lack of proper tooling and the integration of tools to assist with root cause analysis, automated alerting, scanning, etc
- Delivery is often delayed when adhering to the linear nature of traditional change management
- Deployment to production is often delayed by a “big-bang” approach to security
- Compliance and security controls are siloed from the SDLC

InfoSec

- Validation of security is manual, restricting the speed at which changes are delivered
- Product iterations lack threat analysis and/or modeling
- Lack of controls, compliance, secure-by-design training, and cross-functional collaboration
- Teams don’t have proper key risk indicators, key performance indicators, or monitoring controls in place

Tech Risk

- Agile team lacks proper procedures and standards to drive consistent compliance with requirements
- Controls are not documented or automated where possible
- Shift from legacy controls to agile controls

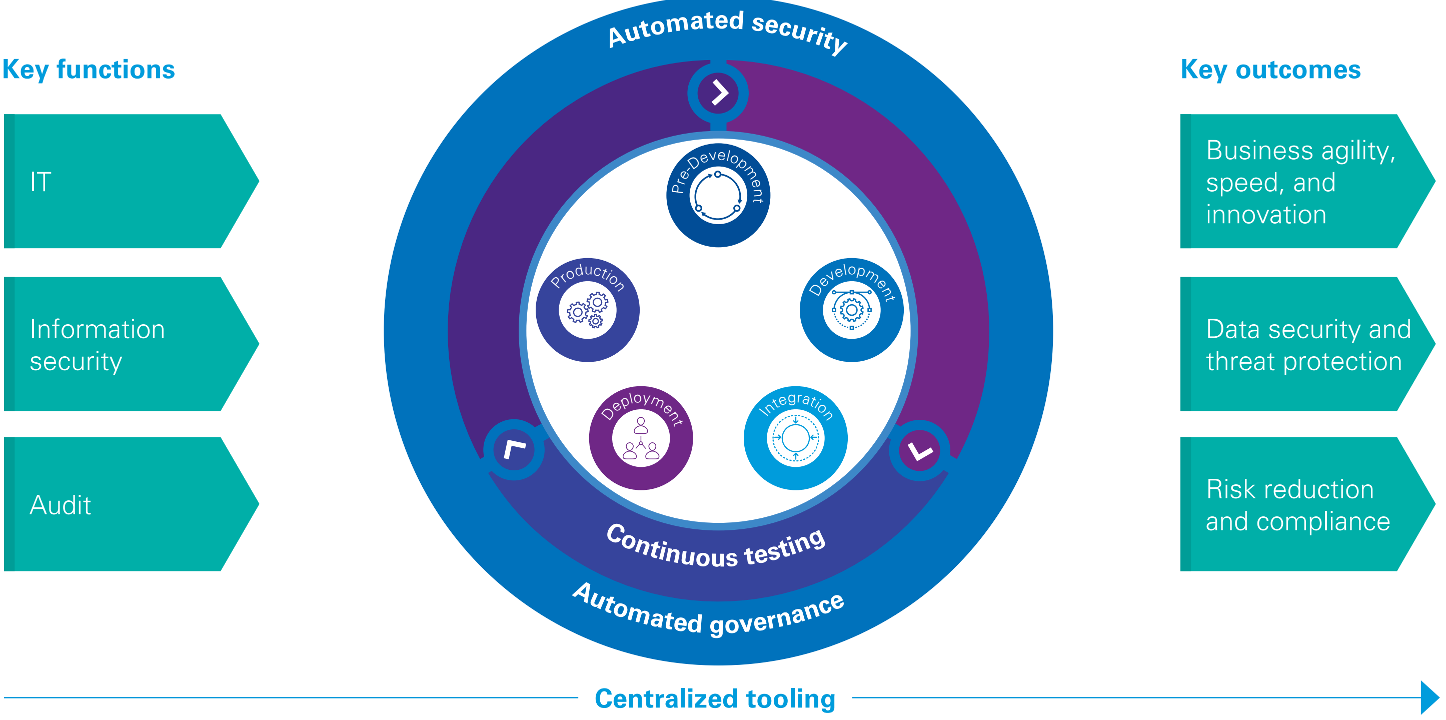
Achieve speed and compliance securely

If your IT Engineering, InfoSec, and Tech Risk functions often operate separately, then your processes, people, and technology will likely also be disconnected, which leads to gaps in agility, security, and operations. Guided by our standardized reference framework, companies can construct a comprehensive picture of how this operational change can benefit their existing process. To deliver value rapidly, ensure security, and conduct relevant, meaningful audits, organizations are encouraged to adopt a build-appropriate plan powered by automation, centralized tooling, and collaborative, well-trained professionals.

From an IT Engineering perspective, most organizations today have multiple operating models in play in relation to how people are organized, how processes are designed to deliver software, and how technology is employed in support of their overall service capabilities.

Imagine a company at which once-disparate groups now operate in a centralized, value-oriented way. This company delivers new features, changes, and fixes expeditiously—without compromising security and governance. Centralized tooling and close collaboration with InfoSec and Tech Risk enable IT Engineering to gather requirements to automate the CI/CD pipeline. Indeed, automated governance and security are at the operational heart of this process—ensuring the organization is not caught unprepared by attackers or slowed down by audits.

Our strategy is designed to mitigate risk, increase compliance transparency, and increase agility and speed



Key functions

IT

Information security

Audit

Automated security

Pre-Development

Development

Integration

Deployment

Production

Continuous testing

Automated governance

Key outcomes

Business agility, speed, and innovation

Data security and threat protection

Risk reduction and compliance

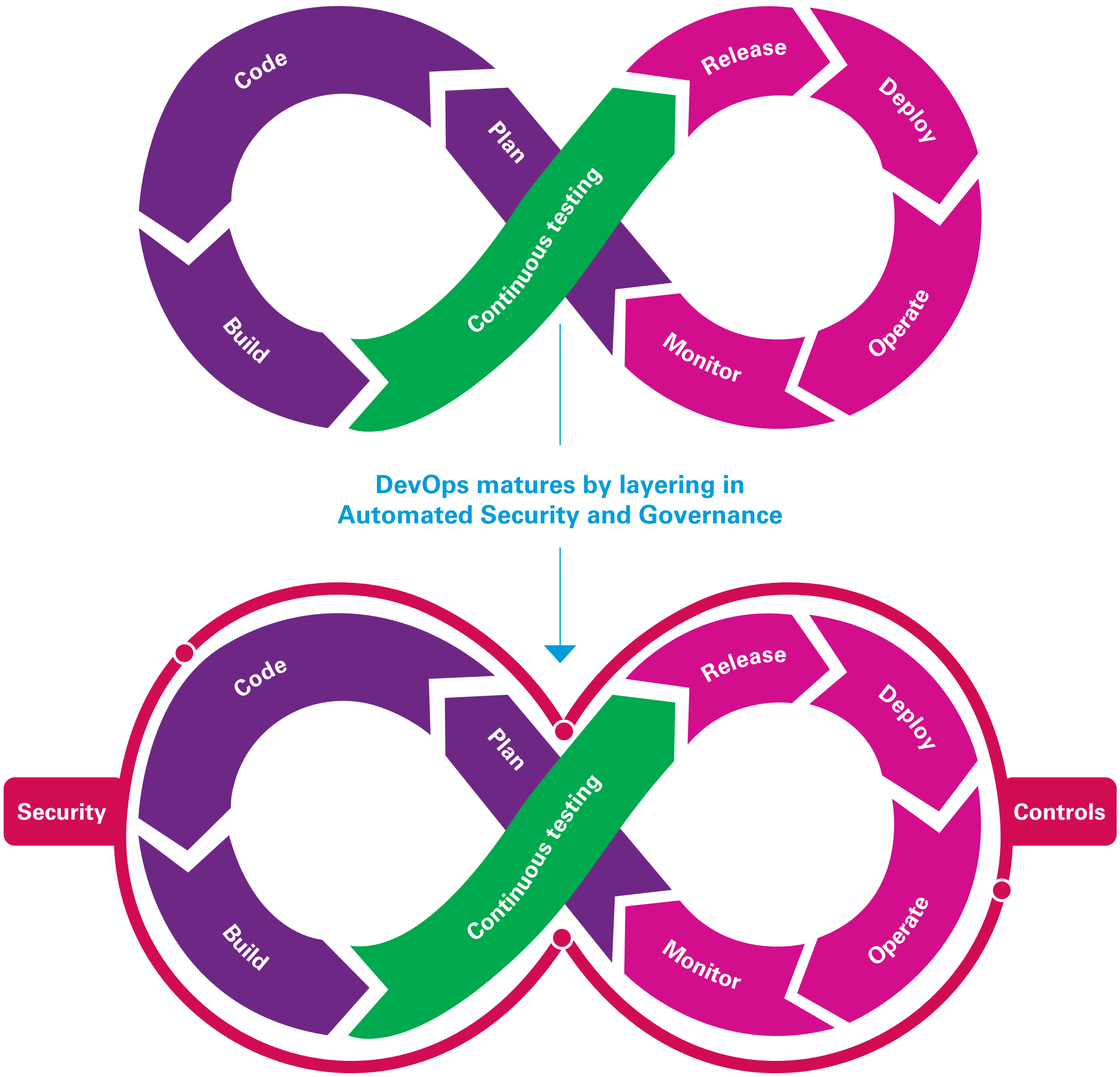
Centralized tooling

The ultimate objective is to sustainably reduce as much operational risk as quickly as possible, with the least friction and least cost, so the business can effectively compete in today's rapidly evolving market. Putting all the pieces and players in place to achieve that state currently is not well understood across many organizations. As a result, the depth, breadth, and frequency of whatever risk-reducing activity organizations want to establish tends to be underdeveloped in the traditional DevOps model.

Get from here (DevOps) to there (Governed Secure DevOps)

At a high level, DevOps is the practical alignment of development and IT operations teams for the purpose of creating business value through the more frequent delivery of new and updated software. Simply stated, Governed Secure DevOps is the integration of security into the DevOps equation at every step. Done well, this approach accelerates development and deployment by adhering to predefined controls and automated testing across the SDLC.

Governed Secure DevOps builds on the traditional model by layering in automated security and governance controls



Governed Secure DevOps brings with it an architecture informed by security, governed by relevant controls, and focused on maintaining delivery speed. Code scanning is built into the CI/CD pipeline to verify secure coding practices before execution and deployment.

Key facets of this approach include:

Shifting security and compliance left

Ensures security and governance standards are addressed from the beginning of the SDLC through automation—not manual processes. Enhances the ability to continuously deploy changes to production with risk mitigated.

Employee-based DevOps resourcing model

Data suggests that outsourcing DevOps functions leads to a significantly higher likelihood that the team will be low performing. Employee-centric teams, comprising true business stakeholders, are much more likely to be high performers.

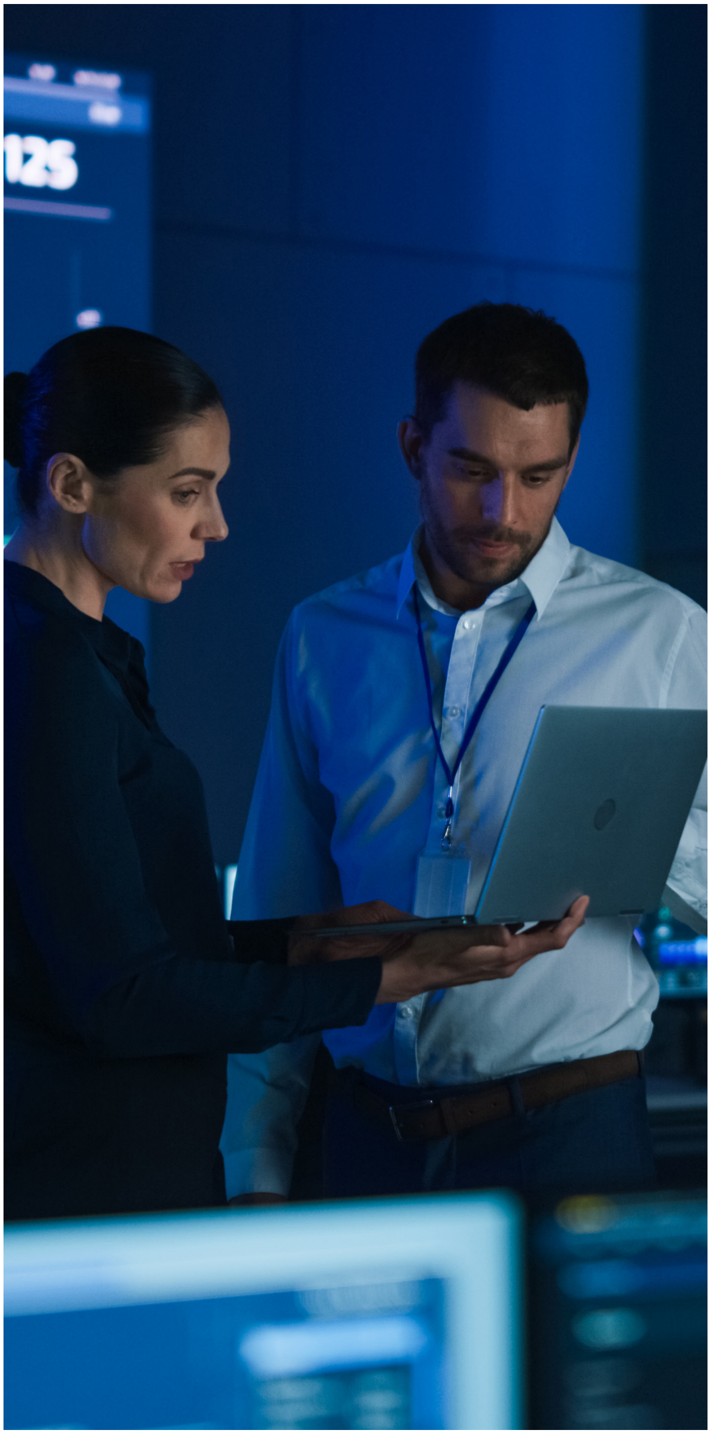
Automated security

Introduces automated testing such as dynamic application security testing, interactive application security testing, static application security testing, and software composition analysis, which evaluate whether security requirements have been addressed in the build.

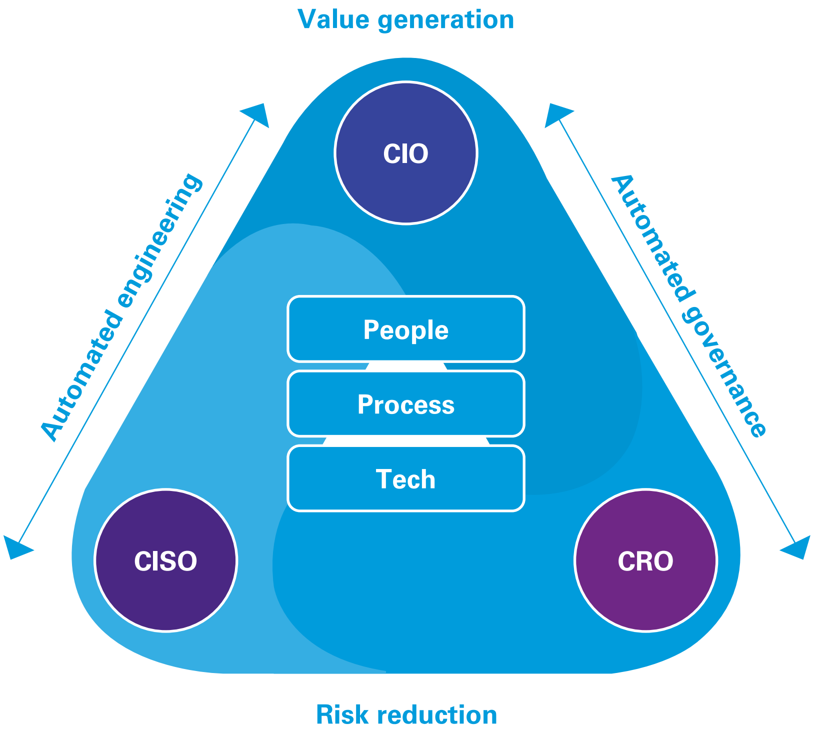
The challenges of developing a secure, governed delivery model has led to the creation of a standard approach to mitigate risks and increase transparency of compliance, while achieving and maintaining business agility and speed. Built on a foundation of automated engineering, governance, and security, Secure DevOps allows for ongoing, productive cross-functional collaboration.

A transformative framework

The KPMG approach aligns organizational objectives by automating engineering and governance wherever possible and practical, enabling faster innovation and less risk visible on a "single pane of glass"



Get from here (DevOps) to there (Governed Secure DevOps)



Strategize and lead transformation from legacy to DevOps

Ensure security is embedded in the development process

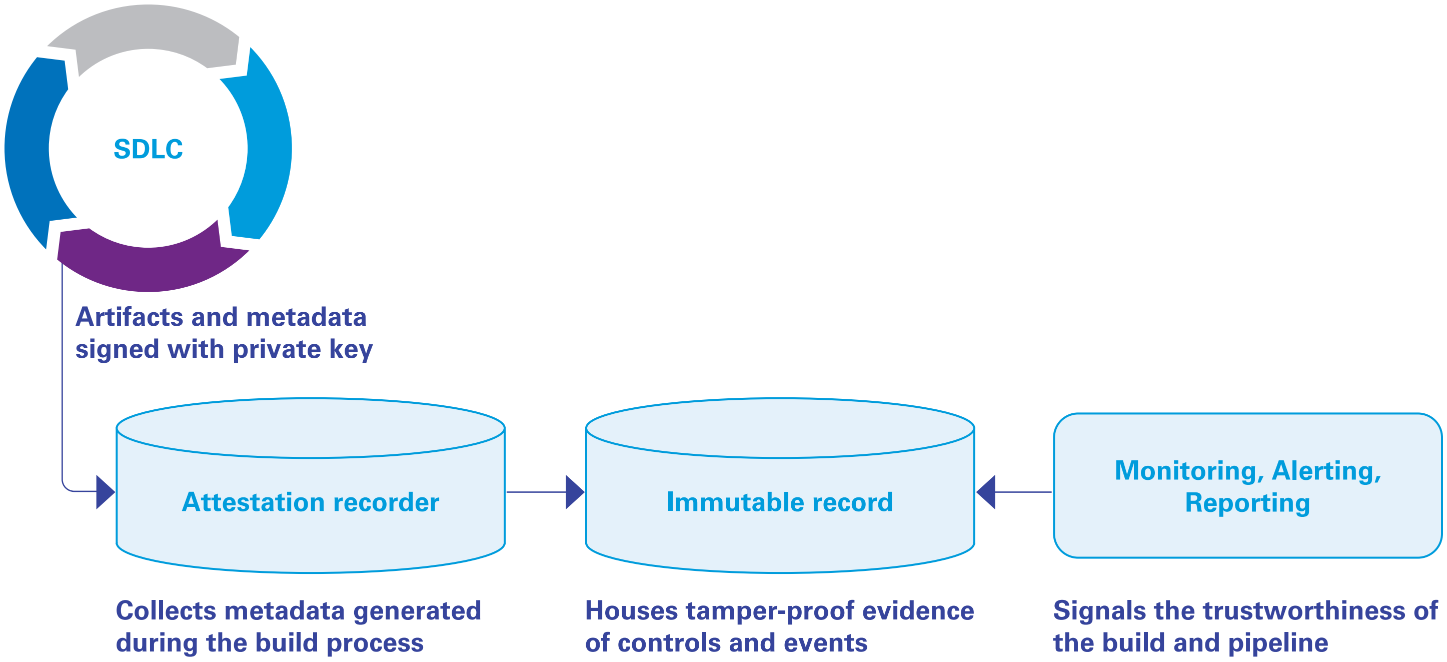
Identify risk in the process and implement controls to address them

Establishing common objectives and setting clear chronological operational milestones with progressive levels of business criticality aligns IT Engineering, InfoSec, and Tech Risk and invests them in each other's success.

When acclimating the organization to a Governed Secure DevOps model, security and controls become a component of the entire enterprise's responsibility set.

Prioritizing traceability

An immutable change record represents a vital element of traceability that many software development firms lack in their CI/CD pipelines.


SDLC
Artifacts and metadata signed with private key
Attestation recorder
Immutable record
Monitoring, Alerting, Reporting
Collects metadata generated during the build process
Houses tamper-proof evidence of controls and events
Signals the trustworthiness of the build and pipeline

Traceability: Where the rubber meets the road

In the Governed Secure DevOps model, an immutable change record—think of it as a tamper-proof audit log of the entire SDLC hosted in a single place—is created from upstream activities and tooling. This record is fed from all the upstream activities and output from the integrated set of tools.

It brings to life the interconnected nature of developing or updating the code (IT Engineering), performing proactive security testing (InfoSec), and ensuring the appropriate controls are triggered (Tech Risk). It's how you can prove the final product is accurate, secure, and compliant every time the pipeline is run.

This automated record is created at the end of the process as a way to package each group's work and check the various steps across the SDLC. When you believe you're ready to release a new product or update, the immutable change record enables you to quickly verify whether it has been successfully tested and peer reviewed. From there, you can quickly make the decision to release with confidence or, if inaccuracies, inconsistencies or vulnerabilities are detected, pause the process, investigate, and make repairs.

A real-world Secure DevOps transformation

A client—a prominent IT management software company based in the U.S.—had experienced a sophisticated software supply chain attack that impacted numerous customers, resulting in a loss of confidence among customers and prospects in the company's capabilities. Ultimately, the company wanted to transform its delivery model without compromising controls or agility.

Primary challenges

In short, the system had failed because the release of application updates had not been managed effectively. The security of the system within which code was built and compiled into an executable format was not accounted for as the company focused on other priorities, particularly speed-to-market. As a result, the risk and security teams had limited visibility into the overall process because of ineffective governance oversight. There was no consolidated Secure DevOps approach at the enterprise level that encompassed IT Engineering, InfoSec, and Tech Risk.

KPMG response

Following an investigation and root cause analysis, we were able to reverse-engineer the code responsible for the attack. This provided insight into the company's existing vulnerabilities and how to address them. Our team reviewed documentation and collected data-driven evidence across applications to develop a detailed roadmap to achieve a high degree of controls auditability, compliance, and security by helping the company devise a telemetry mechanism for collecting, logging, monitoring, and sharing pipeline data.

KPMG worked collaboratively with the company's CIO, CRO, and CISO teams to assess the wide-ranging change management processes, provide visibility into the current state of interconnected pipeline processes, highlight risks through testing, and incorporate monitoring and alerting controls to be used as a basis for incorporating automated security and compliance into the CI/CD pipeline.

Outcome

Simply stated, this exercise was about automating the SDLC and inspiring tighter collaboration between software development, security, and governance to ensure the organization is doing everything possible—in sync—to avoid or mitigate future data breaches. Few organizations are doing it right at the enterprise level because that cross-functional coordination is just not happening consistently.

It's not just a matter of ensuring collaboration and shifting security left in response to an isolated instance. Secure DevOps should be standard operating procedure. It's got to be the way things are done across all delivery pipelines and all production paths. In the end, we helped the company facilitate a rapid, secure, and compliant service-delivery model.

How KPMG can help

KPMG professionals work with clients to help shape their IT strategy. Our specialists build innovative and elegant technology solutions that are designed to transform your delivery model.

Many software development companies are beginning to see the value of transitioning from a traditional DevOps model to an approach that not only focuses on security and controls but also does so without compromising speed.

Our Secure DevOps capabilities include:

- Governed Secure DevOps capability assessment
- Secure DevOps strategy and transformation
- Advanced tooling and engineering orchestration
- Security-centric managed services
- Governance, risk, and compliance/internal audit.

We focus on collaboration between our IT Engineering, InfoSec, and IT Audit practices to deliver value by deploying our resources in the same holistic manner that we recommend clients approach the transition from DevOps to Governed Secure DevOps.

About the authors

Lavin Chainani

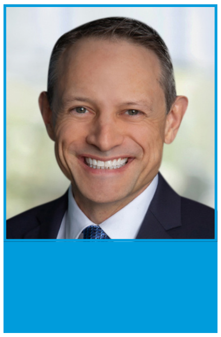
Managing Director

Technology Risk Management

T: 410-949-8834

E: lchainani@kpmg.com

Lavin has 15 years of experience in technology risk management with a focus on IT internal audits, emerging tech risk, system implementation reviews, and building IT compliance teams with focus on technology controls and compliance. Prior to joining KPMG, Lavin worked as a network administrator.



Caleb Queern

Director

Cyber Security Services

T: 512-320-5104

E: cqueern@kpmg.com

Caleb has more than 15 years of technology and information security experience. Prior to joining KPMG, caleb served as the Chief Scientist for a cyber security services firm based in Northern Virginia. He focuses on reducing risk and improving performance so organizations can meet business goals and grow. Caleb has led engagements with companies in the technology and pharmaceutical sectors, as well as higher education.

James Williams

Director

Modern Delivery

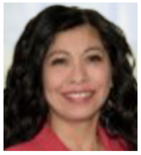
T: 214-840-4822

E: jameswilliams@kpmg.com

As the KPMG Modern Delivery solution leader, James integrates Agile principles, DevOps approaches, product management methodologies, and automated value chain functions to create collaborative cultures that drive outcomes. With more than 20 years of global management consulting and business experience, he applies his advanced knowledge of application development, cloud, and infrastructure automation capabilities to define and execute strategies that break down traditional silos and address critical operational challenges while enabling the successful delivery of new and improved client services.

Contact us

Marcus Murph
Principal
CIO Advisory
T: 214-840-2671
E: marcusmurph@kpmg.com



Cyndi Izzo
Principal
Technology Risk Management
T: 617-988-5613
E: cizzo@kpmg.com

Kyle Kappel
Principal
Cyber Security Services
T: 949-431-7359
E: kylekappel@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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.