KPMG

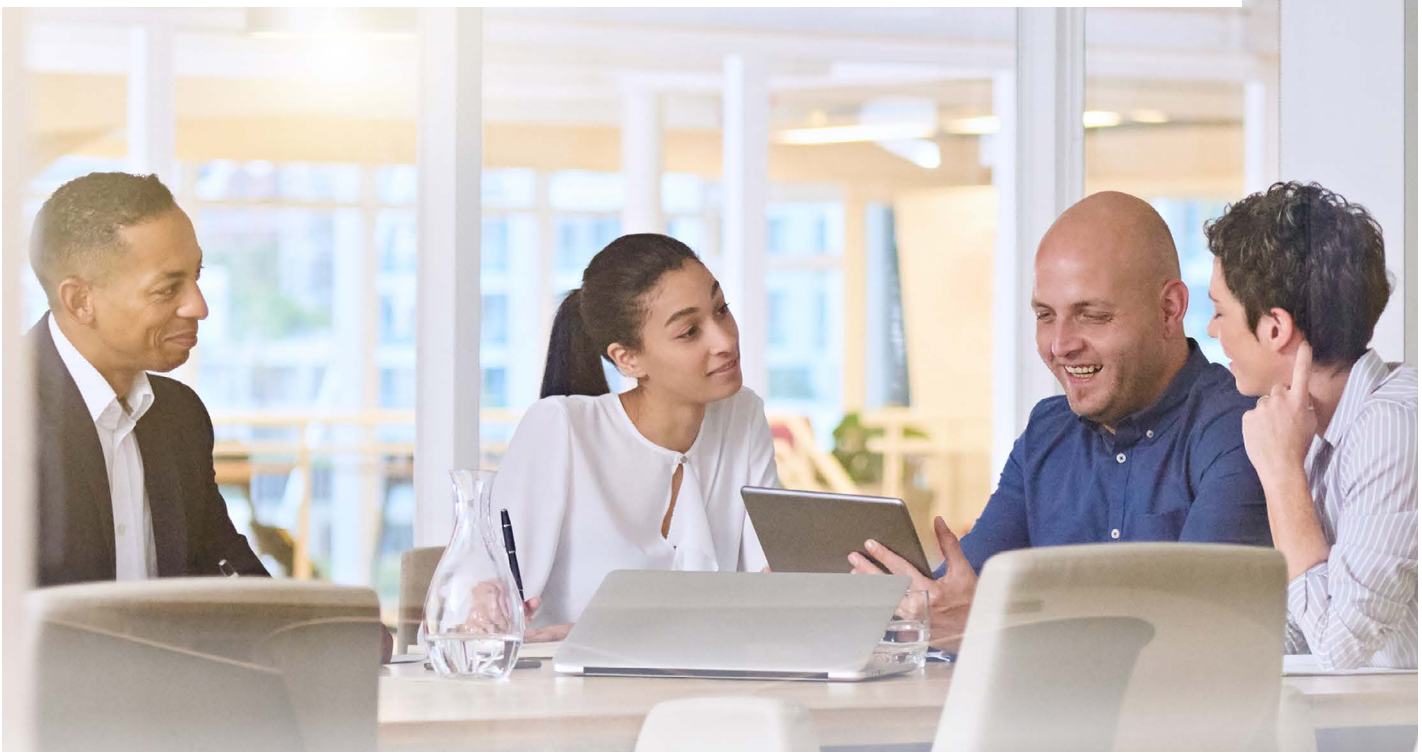
The controls observability imperative

Mitigating risk in System Development Life Cycle (SDLC) real-time

September, 2022

kpmg.com

What you can't see can hurt you



The complexity of modern IT environments often creates new ways for technology to fail. Distributed systems are unpredictable. The shift to the cloud and the rise of containerized workloads complicate the secure movement of data between locations or cloud providers. Multicloud platforms with multiple service providers make it difficult to strike the right balance between tight controls and agility.

Despite sophisticated processes like agile software development and DevOps practices that combine software development and IT operations, cyber-attacks multiply and create major outages. Nearly 30 percent of outages lasted more than 24 hours in 2021, an increase from just 8 percent in 2017.[1] Not surprisingly, the tangible costs associated with enterprise technology failures have increased exponentially.

Challenges like these demand new solutions, including the need to have greater visibility into processes and controls. Controls should be considered for every phase, from planning and development to testing and deployment. While successful organizations are prepared to both prevent and acknowledge failure, they also can safeguard against damage with effective controls and continuous monitoring.

[1] "Uptime Institute's 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short," June 8, 2022.

KPMG

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
NDP370789-2A

Key questions for each line of defense

More than ever, IT organizations are expected to deliver results faster, reduce costs, and play a strategic role in driving critical business outcomes. They're also expected to maintain development speed, protect against cyber-attacks, and meet compliance requirements. Little wonder, then, that real-time monitoring and testing of applications and infrastructure has become a top priority for DevOps and IT teams.

The risk of large-scale failure looms. To mitigate this risk, companies should address a set of questions to each of the three lines of defense to determine the most effective way to modernize controls.

Business operations

The first line of defense includes engineering, products, IT, and operations teams. From system design to implementation, they generate considerable telemetry.

To better gauge the effectiveness of controls and integration tools, leaders should ask how to:

- Leverage the right framework
- Integrate and configure business tools correctly
- Prepare and implement the right controls
- Balance processes with security and compliance controls.

Oversight functions

The second line of defense encompasses finance, human resources, quality, and risk management teams. They need to collaborate with the first line.

Effective standards can add value within this function by asking:

- How do we manage controls and not delay operations?
- How do we collaborate with the first line to provide the right standards and guidance?
- How do we address the shortage of skills, behaviors, and competencies?

Independent assurance

The third line of defense comprises internal audit and independent assurance providers.

For audit teams to keep up with technology changes and develop the right controls, they should ask:

- Do we have the ability to scope systems and tools properly?
- How do we identify possible failures and proper controls?
- Are we agile enough to shift mindsets and processes for improved testing?

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP370789-2A

Next-generation approaches

Siloed approaches to monitoring can no longer handle the large volume of data generated from modern infrastructure. Finding the true balance between value and compliance has become more complex. This paradigm shift paves the way for the transition from monitoring to observability.

At the intersection of cloud infrastructure monitoring, application performance management, and log management, observability solutions actively explore emerging and undefined patterns within IT systems. Observability concerns how well the state of a system can be inferred from the three key pillars of data—logs, metrics, and traces—to gain better insight.

A recent survey of IT practitioners reveals that 90 percent consider the absence of observability services to give rise to monitoring challenges.[2] Beyond operational demands, customer expectations also make a compelling case for observability. In the global retail industry, more than 60 percent of IT leaders say they are opting for full-stack observability to improve customer engagement.[3]

In addition, compliance and security are important use cases for full-application-lifecycle monitoring. Being armed with the right portfolio of observability solutions helps organizations drive control compliance and real-time visibility to reduce risk.

This next-generation method for observing and troubleshooting complex distributed systems uses new approaches, such as distributed tracing, container monitoring, AI-assisted operations, and DevOps processes. Observability, in fact, works in conjunction with DevOps: By creating better observability in an existing system, you can enable better testing.

Observability has enabled DevOps teams to refine the functionality, performance, testability, operability, efficiency, and usability of their stack. IT stakeholders agree that observability capabilities would benefit their organization and are reporting compelling use cases for observability platforms.[4]

Observability, security, and continuous integration/delivery (CI/CD) capabilities are increasingly offered as integrated solutions in the market. Some 52 percent of respondents in a recent survey say they collect data from their application environment using more than 10 observability tools.[5]

Despite the number of tools, observability has found a place in the world of controls. Led by next-gen technologies, application projects and IT architectures have pushed organizations to consider the large financial and reputational impact that a lack of proper controls can have.

Clearly, now is the time for a controls observability solution.

---

[2] "The State of Observability," VMware, 2021.

[3] "The Journey to Observability," AppDynamics, 2021.

[4] "The State of Observability 2021," VMware.

[5] "The State of Observability 2022," Splunk survey of 1,250 observability practitioners.

KPMG

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
NDP370789-2A

The KPMG controls observability framework and solution

The KPMG controls observability solution combines people, methodologies, and accelerators so an organization can monitor its key controls across the entire change lifecycle in real time. The solution can be deployed at scale to drive control compliance and visibility, leading to risk mitigation and control validation.

As the graphic shows, culture and awareness are at the core of a framework that revolves around governance, monitoring, and improvement. Successful outcomes require collaboration among engineering, security, compliance, and audit teams.

KPMG

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
NDP370789-2A

1. Change management policy

Enhance a global practical **change management policy** and procedure that addresses end-to-end change management.

2. Branch and release standard

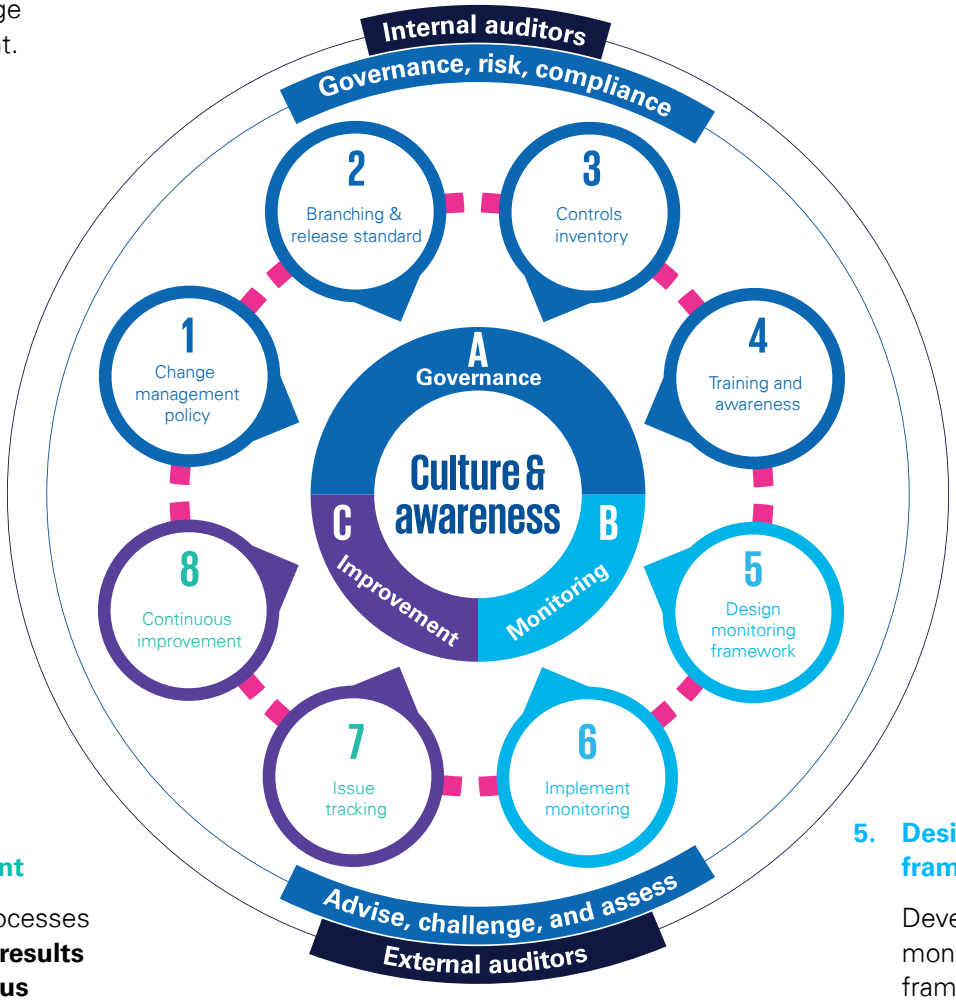
Integrate strategy, settings and guidelines for **branch and pipeline management** with clear path to production.

3. Controls inventory

Enhance process flow for each product and **establish** key and operational controls to address the risk.

4. Training and awareness

Enhance **awareness** of the key risks and controls among the development teams.



8. Continuous improvement

Establish processes to **leverage results of continuous monitoring** and issue tracking/ remediation to determine where there is an opportunity to **continuously improve** the overall process.

7. Issue tracking and reporting

Establish the process to put guardrails in place to generate the **retrospective reviews**, issues, and tracking where possible.

6. Implement monitoring

Leverage **data and automation capabilities** to monitor deviations from the controls and baselines implemented to address the risks.

5. Design monitoring framework

Develop a monitoring framework and **point-in-time control triggers** that when aligned properly with **impact zone of a change** will provide a more integrated assurance model without slowing down the speed.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP370789-2A

Three-pronged strategy

By focusing on governance, monitoring, and improvement, our observability solution enables speed with reliability and traceability.

Governance

Take these steps for policy standards, controls, and training to lay the foundation for effective change and program management:

- Implement and/or review change management policy. Leverage service management tools and understand the organizational vision to define minimum requirements and responsibilities across all technology layers.
- Establish standards for branching and release with alignment to end-to-end change processes. Include clear requirements for pipeline and branch management.
- Refresh and/or create controls for each product. Also create documentation for each control in accordance with global standards.
- Review the training focused on risk, controls, and security. Update existing training with elements of change management. Periodically assess training on the completion cycle to be sure it is up to date from process to monitoring.

Monitoring

Follow these steps to achieve customized insights for efficient compliance metrics:

- Design a framework and process to monitor the product and business-level changes to gain insights against control performance
- Implement monitoring at all product levels to align with the framework and risk assessment.
- Continuously monitor application processes and leverage technology solutions to perform monitoring.

Improvement

Set the right tone to foster continuous assessment and internal evaluation by taking these steps:

- Establish processes to proactively track issues, determine the root cause of failures, and implement remediation plans.
- Design key performance indicators for tracking improvement and establish a defined feedback loop.

KPMG

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
NDP370789-2A

Unlock value with KPMG

The KPMG controls observability solution powers innovation and collaboration. We work with all three lines of defense to help ensure that you have the design you need—with the right controls and integrated tools configured at scale—to effectively leverage all the data produced.

We bring a pragmatic approach to controls observability because we know that traditional controls may not apply in the fast-paced world of continuous DevOps delivery. Our cross-functional team has deep skills in areas including, engineering, control assessment, cyber security, target operating models, strategy, and road mapping.

We know what industry-leading solutions look like. Rather than simply focus on the change and release element, we take a holistic view—encompassing the change management process from ideate/plan, develop, build, and test to release/deploy, run/operate, and govern.

Contact us to learn how to build a controls observability function that is reliable and immutable.

Together, we help you unlock value for security and governance operations and build the operating model of the future.

KPMG

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
NDP370789-2A

KPMG Technology Risk Modernization Centers of Excellence

The threat landscape in today's volatile environment continues to evolve shifting attack vectors and variable risks. As digital transformations accelerate in business functions at a record pace, our Technology Risk Management network has developed the KPMG Technology Risk Modernization to provide insights and help organizations evolve their capabilities to respond to digital acceleration, cloud transformation, and emerging technologies.

Learn more at: visit.kpmg.us/TRMCOE

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
NDP370789-2A

Contact us

Contact us to learn how to build a controls observability function that is reliable and immutable, turning raw data into real, actionable insights that can better predict risk points and prevent noncompliance or outages—all at warp speed.

Learn more

Read.kpmg.us/TRM or scan our QR code for the latest risk insights

Lavin Chainani
Managing Director
Technology Risk Management
KPMG LLP
T: 410-949-8834
E: lchainani@kpmg.com

Kevin Coleman
Partner
Technology Risk Management
KPMG LLP
T: 415-963-7209
E: kmcoleman@kpmg.com

Raj Konduru
Principal
CIO Advisory
KPMG LLP
T: 216-224-3920
E: rkonduru@kpmg.com

Shahn Alware
Managing Director
CIO Advisory
KPMG LLP
T: 858-366-3440
E: salware@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.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. NDP339886-2A