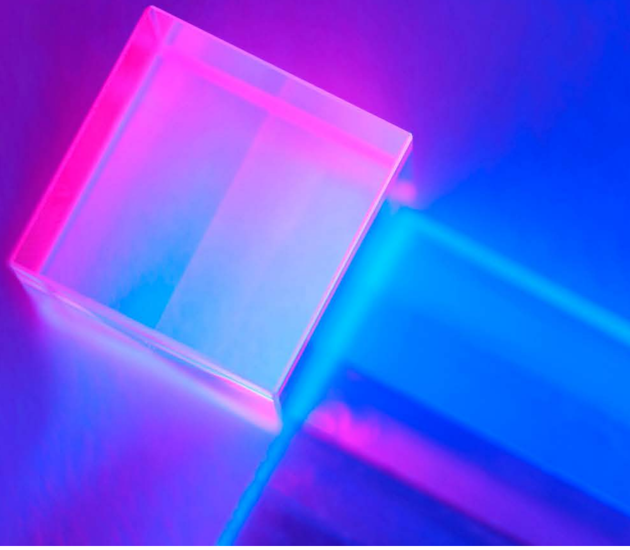


How to enable controls observability and trust at market speed

Safeguard data and mitigate risk in real time

Warp speed applies to more than just Star Trek. Agile software development and DevOps practices that combine software development and IT operations shorten the system development lead time to the point where software can be built and delivered 100 or even 1,000 times faster.

But add speed to quantity—the thousands of metadata points generated for every action taken on repositories, integration and deployment tools, service management systems, and production environments—and your organization can be on a collision course with inadvertent changes that lead to outages and incidents. The threat is significantly higher in monolithic systems that have a large inherent technical debt.

There is no shortage of tools today in the market and tool sprawl is common across the board. Siloed monitoring tools cannot handle the sheer amount of data, much less find the true balance between added value and compliance. What's needed is a simpler, tailored approach to stitch this data in a meaningful manner that is efficient for cross-functional teams. This simpler solution requires a well-engineered and automated solution that utilizes data and analytics to observe controls just as cloud systems already measure availability.

Most organizations don't have comprehensive observability capability, and they're paying the price. The average annual cost of downtime for leading organizations with fit-for-purpose observability solutions is $2.5 million, compared to $23.8 million for those without, according to a 2022 study by Splunk.[1] The rise in incidents with losses over $100,000 has also increased by more than 50 percent.

[1] Splunk, "The State of Observability 2022"

Benefits of real-time controls monitoring and testing

Controls observability—gaining insight about a process or application by measuring its output—has become a core necessity. It helps fix problems faster and improve reliability. A full 93 percent of global IT leaders consider observability to be a key component for modern enterprises, according to a 2021 LogicMonitor study.[2]

A well-designed observability function is founded on four pillars:

- **Logging** so that every edit generates data
- **Traceability** to track every edit
- **Monitoring and alerting** so that every change can be acted upon
- **Visualizing** to gamify observability data.

The process begins by mapping the details of everyday processes to identify the relevant control points for decision making. Control points are then turned into data to help enforce control activities. Finally, by leveraging data points in conjunction with an organization's codified policy checks, a data-driven, real-time observability capability/ platform can be built.

This approach yields several key benefits by:

- **Reducing manual** controls, increasing controls automation, and automating testing and monitoring
- **Enabling exception-based monitoring** to flag and remediate issues more easily.
- **Relying more on preventative controls** to reduce the risk and potential errors.
- **Streamlining security and control processes** for shorter downtime and better performance.

Enabling speed with reliability and traceability

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

As shown in the graphic below, our framework is anchored around governance, monitoring, and improvement functions. It requires collaboration among an organization's engineering, security, compliance, and audit teams to achieve success.

[2] LogicMonitor, "2021 Tech Convergence: ITOps and DevOps"

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

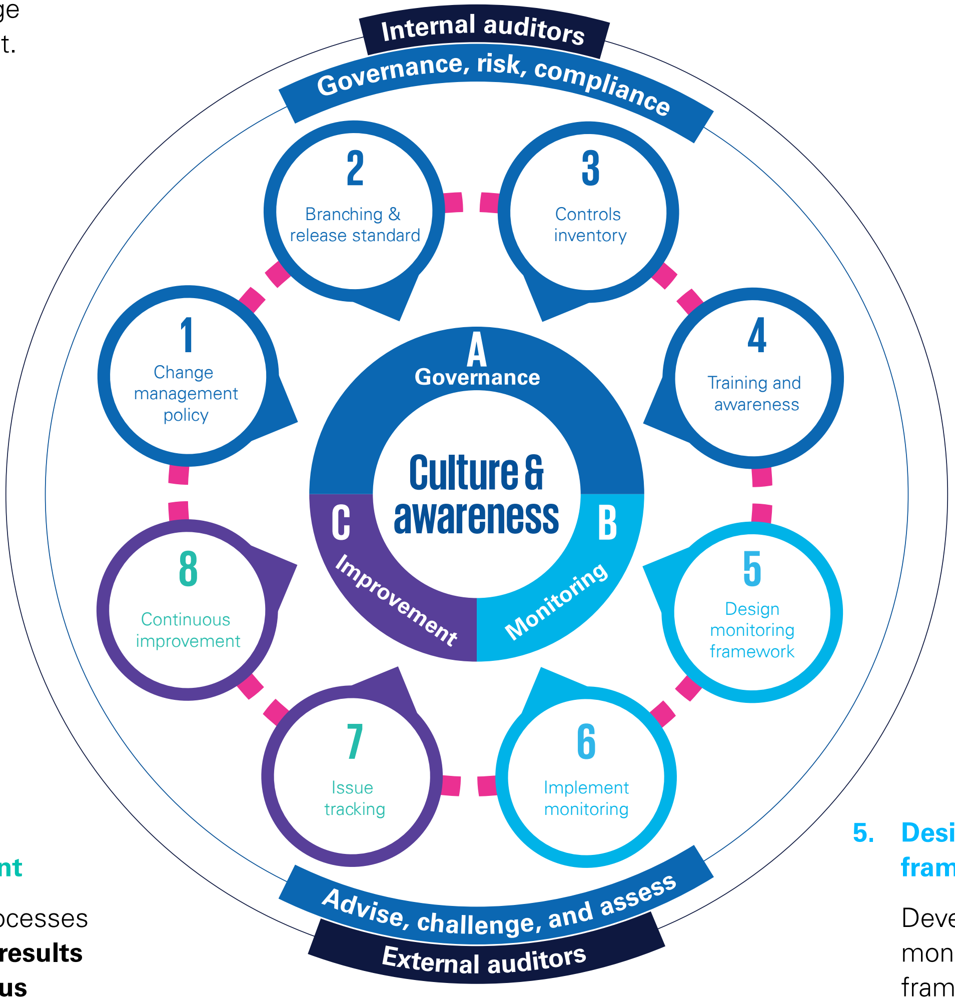
Integrate strategy, settings and guidelines for **branch and pipeline management** with clear path to production.

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.

Why KPMG?

We bring a pragmatic approach to controls observability because traditional controls may not apply in the fast-paced world of continuous DevOps delivery. We know what industry-leading solutions look like. Our cross-functional team has deep skills in engineering, controls, cyber security, target operating models, strategy, and road mapping.

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.

We collaborate with all three lines of defense—business operations (first line), oversight functions (second line), and audit teams (third line)—to help ensure that they have the design they need, with the right controls and integrated tools configured at scale and are effectively leveraging all the data produced.

Best ways to begin

With IT organizations moving at market speed, it can be hard knowing where to start. We suggest the following five actions:

- **Establish a strategic vision for your products**, aligned to organizational commitments.
- **Collaborate with other lines of defense** and consider how they are aligned to the requirements and data gathered.
- **Develop standardized requirements** to measure performance and compliance.
- **Design monitoring in a flexible but feasible way**, using processes that each team follows to provide meaningful signals.
- **Focus on small, impactful improvements**, leveraging feedback and data points from your monitoring to drive continuous improvement.

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 framework 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

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 following information is not intended to be "written advice concerning one or more Federal tax matters" subject to the requirements of section 10.37(a)(2) of Treasury Department Circular 230.

The information contained herein is of a general nature and based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your tax adviser.