Leveraging technology to help enhance trust in internal controls

4 ways you can work smarter, reduce risk and change the game with controls automation

The rise of material weaknesses (MWs) we've seen in organizations' SEC Form 10-K submissions between 2016 and 2021, 2022 and Q1 2023 can pose significant risks to organizations and undermine the trust of investors and stakeholders. Understanding the causes of MWs can be crucial for developing effective mitigation strategies.

Technology can help automate the operation and testing of controls — helping to increase overall trust and enhance the reliability and accuracy of financial reporting. Organizations can use these tools to help streamline processes, strengthen internal controls and reduce the overall risk of MWs — ultimately upholding the integrity of financial information and meeting regulatory compliance standards.

Enterprise resource planning (ERP) transformations are a great time to start your controls automation journey. While it's true that MWs are increasing, a well-planned intelligent controls strategy can help you prevent them. With an effective strategy in place, you can identify potential controls breakdowns early. The added benefit? Controls automation can help your organization reduce the cost of compliance.

View ERP transformations as an opportunity to help modernize your controls environment and shift the ratio of manual to automated controls in the right direction. But to achieve a resilient, efficient and sustainable enterprise ecosystem, it's not enough to simply automate controls by design; you should automate testing and monitoring as well.

In fact, the key to successfully bringing controls automation to life — specifically these four components — is execution of the control itself and testing efficiency.

1. Streamline security with enterprise systems security and configuration

- Security that provides “least privileged access” to users based on their jobs
- Goal: roles free of inherent segregation of duty (SOD) conflicts

Take advantage of standard configuration to drive appropriate posting authorizations or to drive the way a transaction behaves. Review specific configurations instead of sample-based tests to gain increased confidence over a higher population of documents. Rather than testing a sample of transactions to confirm their behavior, this enables you to test specific configurations in that application. By confirming that a configuration is set a certain way, you’re essentially confirming how that transaction will process.

Business application security is complex. Users should only have access to the system relevant to their job function. All too often, systems aren’t aligned with business requirements. This can lead to users having more access than necessary.

Your answers to these questions can inform your need for enterprise controls:

a. Do you know who has access to sensitive transactions?
b. Is your SOD risk defined at the system level?
c. Are you mitigating controls operation effectively?
d. Do you know if someone performed an incompatible function and what the financial impact is?
e. Do you routinely have to perform time-intensive look-back procedures?

2. Establish internal controls with monitoring / GRC technology

- Focus on automating controls design
- Use exception-driven analytics for manual controls, manual review of SOD / access violation report

Enable continuous monitoring of key configurations in the system and certain aspects of security. This is a fairly broad category — and there are applications and solutions you can use to implement or monitor risk, like certain types of GRC (governance, risk management and compliance) technology. You can leverage this technology to essentially baseline key settings and rely on continuous monitoring to alert for changes.

When you baseline these settings, if there's a change from what you expect and what you configure your GRC tool to look at, you'll get a warning. This way, you'll know there has been some type of change to a key control or a key configuration — or a security setting that you should be monitoring.

3. Use monitoring controls, controls automation and analytics

- Rules-based automation within a specific application
- Automated SOD management, automated configuration change tracking and transaction monitoring

Apply analytics to translate transactional data into actionable insights. Review results of analytics to identify outlier transactions and potentially fraudulent postings.

Controls analytics are extremely helpful in situations where you have large amounts of data that need to be analyzed for very specific attributes. We see this used frequently in fraud testing. You can use analytics to pinpoint risk in a large amount of data. From a testing standpoint, that can be quite helpful. Essentially, the analytics can use system data to find an outlier transaction that needs to be reviewed.

4. Use intelligent controls for exception-based manual activities

- Automate labor-intensive, repetitive activities across multiple systems and interfaces
- Combine traditional analytics with artificial intelligence technologies that learn over time and improve workflows

The final item is your manual activity. In controls automation, we're focused on the concept that all manual activity should be exception-based. This applies from both an execution and a testing standpoint.

Rely on automated configuration monitoring and analytics to provide only the items that require manual action or review. Reduce the time you spend on testing by focusing on exceptions resulting from analytics or continuous monitoring. These should be a small set of activities where you're unable to apply automation. Instead, use automation to get down to the exception — essentially the transactions or the data that should be reviewed manually.

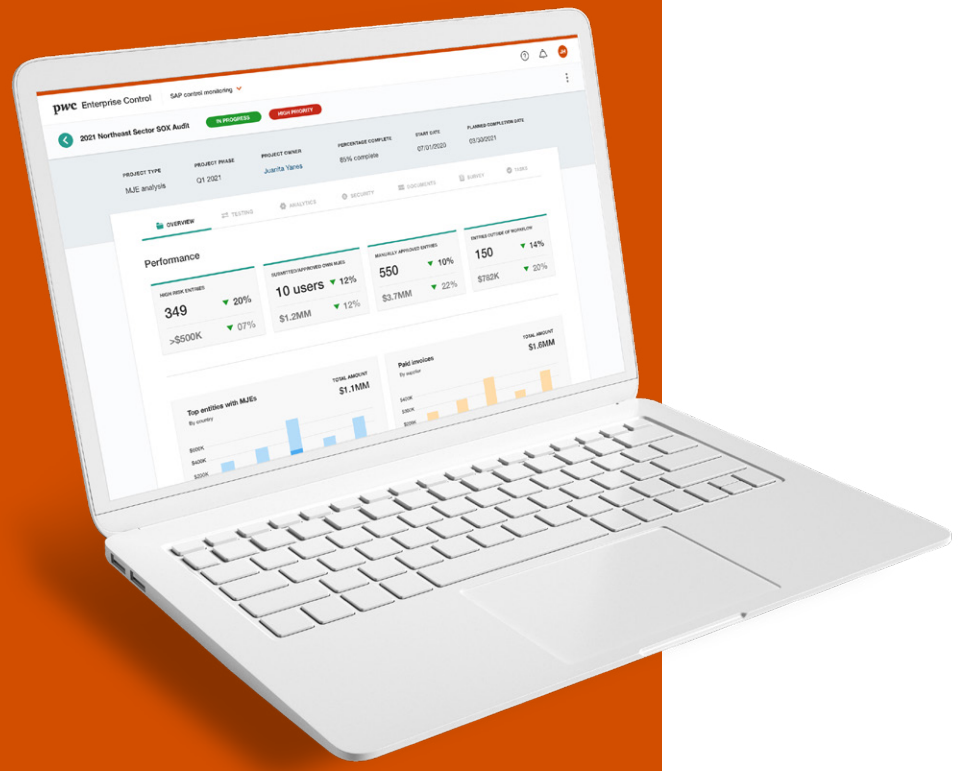
You might be wondering: When is the right time to do this?

The answer is:
There's never a wrong time to do this right.

Start by understanding the controls you operate today. Increased maturity amplifies the impact of technology by enabling more intelligent controls. Understanding the causes of MWs can be crucial for developing effective mitigation strategies. View ERP transformations as an opportunity to help modernize your controls environment and shift the ratio of manual to automated controls in the right direction.

Enterprise Control is a technology platform infused with trusted PwC knowledge to help you automate controls operation and testing. It can monitor systemic risks proactively with easy-to-use dashboards and can automate control testing in an end-to-end risk and control solution.

With Enterprise Control, you can lower the cost of compliance with automation, exert control over unexpected risks, and designate accountability to drive quicker response and results. This solution's ability to automate the creation of test workpapers is based on PwC's knowledge of enterprise applications and internal controls. Enterprise Control can help reduce the need for manual execution and testing time without sacrificing the quality and accessibility of information needed to produce results.



As technology advances and your workforce strategy changes, your business' automation should scale accordingly.

Enterprise Control allows you to work smarter, better leverage your current resources and drive your compliance program more efficiently. With PwC-powered technology and knowledge, Enterprise Control helps you manage risk and compliance costs.

Connect with our team to learn more.

Contact us

pwc

Enterprise Control

A PwC Product