SOX and the impacts from technology

May 24, 2022

Webcast summary

With rapidly changing marketplace and a multitude of regulatory requirements, achieving Sarbanes-Oxley (SOX) compliance is becoming tedious and costly. A technology-fueled approach with actionable insights can help modernize and streamline SOX programs in a cost-efficient way.

The webcast highlighted key considerations for optimizing SOX programs amid evolving technology changes and the emerging trends affecting SOX compliance.

The panelists addressed the following topics:

- Information technology (IT) audit focus areas
- DevSecOps and impact on SOX compliance programs
- DevSecOps risk and controls
- Securities and Exchange Commission (SEC) proposed cybersecurity disclosures.

IT audit focus areas

IT plays a critical role in SOX compliance in ensuring financial data security and accessibility. Although having the right resources and the ability to respond to technology changes remain the top concerns in IT audit, the following obstacles continue to hinder proper adherence:

Risk assessment

- Inconsistent involvement of IT professionals in business process walkthroughs—configuration or application access—affects the timely identification of Information Produced by the Entity (IPEs).
- Failure to detect relevant systems and tools supporting the flow of transactions in time causes inadvertent reliance on systems.
- There is a lack of the right people for identification of critical interfaces.

Automated controls testing

- Shortage of right skills to spot risks and corresponding controls in process walk-throughs result in process risk points being overlooked and not addressed.
- All configuration types or all relative data elements within a configuration—such as for inventory counts, revenue types, and accounts receivables—are often not tested to evaluate the specifics for configuration controls.

C&A of information in reports and IPE

- Identification of systems where relevant data is coming from continues to be the biggest focus area.
- Relevant data elements (RDEs) and calculations within spreadsheets need to be assessed by the control owner. The data is then required to be reviewed by the SOX auditor to test management's control and ascertain the right level of precision within the spreadsheet.
- It's crucial to understand the source of RDEs. As data moves from the source to the target system, such as spreadsheets, it is important to confirm the accuracy of RDEs as well.

Developer access to production

- As organizations move towards DevOps practices, they struggle to identify the appropriate mitigating controls over developers' access to production.

Change management

- Scope in tools that support change management process as a part of SOX testing. Often these ancillary tools don't require a full scope, but they do require testing around access controls to confirm they are being supported appropriately within the environment.

Third-party/SOC reports

- As organizations move to off-prem, cloud, or SaaS-based solutions, there is a growing reliance on third-party systems without SOC reports. Depending on inadvertent information within SOC reports continues to be an issue.
- Mapping SOC report with CUECs to client's control environments needs to be done appropriately to address risks.

Other areas

- System access is a major issue, particularly with a spike in initial public offerings. Private companies transitioning to public, or public companies acquiring private organizations, often lack mature controls and tend to have IT privileged accesses that are not appropriate from the SOX perspective.

- Instead of treating controls as a homogeneous population, verify that the controls support all applications and systems while testing. Find all the key attributes of a control to prove it is operating as designed.
- SOX teams continue to trust application controls or key reports that have inappropriate access, which eventually ends up being an inadvertent reliance.
- Journal entries continue to be a focus area, mostly due to the completeness of the populations. The key is to realize that there are several ways in modern systems to identify and create a complete set of populations efficiently.

DevSecOps and impact on SOX compliance programs

Having technology-enabled DevSecOps processes gives organizations the ability to pursue efficiencies by driving. Although it creates a challenge for compliance teams to keep pace with the changing paradigms and complex tooling, it also offers an excellent opportunity to leverage technology to move the control environment and testing program towards more automated and real-time monitoring controls.

Overview of DevSecOps

- Understanding your business model enables you to carefully consider different risks along the pipeline of changes in the environment, starting from inception to monitoring and response. A powerfully designed DevSecOps framework drives an organization's technology to meet the needs of its stakeholders more rapidly while allowing for seamless integration of security and compliance at scale.
- A culture of cross-collaboration is a core principle of DevSecOps. The collaboration across the development, operations, security, and compliance teams helps identify risks quickly and resolve security and quality issues during the development stage itself.
- A big difference between a legacy environment and DevSecOps is continuous testing that makes sure the code doesn't break and provides the desired outcome.

Key concepts and terms

- **Continuous build** occurs between the development and the build phase of the lifecycle. If the build doesn't complete successfully, or it doesn't meet business expectations, then the commit is sent back to the submitting engineer.
- **Continuous integration** operates between the development build and test phase of the lifecycle. Once the build loop completes, the build gets merged into the master branch, which initiates a series of automated and integrated tests.
- The level above that is **continuous delivery**, which is a feedback loop that iterates between plan, develop, build, test, release, and deliver. It's pertinent to understand that release and delivery do not necessarily mean the code gets pushed to production.
- The next step is **continuous deployment**, which acknowledges the features in the coding. It means that the code gets peer-reviewed and passes through all testing requirements before getting deployed. Above this phase is **continuous operation**, which integrates the feedback from the plan.
- The iterative loop—plan, develop, build, test, release, deploy, and operate—makes sure the development, security, and compliance teams are fully integrated and embedded as part of the development and operations cycle.
- What's important here is to have automation in these steps with minimal human intervention, thus improving the speed and delivery of the software to the market. It is also important to fully integrate cybersecurity in each of these phases.

Development models

Waterfall method: It follows a linear sequential design approach. It means having a master plan at the beginning and then logically stepping through the phases towards an end product. In this method, the development team needs to complete each project phase successfully before moving on to the next one, resulting in a longer process duration and less flexibility to incorporate real-time changes.

Agile method: It follows an incremental design approach, which incorporates continuous iterations and testing throughout the development process. The work plan is broken up into small chunks that allows development team to remain agile—by responding rapidly to the changing requirements and expectations of stakeholders while keeping pace with competitors. The feedback from testing is factored in and the flexibility makes it easy to prioritize and reprioritize.

As organizations scramble to respond to changing customer demands and digitize their services, agility gives them a competitive edge. Agile software development method is becoming a norm as opposed to the waterfall process, which prioritizes planning and structure over releases and effort, particularly within customer-centric organizations.

Software development best practices

- Over the last 30 years, software development best practices have evolved as new ideas, frameworks, capabilities, and radical innovations became available. We've moved away from the historic waterfall model that built monolithic applications to a nimble, microservices orientation where small teams are focused on narrow slices of functionality. Organizations are increasingly moving away from a physical environment to a cloud-based environment, where the operating system and IT infrastructure is quite disintermediated from the computing layer.
- These evolutions have enabled the implementation of a more dynamic software development process capable of facilitating real-time, frequent changes—DevSecOps. One of the biggest influencing factors for moving towards DevSecOps is efficiency driven by intelligent automation that allows a great level of control and a highly engineered, coded environment as opposed to manual configurations or processes.

Impact to SOX compliance programs

- The key to continuous building, integration, deployment, and operation is having a high degree of automation in place. This also drives a high level of complexity, particularly for SOX programs, as there is a plethora of tools available in the market.
- It is critical to understand which tools are in scope and at what stage. Start focusing on how those are being managed and which controls need to be tested.
- Keeping up with all the audits, scans, and regulatory requirements involves significant manual effort. Streamlining the compliance process with DevSecOps tooling and practices can help organizations stay compliant as well as improve program efficiency.

DevSecOps risk and controls

There is no one-size-fits-all when it comes to risks and controls. It's specific to the technology stack and the controls environment. And, with the approach of "shifting left," it's important to use only the controls that add value to the organization. With DevSecOps, it is possible to automate a greater number of controls and gain more reliability and assurance, but it also poses two risks in the SOX area: lack of documentation and developers having access to production.

Controls that enable you to address the risk of lack of documentation

- Have well-defined standards, policies, and branching strategies and communicate them clearly to the developers, product teams, and third-party contractors and vendors.
- Be able to bifurcate between critical and noncritical changes. Only critical changes have external rigor and are required to undergo the various agile controls.
- Conducting peer/independent review of the code by another developer makes sure it meets expectations and is ready to be deployed in production.
- Having robust code management verifies the code repository available for the developers' work is secured. Access to these codes gets reviewed periodically to make sure the entry point into the development process is well controlled.
- Automation in testing helps verify that every code change meets the criteria and has been successfully tested before it got deployed into production.
- Automation in release helps confirm that what has been developed and approved is the same code implemented in production.

Every organization is looking to have the ability to modernize the change management process that supports automated control testing and validation with no manual process of moving code into production.

Controls that enable you to address the risk of developers having access to production

- Robust logging and monitoring allows a quality review and approval of changes in a timely manner and helps mitigate risks of developers with elevated access.
- Ability to reconcile between the logs lets you oversee what went into production against what was done across the lifecycle of the change all the way from planning.
- Having segregation of duties—putting additional layers of access restrictions—prevents developers from having access to critical and conflicting business functions.
- Develop a preventative control mechanism that automatically requires a preauthorization before developers can make certain types of production data edits.
- Reducing the amount of code per deployment also helps reduce unintended vulnerabilities or bugs in each commit.
- Ability to roll back quickly to a known good state mitigates the risks of pushing new code to production.

Four key metrics for risk assessment

- **Deployment frequency** determines the frequency at which an organization can successfully release to production. A higher frequency of successful release means well-optimized processes and robust controls.
- **Lead time for changes** refers to the time taken for a commit to get into production A longer time suggests less optimized processes or insufficient automation.
- **Change failure rate** highlights the efficiency of the deployment process. The lower it is, the better.
- **Restoring a service quickly** is a good indicator of processing controls. It also shows your confidence to relate and use observability data around the change management process.

SEC proposed cybersecurity disclosures

Cost of cyberattacks

- Organizations have seen an uptick in cyberattacks and ransomware in recent years: the number of reported breaches by public companies over the last decade went from 28 in 2011 to 117 in 2020. From 2020 to 2021, ransomware attacks spiked by 93 percent. Companies feel that remote work has become a problem with their security breaches rising by 17.5 percent.
- Three biggest cyber threats last year were **compromised credentials**—consisting of 20 percent of attacks and $4.3 million in average cost; **phishing**—consisting of 70 percent of the attacks and $4.6 million in average cost; and **cloud misconfigurations**.
- The SEC believes that investors should be aware of these costs and would benefit from timely and consistent disclosure about material cybersecurity incidents.

Five proposed new rules

The SEC has released guidance on defining key terms (such as "information systems," "cybersecurity threat," and "cybersecurity incident") and has determined new standards for reporting should be applicable considering the current environment. It must be noted that these standards are currently in the commenting phase and are not policy.

Reporting cybersecurity incidents on a Form 8-K: This would require organizations to disclose a material breach within four business days of the organization determining the incident was material. Presently, most organizations are taking 268 days on an average to identify and remediate a breach, which makes this particularly difficult.

Disclosing cybersecurity incidents in periodic reports: Amendments to Forms 10-K and 10-Q would require periodic updates on material incidents by disclosing material changes, additions, or updates of incidents previously disclosed on Form 8-K, as well as disclosure of previously undisclosed immaterial incidents when material in the aggregate.

Disclosing cybersecurity policies and procedures: Organizations would require disclosing policies and procedures on cybersecurity risk management and strategy in Form 10-K.

Disclosing management's role in cybersecurity governance: This would require description of management's role in assessing and managing cybersecurity-related risks and in implementing cybersecurity policies, procedures, and strategies.

Disclosing cybersecurity oversight by the board of directors and the directors' expertise: This requires disclosure of the board's oversight of cybersecurity risk and board member cybersecurity expertise in annual reports and certain proxy filings.

Materiality

A key challenge for companies will be to identify incidents that are in fact reportable events. The SEC offers limited guidance and no quantitative thresholds for reporting. However, the SEC has the following considerations that registrants should take into effect in determining whether an incident is material:

- Incidents are material if there is a substantial likelihood that a reasonable shareholder would consider it important when making an investment decision.
- Registrants need to evaluate the total mix of information thoroughly and objectively, considering all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors, to decide whether an incident is material.
- Incidents must be reported within four business days after materiality has been determined, as well as the analysis needs to consider the incidence both individually and as an aggregate.

For example, if there is unauthorized access that compromises the confidentiality, integrity, and availability of data, or if there's an interruption or the loss of an application, then those are incidents that potentially should be disclosed.

Organization disclosures

There is no expectation that the registrants must disclose specific or technical information about their cybersecurity program. However, the disclosures need to be detailed enough so that a reasonable investor understands. Here are few considerations of what information registrants are required to provide:

- Description of the cybersecurity risk assessment program
- Engagement with assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program
- Policies and procedures in place to identify and manage any cybersecurity risks
- Previous incidents that impacted any financial or operational system and the capabilities to transact and record these financial transactions.

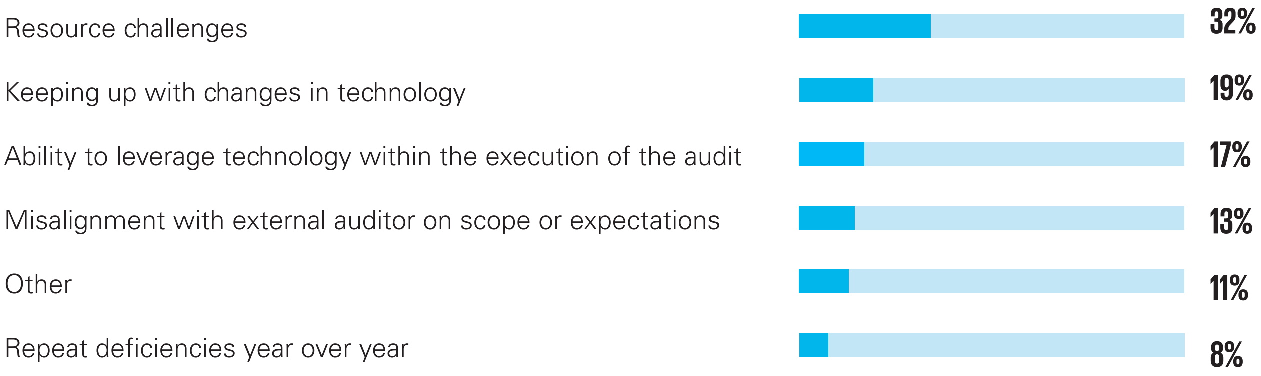
Role of leadership

Under the proposed rules, leadership and the board have very specific responsibilities when it comes to cybersecurity, and as part of these responsibilities, organizations must disclose their cybersecurity governance, including:

- Board members or a board committee that is responsible for the oversight of cybersecurity risks
- Processes by which the board and leadership committees are informed about cybersecurity risks and incidents and the frequency of such discussions
- Considerations about cybersecurity risks as part of business strategy, risk management, and financial oversight
- A designated chief information security officer or someone in a similar position who has the day-to-day responsibility for managing their cybersecurity program.

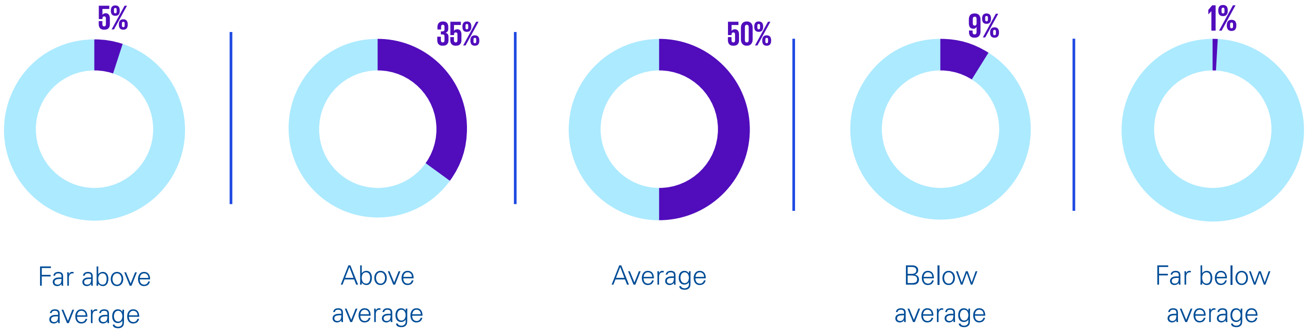
We polled individuals who hold various risk roles at their organizations, and here is what we discovered.

Which of the following is your biggest challenge related to your IT SOX audit?

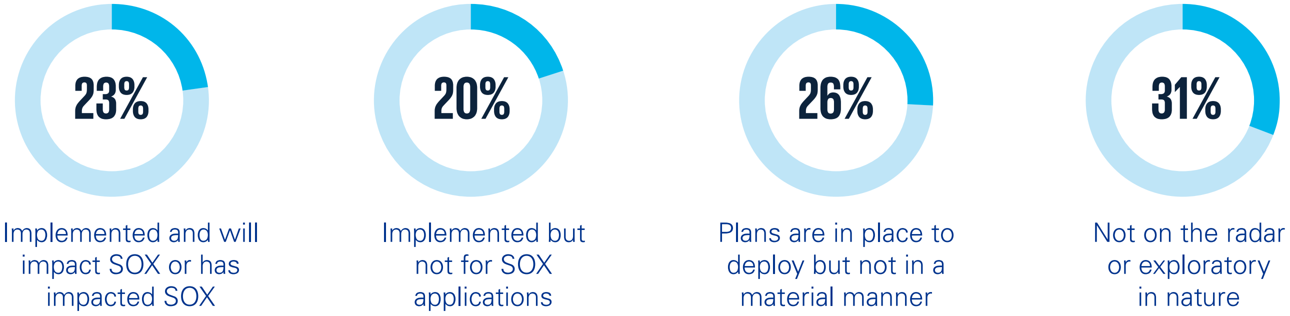


We polled nearly 1,500 individuals who hold various risk roles at their organizations, and here is what we discovered.

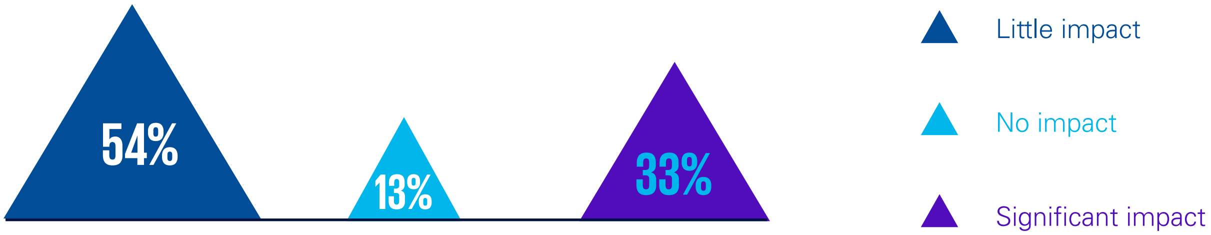
How would you rate your technology team's ability to meet customer needs?



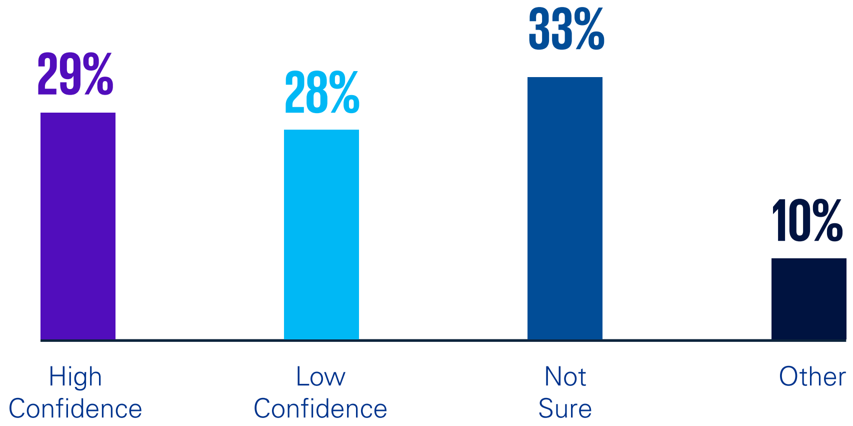
Where is your company's technology organization in the journey to adopt DevSecOps?



Do you think DevSecOps will have an impact on your SOX program?



How confident do you feel that your SOX program can identify and truly test the DevSecOps controls?



Data was gathered from responses to polling questions posed during our Future of SOX: SOX and the Impacts from Technology webcast, which took place on May 24, 2022.

For more insights, visit our Future of SOX webcast series page at visit.kpmg.us/FutureofSox

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 on such information without appropriate professional advice after a thorough examination of the particular situation.