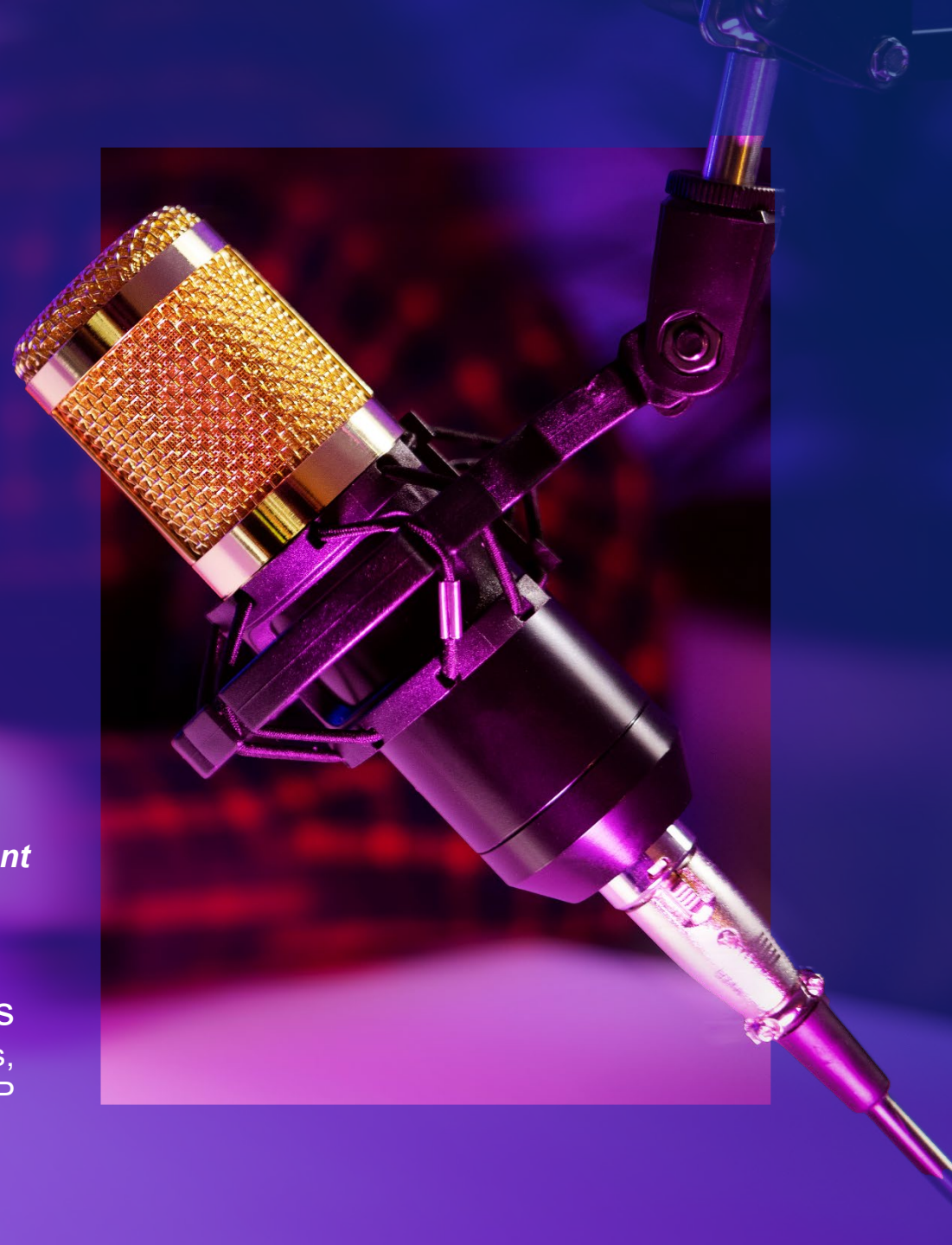
KPMG

Mastering IT Scoping for SOX Compliance

From Theory to Practice

> ***The most critical element of a defensible SOX program: the risk assessment. Too often, organizations treat it as a check-the-box document rolled forward each year, but that mindset must change. A well-executed top-down risk assessment isn't a compliance button –it's your most powerful strategic tool.***

–Subash Samuels
Principal, Internal Audit & Controls,
KPMG LLP



What's driving SOX challenges today

Based on the key findings from our February 2026 webcast, where we polled over 2,900 audit and risk leaders, the following facts have emerged that have defined today's SOX compliance challenges…

The SOX expansion era

52% of audit leaders believe the number of systems coming under the SOX scope for their organizations have increased

ICFR meets cloud chaos

69% believe the complexity of ICFR has increased as companies continue to transition to the cloud

Agile moves, docs don't

30% cite inadequate documentation as the primary risk associated with agile software development life cycle (SDLC)

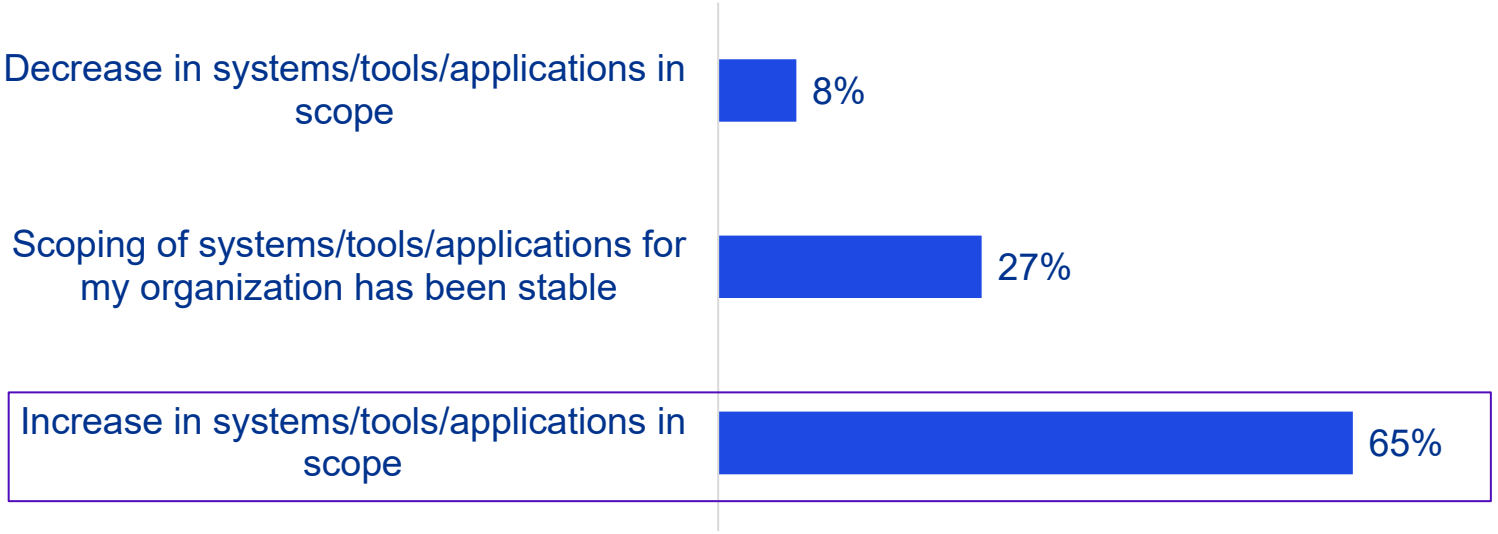
ICFR pain starts here

User access review deficiencies (**#1**) and key Report/IPE deficiencies (**#2**) are the biggest challenges faced by audit leaders in IT scoping for SOX compliance

Rising system counts are redefining the SOX landscape

Organizations are seeing a clear expansion in SOX system scope, underscoring the need to modernize risk-based scoping approaches so they can stay ahead of increasingly complex, cloud-driven financial reporting environments.

What has been your experience regarding the number of systems coming into scope for SOX scope for your organization?



> ***Technology runs everything these days. So, there's more applications that are becoming in scope…But if you apply Subash's five-question litmus test – like whether the system handles financial data, executes key controls, produces IPE, enables privileged bypass, or is an outsourced SOX-relevant system – and the system meets any of those criteria, then it should be considered for scoping .***"
>
> **—Steve Estes,**
> **US SOX Solution Leader,**
> **KPMG LLP**

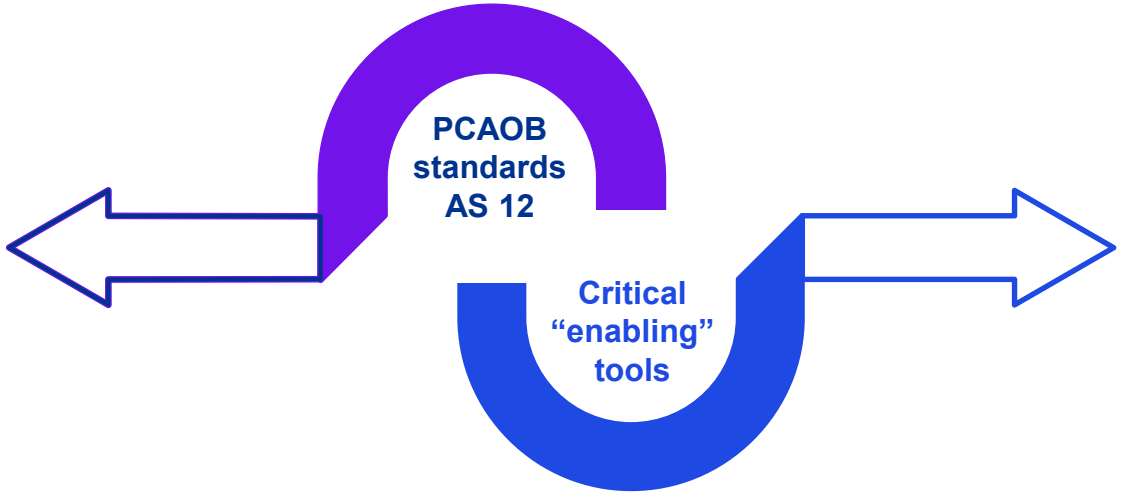
SOX scoping: The standard and the new reality

The foundation: the PCAOB standard (AS 12)

Our approach is anchored in the official standard, which dictates that a system is in scope if it:

- Processes financial transactions (initiates, records, processes, or reports them), or
- Is relied upon by key manual controls (for approvals, reviews, reconciliations, etc.)

Our scoping philosophy is built on two core pillars: the foundational guidance from the PCAOB and the practical reality of modern IT environments



"A complete SOX IT scope includes not only core financial applications but also the critical enabling tools that are relied upon to secure them."

– Subash Samuels, Principal, Internal Audit & Controls, KPMG LLP

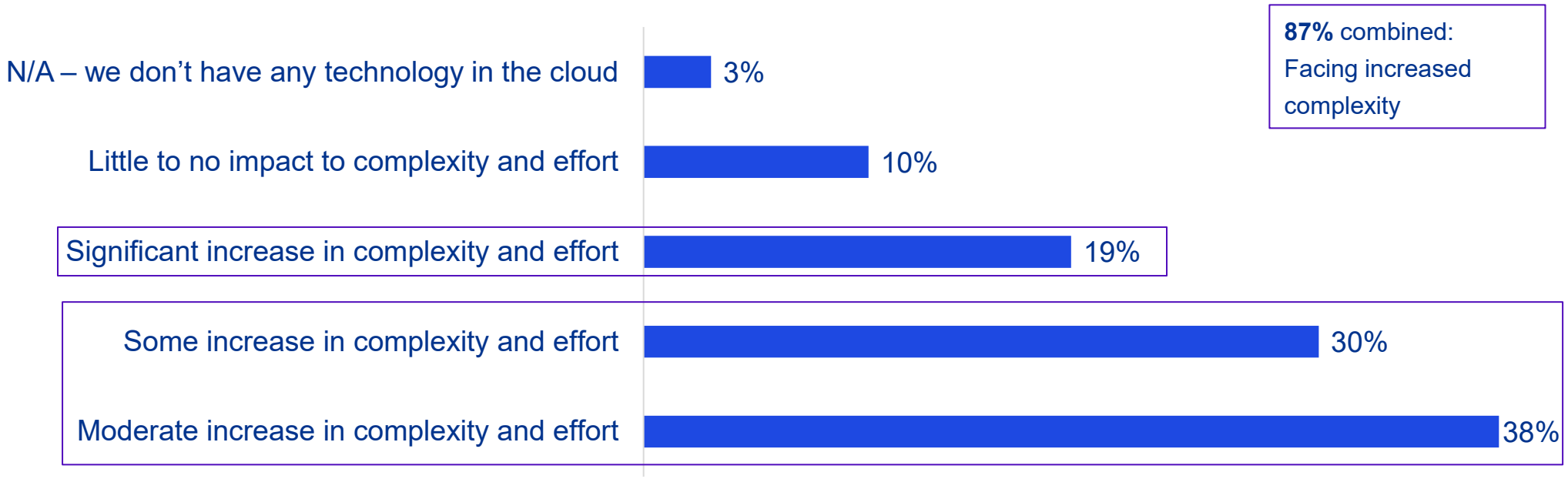
The new reality: critical "enabling" tools

A system is in scope if it is used to initiate, record, process, or report transactions that affect significant financial accounts

Cloud adoption is driving a new wave of ICFR complexity

With **87%** of respondents reporting increased complexity, cloud adoption is elevating ICFR demands by adding more configuration controls, expanding access oversight, requiring deeper SOC 1 scrutiny, and tightening validation of financial-impacting data flows.

What has been the ICFR impact of moving to cloud-based environments?



Complexity of modern dataflow architecture

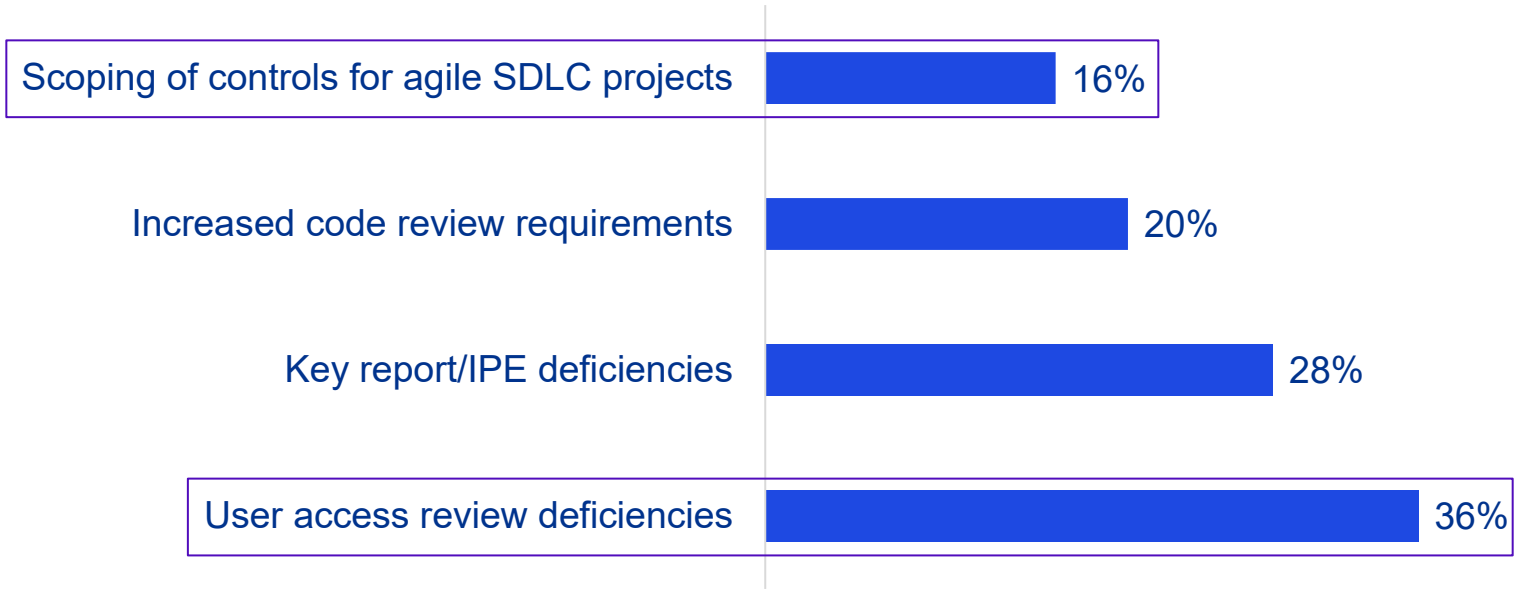
Data origins	Transformations		Consumption
Sources	**Ingestion**	**Storage**	**Access**
Systems of record containing business data	Applications used to connect and extract both batch and streaming data from source systems using automated pipelines	Data layer storage for natural and raw formats, consisting of structured and unstructured files, including cloud-native platforms	Controlled access to establish communication and information exchange between applications, as well as internal and external consumption, including microservices and APIs
Additional unstructured and structured data sources	**Data transformation and integration**		**Presentation layer**
	Industry-standard frameworks to convert, cleanse, and structure data into a common data model format for improved analytics and analysis		Data consumption via operational reporting, visual analytics, and application tools to support multiple personas
AI/ML, analysis, and analytics	Scalable, predictive modeling tools to enable enhanced and accelerated AI/ML models		
Data quality and metadata	Quality, observability, accuracy, completeness, lineage, and reliability		
Governance	Standard industry software to manage the accessibility, availability, usability, consistency, and trustworthiness of data for consumer usage		
Platform security	Modern technologies for protecting usability and integrity of an organization's infrastructure		

Where SOX efforts struggle the most…

This complexity isn't theoretical — it drives very specific, repeatable SOX failures

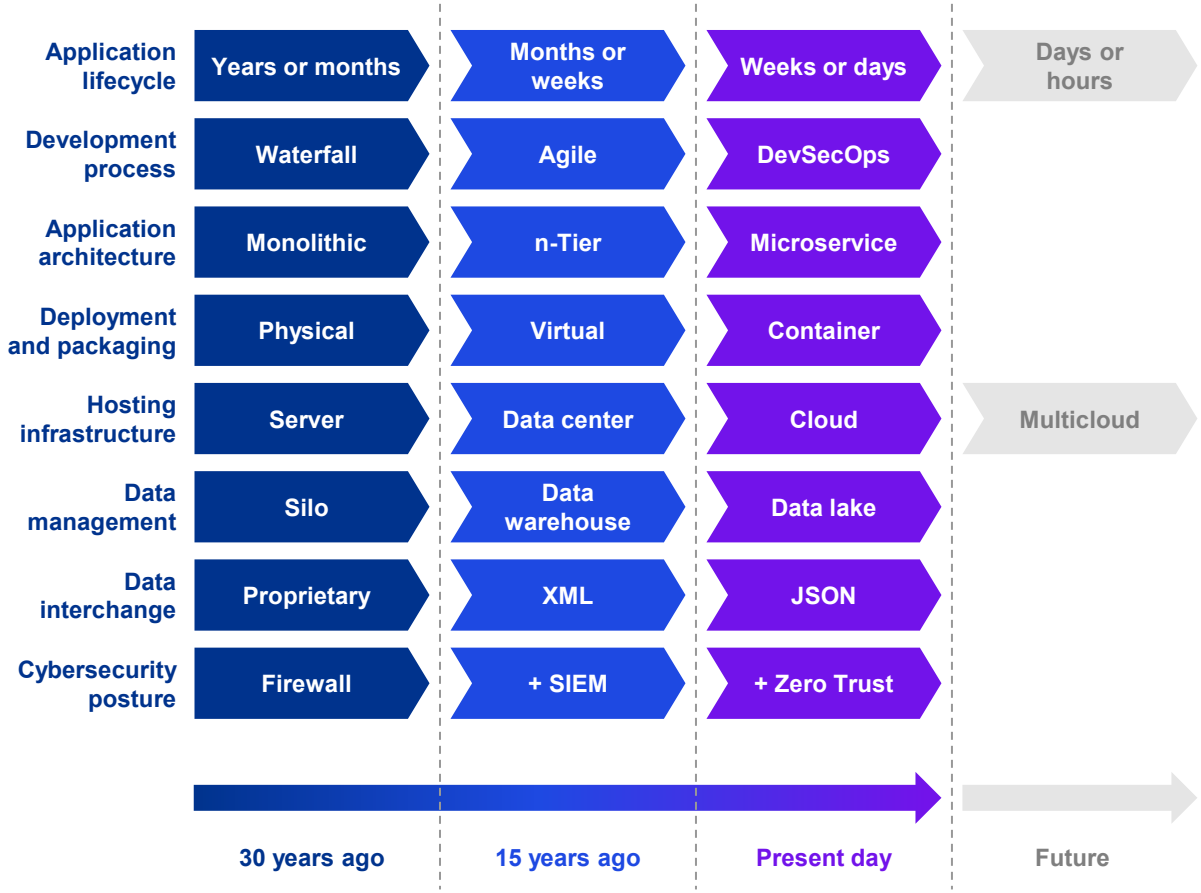
SOX issues such as user access review and IPE deficiencies, and increased code review requirements surface when organizations rely on informal knowledge, fragmented data, and reactive governance instead of structured, evidence-ready processes.

Biggest challenge faced by organizations in SOX compliance



> ***The whole concept of IPE first came out in 2012. And here we are, 15 years later, we're still struggling with it. So, I do think that is going to continue to be the gift that keeps on giving. Again, I know everybody's talking about AI solving all issues and yes, it is going to be amazing what it can solve or what it already can solve, but IPE is going to continue to be a challenge for us."***
>
> **—Sue King,**
> **US SOX Solution Leader, KPMG LLP**

Evolution of software development



Source: Department of Defense, Office of Prepublication and Security Review, May 12, 2021

Software development best practices are constantly evolving as new ideas, frameworks, capabilities, and radical innovations become available.

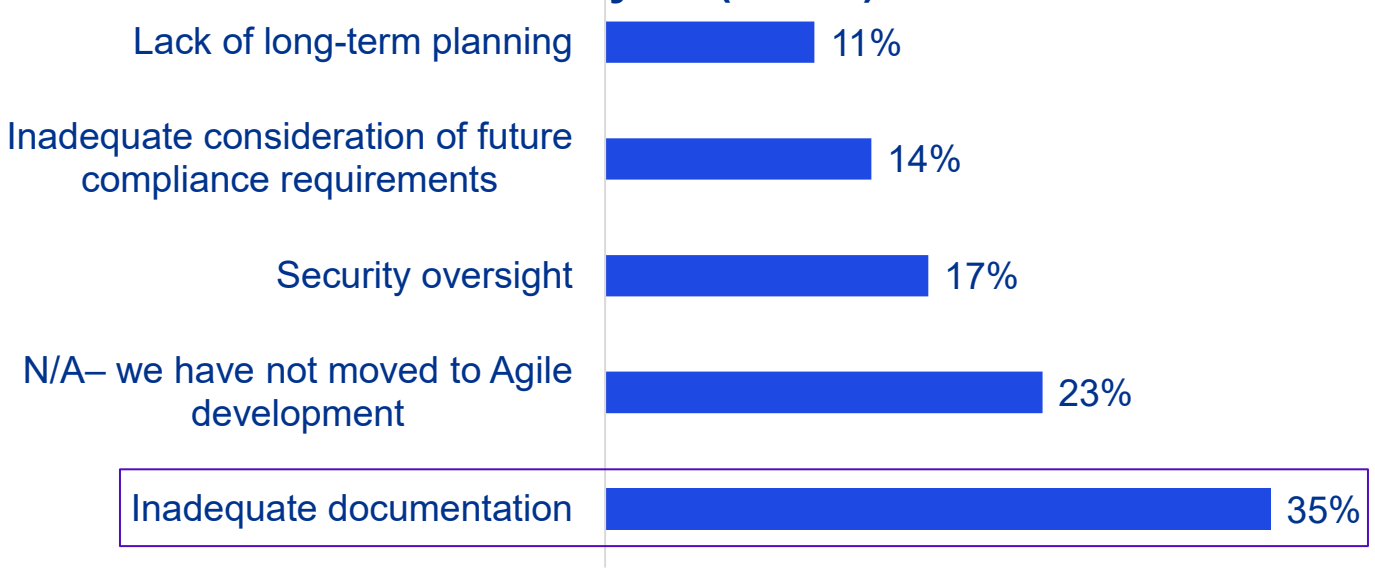
Over time, we witness technological shifts that relegate what was once state of the art to be described as legacy or deprecated.

Software is no different, and the graphic depicts the broad trends over the last 30 years. Different programs and application teams may be more advanced in one aspect and lagging in another.

The risks lurking in fast-moving SDLC models

Agile SDLC risks stem from inadequate documentation, outdated controls, and failing to redesign processes for Agile and DevOps, leaving fast-moving system developments exposed to weak governance and significant compliance risks.

What is your organization's primary risk associated with the Agile Software Development Life Cycle (SDLC)?



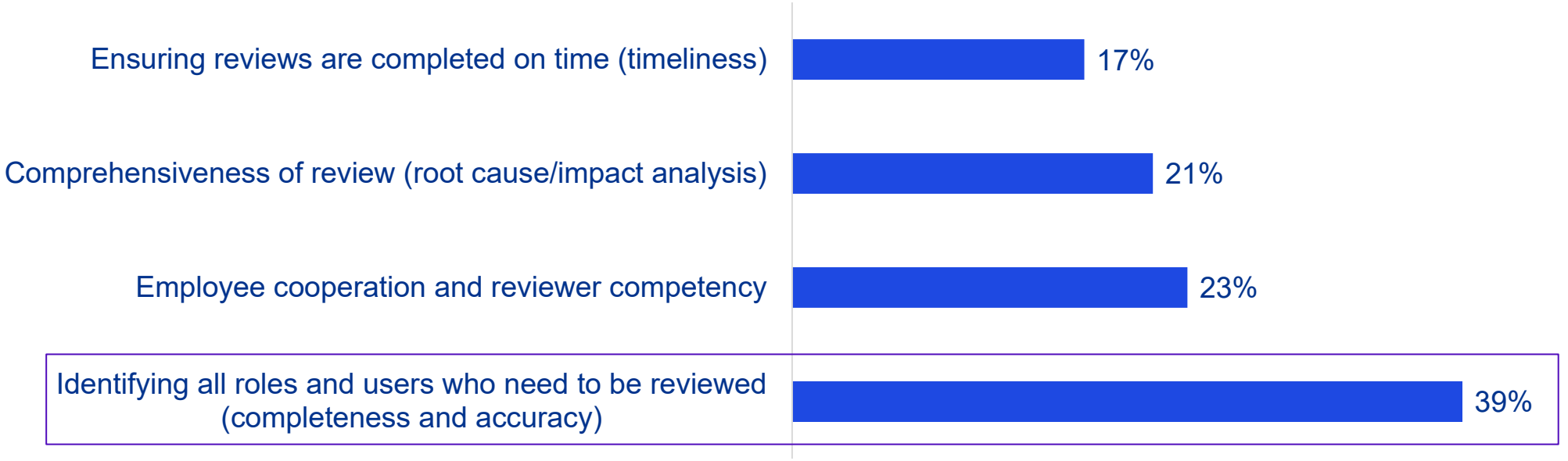
> ***Agile methodologies do introduce new risks into the control environment… You really cannot be counting on your old traditional waterfall SDLC controls… You have to shift with the way technology is moving and strengthen those controls in response to the new risks."***

—Subash Samuels,
Principal,
Internal Audit & Controls,
KPMG LLP

User Access Reviews: Small errors, big SOX problems

User Access Reviews break down when identity data is inaccurate or reviewers misunderstand permissions, leading to weak approvals; this competency gap, combined with incorrect impact analysis and timeliness, drives recurring ICFR deficiencies in organizations.

What does your organization find to be the biggest ICFR pain point for User Access Reviews?



User Access Reviews – Why do they keep being an issue?

Completeness and accuracy

- How will we evaluate the accuracy and completeness of the list being reviewed with respect to users, departments, locations, etc.?
- Are there adequate C&A procedures over all listings, including shared account listings?
- Is there precision in the review of shared accounts, and who has access to the accounts?
- Was the precision of the review performed at user role and permission level to determine appropriateness?

Timeliness

- Is there a defined timeline for the completion of review, and are there escalation procedures when the review is not completed within the defined timeline?

Reviewer competency

- Does management and the control operators understand the rights and privileges attached to the role?
- Are control operators being trained on the overall control risk?
- Who is authorized to perform the access reviews, and how are all reviews coordinated?

Lack of SOD as part of the review

- Who reviews the access of managers performing the reviews?

Root cause/impact analysis

- If inappropriate access is flagged, then how does management assess the impact of the inappropriate access (i.e., what activities were performed by that user account)?

A sample two-pronged approach for effective User Access Reviews

Implement an automated identity governance platform

A strategic solution that leverages technology to automate manual tasks for greater reliability and efficiency

- Automates data integrity: directly connects to source systems to generate complete and accurate user lists with a full audit trail, eliminating the need for manual IPE validation
- Enforces process by design: Automated workflows enforce deadlines with reminders and escalations while systemically preventing self-approval to help ensure SOD
- Integrates impact analysis: automatically creates tickets for both immediate access revocation and formal impact analysis when issues are flagged, helping ensure crucial follow-up

Formalize the process with an evidence-based checklist

An immediate, tactical approach that uses a formal checklist to enforce diligence and create a strong audit trail, ideal for nonautomated environments

- Mandate as official evidence: The checklist becomes the required, official evidence for every review; its submission is necessary for completion
- Prove diligent review: forces reviewers to formally attest to performing critical steps, such as checking for terminated users, SOD conflicts, and generic accounts and verifying specific permission levels
- Establish clear accountability: Formal sign-offs create clear accountability for both preparers and reviewers, which discourages “rubber-stamping” and reinforces ownership of the control

Persistent audit findings in User Access Reviews stem from weaknesses in manual processes and inconsistent oversight. A leading-practice approach directly targets these issues through a dual approach: leveraging technology for automation and data integrity while formalizing the human element with a structured, evidence-based review process.

The path forward: A practical playbook for advancing IT SOX scoping

While User Access Reviews remain the biggest immediate pain point, SOX leaders must also prepare for broader change-driving priorities to meet rising PCAOB expectations and increasingly complex technology environments.

Make risk assessment a living workflow

Continuously refresh risk assessment as systems evolve, business models shift, and new data flows emerge

01

Build defensible scoping rationale

Document both scope decisions and the reasoning behind them, supported by system and control mapping

02

Stronger evidence foundations

Ensure completeness and accuracy of populations, logs, and IPE before relying on them for conclusions

03

Rigorous core control execution

Ensure change, access, and ITGC testing is thorough, evidence-driven to prevent superficial reviews

04

Heightened third-party scrutiny

Reassess reliance on SOC reports and external data; understand coverage, assumptions, and residual risk

05

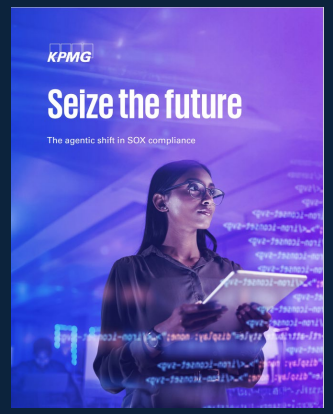
Prepare for emerging technology risks

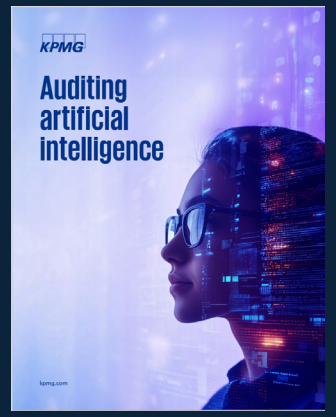
Enhance readiness for ai-related data flows, DevOps automation, crypto-related environments, and third-party dependencies

06

> ***"Risk assessment is really the gateway. It dictates everything that follows – from scoping and control selection to testing and evaluation. Without a robust risk assessment, you're essentially driving blind."*** —Subash Samuels, Principal, Internal Audit and Controls, KPMG LLP

Explore more by reading our recently-published thought leadership





For more internal audit insights, visit our thought leadership webpage:

The KPMG Future of SOX insights

Contact us:

Sue King
US SOX Solution Leader
KPMG LLP
E: susanking@kpmg.com

Steve Estes
US SOX Solution Leader
KPMG LLP
E: sestes@kpmg.com

Subash Samuels
Principal, Internal Audit and Controls
KPMG LLP
E: ssamuels@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**