Substantive Testing is Not the Answer: Perform Financial Risk Quantification Instead

Keri Bowman, Sr. Director, Product Marketing, Pathlock
John Scaramucci, Assoc. Director, Business Platform Transformation, Protiviti

Las Vegas

2024

SAPinsider

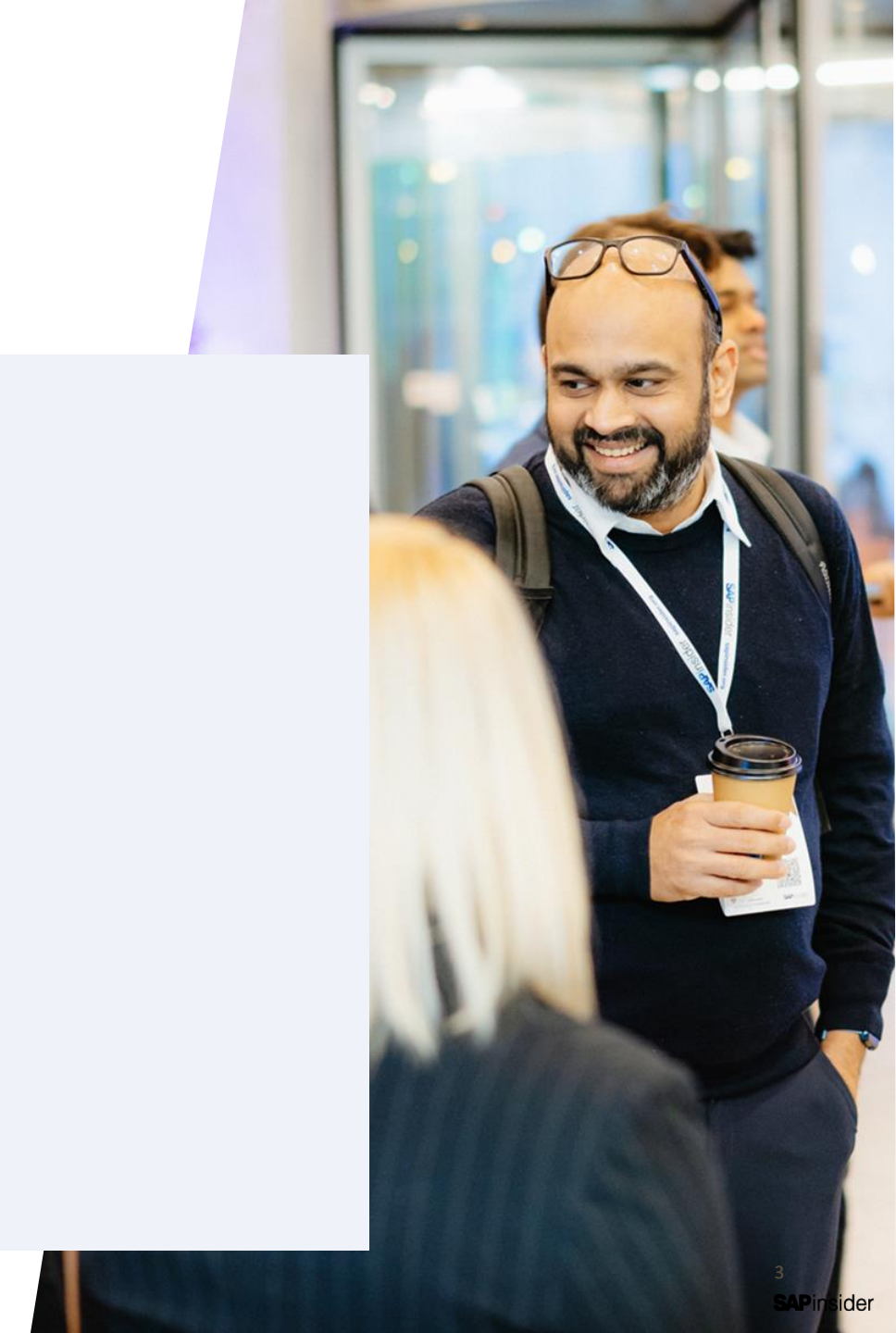
In This Session

We will discuss how to:

- Mitigate access risk with automated monitoring controls across your application landscape.
- Implement a process to engage business managers to review identified exceptions with detailed reporting.
- Develop effective access risk compliance and governance initiatives within your S/4HANA transformation.

What We'll Cover

- Intro to Access Risk Management
- Financial Risk Quantification
- Implementation Best Practices
- Access Governance and S/4HANA
- Wrap-Up



Access Risk Management

Let’s discuss the concepts and challenges of managing Segregation of Duties (SOD) and Sensitive Access risk

Common Problems involving Access Risk

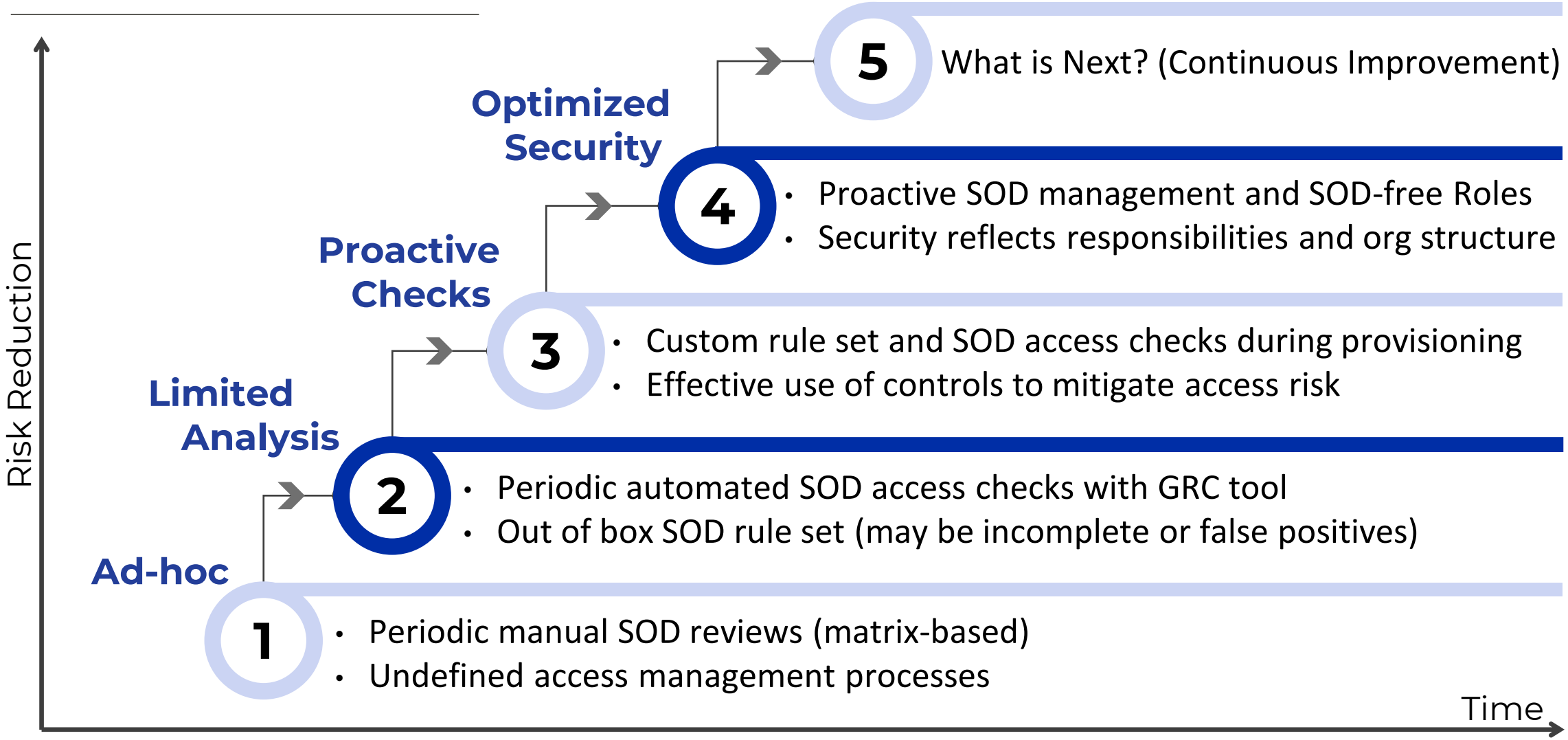
Company size and (risk) culture?

Security is not a priority (unless something is wrong)?

Risk appetite and regulations?

Organizational structure and complexity?

Access Management Maturity



Problems in Optimized Environments

Significant number of outstanding SOD violations after an initial remediation project

Expensive security redesign project fails

Mitigating controls do not address risk or are not performed regularly

Excessive use of “firefighter” as a cure-all for SOD issues

Increased scrutiny around control performance by compliance/audit

Wasted remediation efforts as next audits uncover new SOD issues

Organizational turnover

Competing priorities make maintaining integrity difficult

Financial Risk Quantification

A conceptual overview of mitigating access risk with Financial Risk Quantification and the associated benefits

Testing Approach Comparison

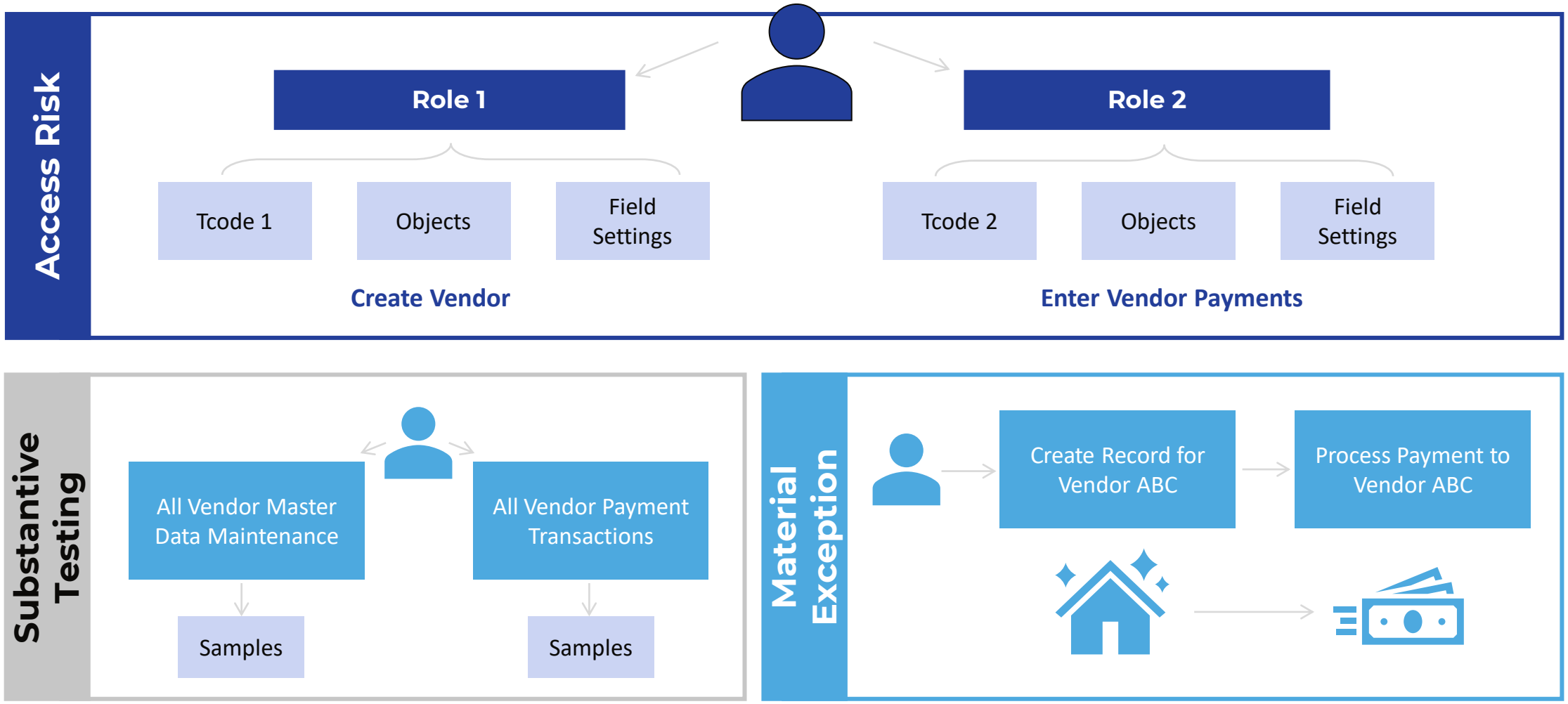
Typical Substantive Testing

- Based on reporting of “potential” violations
- Occurrences are investigated if issues are identified (audit or fraud)
- Excessive use of mitigation controls requiring additional validation
- Identification of conflicted or unmitigated users
- Often based on one side of the process
- Can have large time and cost associated

Financial Risk Quantification

- Identify who conducted actual risk violations (mitigated or unmitigated)
- Quantify how many times conflicting transactions were executed
- Calculate the precise financial risk exposure related to access conflicts
- Initial investment costs have tangible ROI
- Automation opportunities available

Materialized SOD Risk



Isolate Risk Exposure

"Can-Do" Access Risk

Example: 100's of users across many different countries have access to conflicting functions.

Test 100% of the Population

"Did-Do" Occurrences

###

transactions

$$$

Find the actual users who had carried out conflicting transactions, how many times, and for how much.

Quantify Financial Impact

Quantify Financial Impact of Access Risk

Gain Visibility to Powerful Insights

		Potential Risk		100%	Materialized Segregation of Duties Issue		
Example SOD Risks		**"Can-Do" Access Conflicts**		**Activity Volume**	**"Did-do" Transaction Violations**		
ID	**Description**	**Users**	**SODs**	**Business Process Transactions**	**Users (% of can-do users)**	**Exceptions (% of all transactions)**	**$ Value**
P001	Create or maintain suppliers and process supplier invoices	208	2,277	114,962	4 (2%)	1,040 (1%)	$5,149,290
P002	Create or maintain suppliers and process payments	22	105	28,739	2 (9%)	269 (1%)	$452,517
P003	Process invoices and process payments	37	83	110,941	3 (8%)	3,469 (3%)	$11,509,010
P004	Process purchase orders and process invoices	0	0	0	1 (>100%)	8 (>100%)	$65,000
P005	Process purchase orders and payments	23	248	22,138,321	0 (0%)	0 (0%)	$0

Only 2% of users with access performed actual transactions

Low access conflicts can still have a large material impact

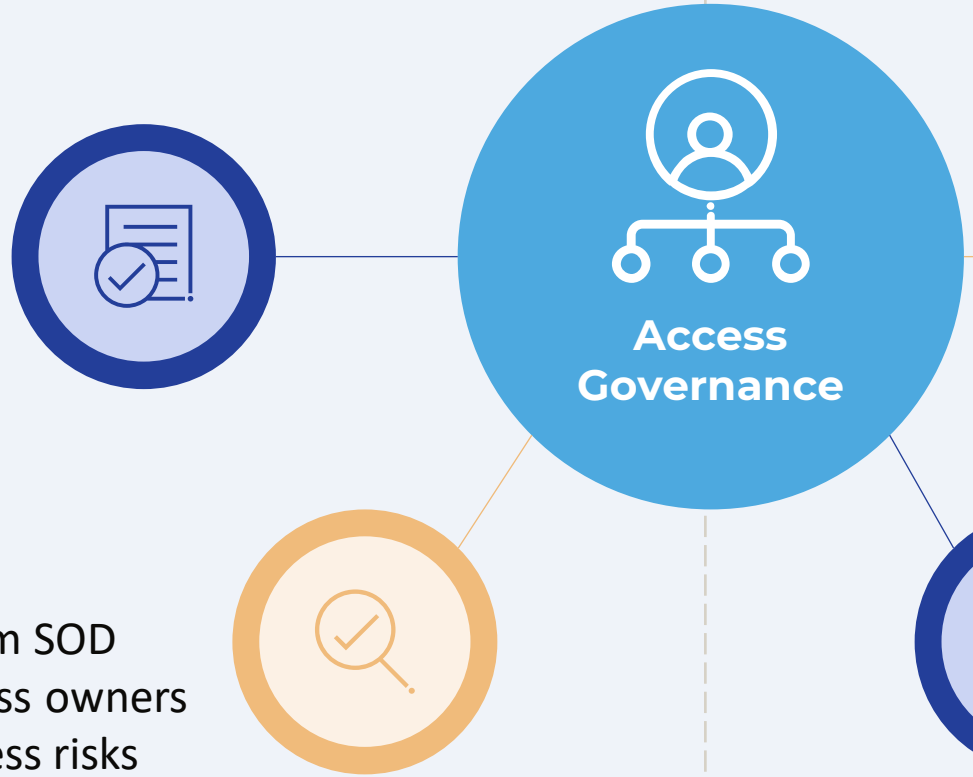
Users not found in point-in-time SoD analysis might have exceptions

Dramatically reduce effort when nothing occurred

SAP AVM by Pathlock

System Integration Edition
"Can Do" Analysis
Preventing

Risk Assessment Edition
"Did Do" Analysis
Detective



Extend
Extend the capabilities of SAP Access Control across enterprise systems

Mitigate
Act on what matters based on financial impact

Identify
Identify cross-system SOD violations so business owners know potential access risks

Monitor
Review user business transactions for materialized SOD violations

Implementation Best Practices

How to implement Risk Quantification successfully within Pathlock Access Violation Management (AVM)

Risk Quantification Use Cases

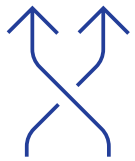
Before

Before SOD Remediation

Focus effort on truly high-risk areas

How Bad Is It?

During



During S/4HANA Implementation

Go live with leading practice transaction monitoring and SOD mitigation

Give Yourself Time!

After

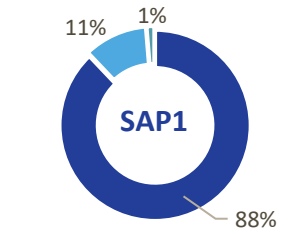
Ongoing Monitoring Controls

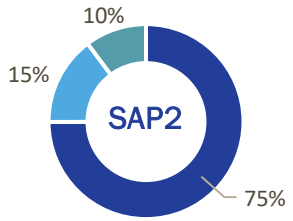
Gain visibility and control over outstanding SOD violations

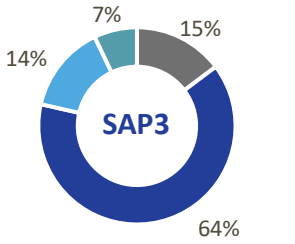
Stay on Top of Risk

Risk Selection and Prioritization

Coverage by System
(# of unique conflicts)



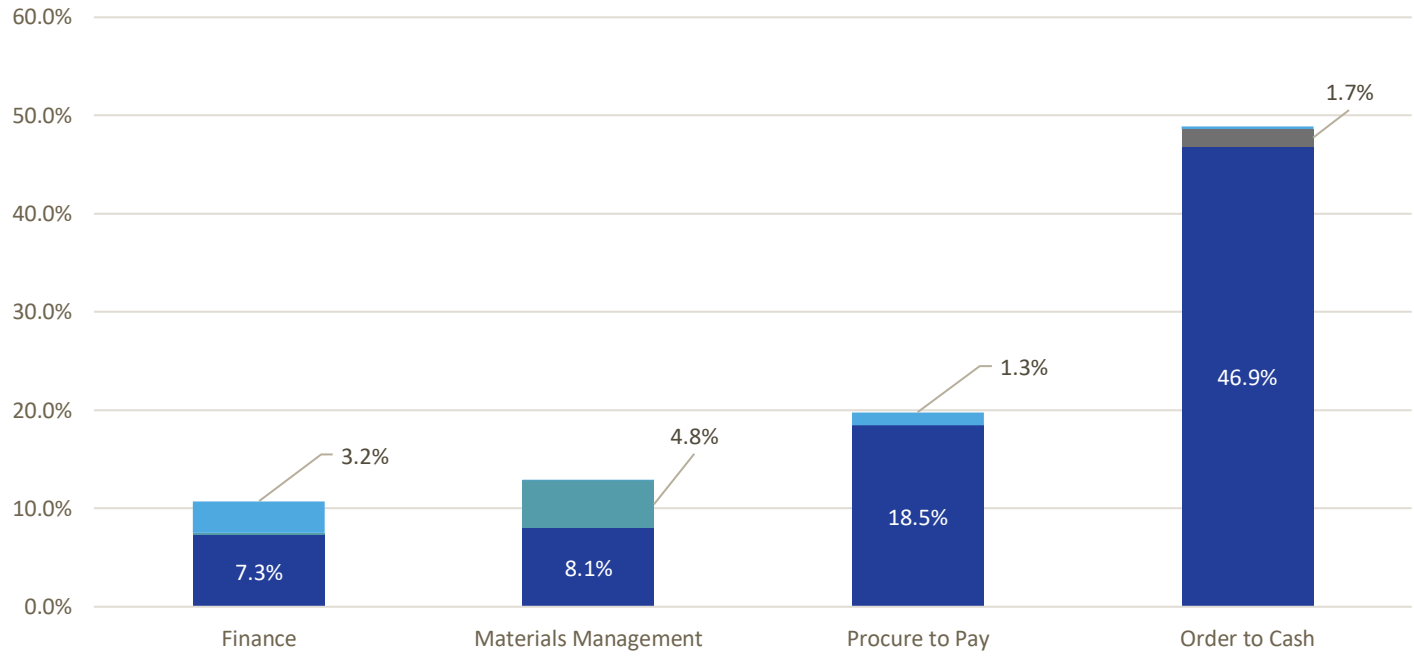




Legend

- AVM Control Proposed
- AVM Control Proposed (Cross System Risk)
- AVM Control Proposed (Some Customization Required)
- Non-Quantifiable or Significant Customization Required

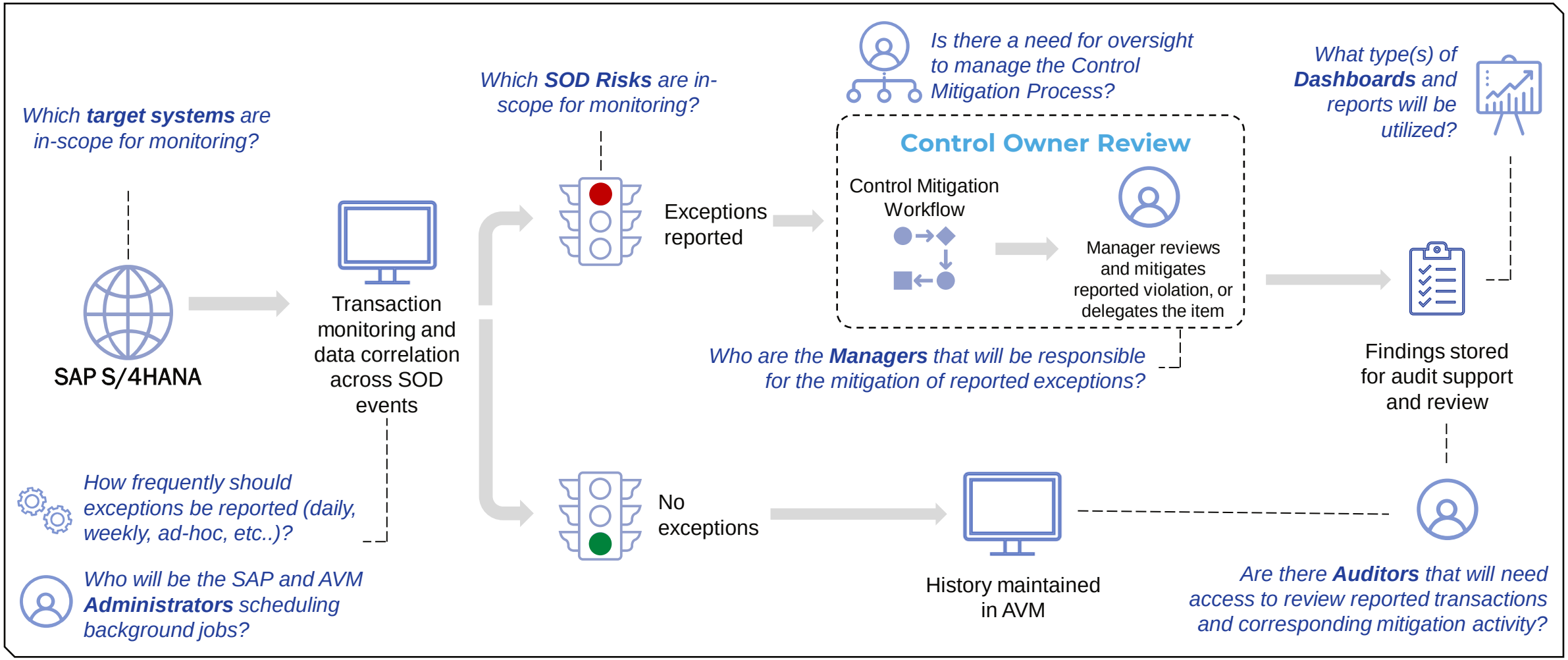
SOD Risks with AVM Coverage by Business Process



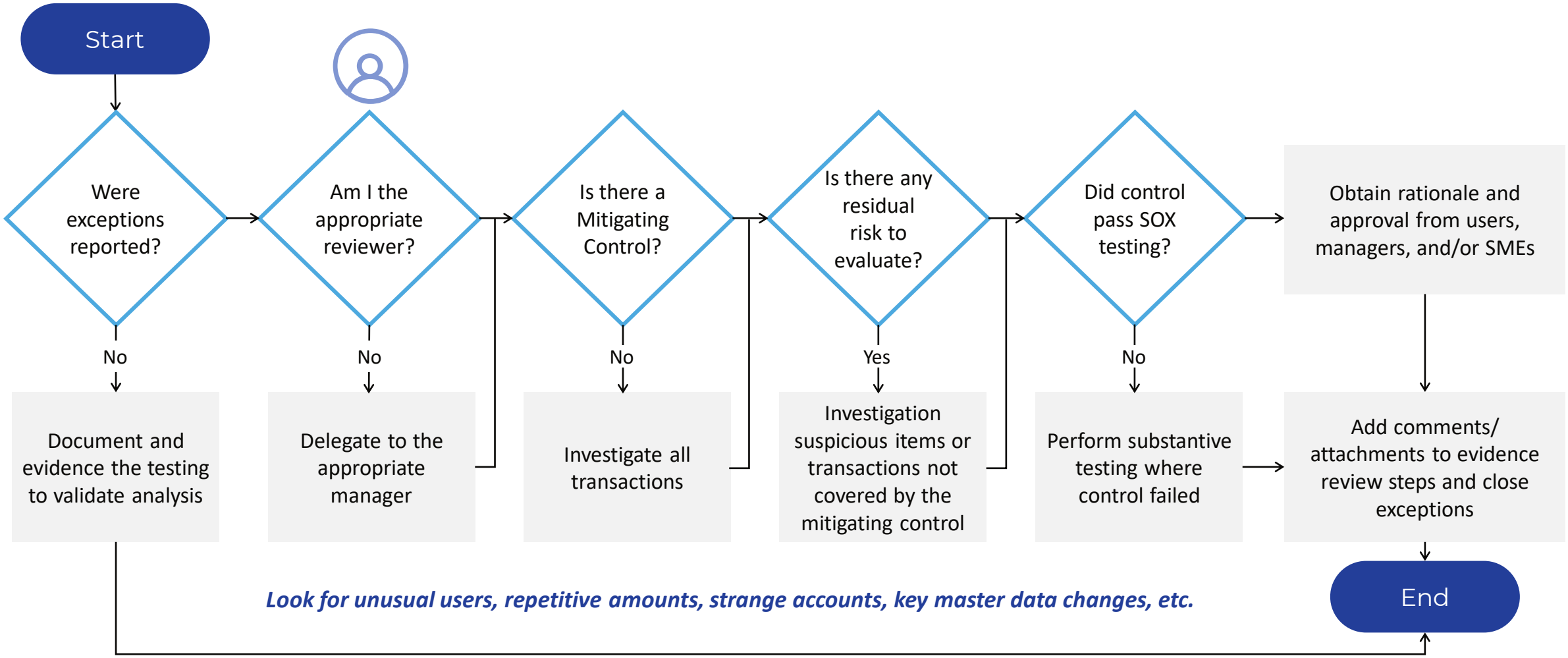
Notes:

- User access statistics based on GRC Access Risk Analysis
- Counts and percentages are based on non-distinct conflict counts (i.e., number of unique user-risk combinations)

Monitoring Process Design

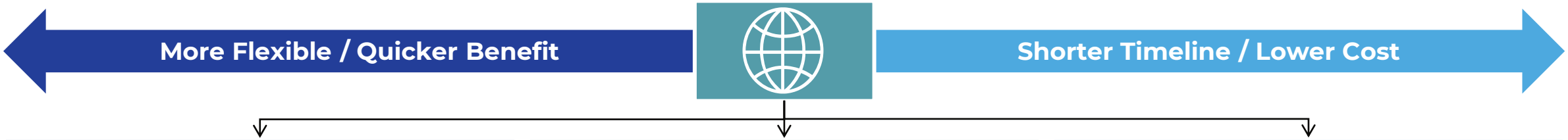


Example Control Owner Review Process Flow



Look for unusual users, repetitive amounts, strange accounts, key master data changes, etc.

AVM Implementation Options



Multiple Rollouts by System

Phased implementation plan where SOD quantification monitoring using AVM is deployed for one SAP Production environment during a Phase 1, followed by subsequent SAP systems during additional phases.

Pros	Cons
• Realize benefits more quickly than "Big Bang" • More flexibility for business/IT schedules • Establish repeatable program for Phase 2+	• Longer timeline to fully deploy • Higher cost of implementation

Releases Prioritizing SOD Coverage

Deploy a Release schedule for High Criticality SOD risks across multiple environments to enable better planning and user adoption:

- Release 1: Top 50-55% of Total High SODs
- Release 2: Next 30-40%
- Release 3: Remaining 5-10%

Pros	Cons
• Fastest realization of benefits • Lower cost than #1 • Allows for customization time	• Potentially more time required from SAP business and IT leads

"Big Bang" AVM Deployment

An alternative option is to fully deploy AVM within a single Release across all target Production environments as part of one Go-Live. This approach is typically not recommended for larger organizations.

Pros	Cons
• Shorter timeline overall to fully deploy • Less implementation cost	• Hard to adjust solution design once testing has started • Increased demand on business and IT resources

Typical Resource Allocation

The following table summarizes the commitment estimate of different resources for each phase of an implementation project:

Project Activity	Level of Effort Required				
	Project Team / GRC Lead	Business Process Owners / End Users	SAP Security	SAP Basis / Dev	Compliance / Internal Audit
Planning, Blueprinting, & Design	High	High	High	Low	Medium
Build / Configuration	Low	Low	Low	Medium	Low
Unit Testing	High	Low	Medium	Low	Low
User Acceptance Testing	Medium	High*	Medium	Low	Low
End User Training	Medium	Medium*	Low	Low	Low
Go-Live / Hypercare	High	Low	Low	Low	Low

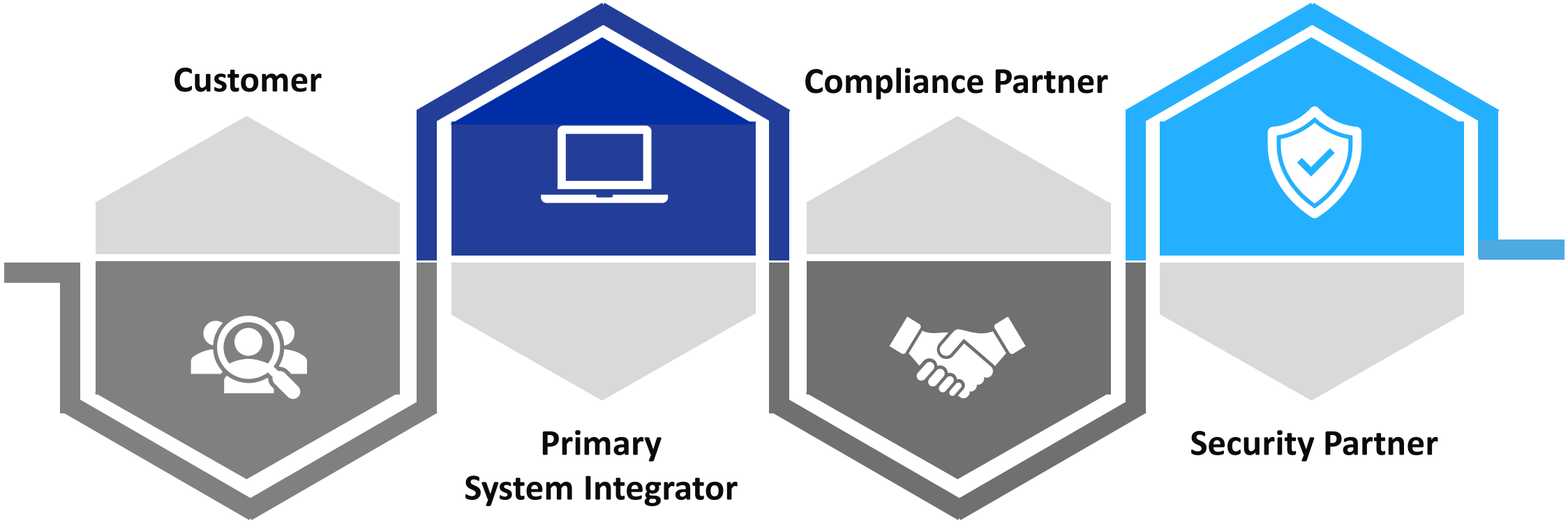
Level of Effort	Hour Estimates (per week with Key Activities)
Low	0 – 4
Medium	4 – 8
High	8 – 12

**Level of involvement from Business is dependent on the solution design (i.e., whether reported exceptions will be pushed out to the Business after go-live)*

Developing Access Governance

How to cultivate compliance initiatives into a sustainable Access Management program during an S/4HANA transformation

Defining Key Partnerships



Compliance Workstream Overview

GRC, Security and Controls should be considered from the beginning of your S/4HANA transformation journey.

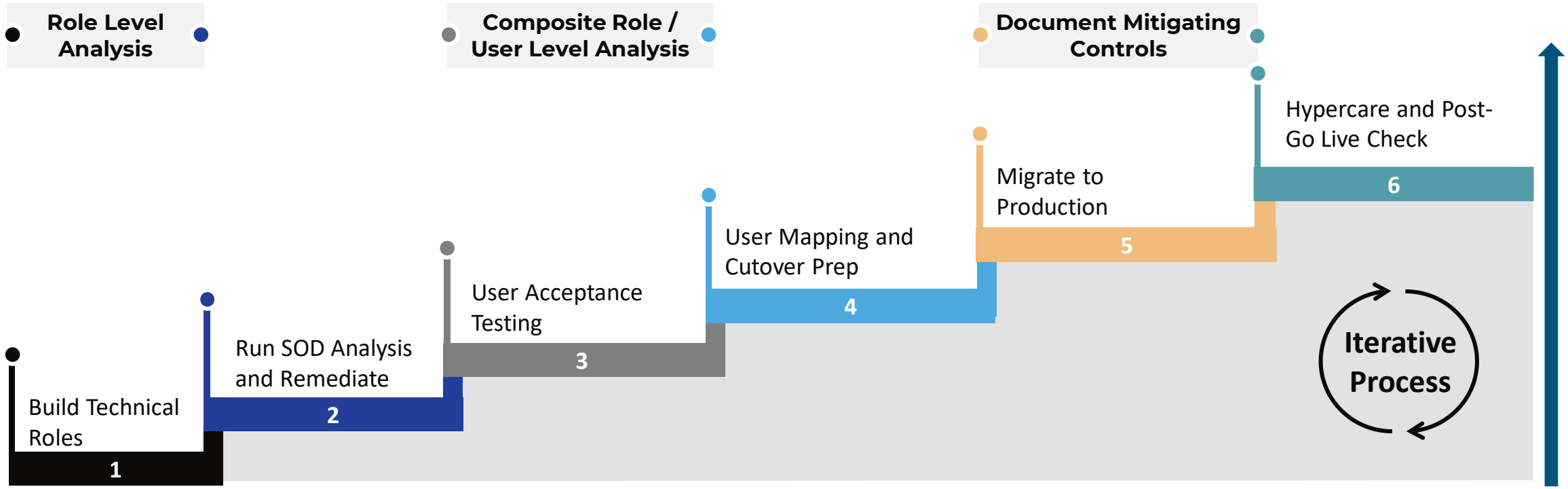
By integrating compliance initiatives from the start, you can ensure your system is going live with key strategies (e.g., Access Management, Role Design, Monitoring Controls, etc.) that will help ensure your system stays compliant with regulations.

The compliance workstream should consist of the following core areas:

- **GRC** (Risk Analysis, User Access Reviews, Firefighter)
- **Security** (Role Design and Maintenance, User Provisioning)
- **Controls** (Risk Quantification & Other Monitoring)

Pre-Implementation SOD Review Process

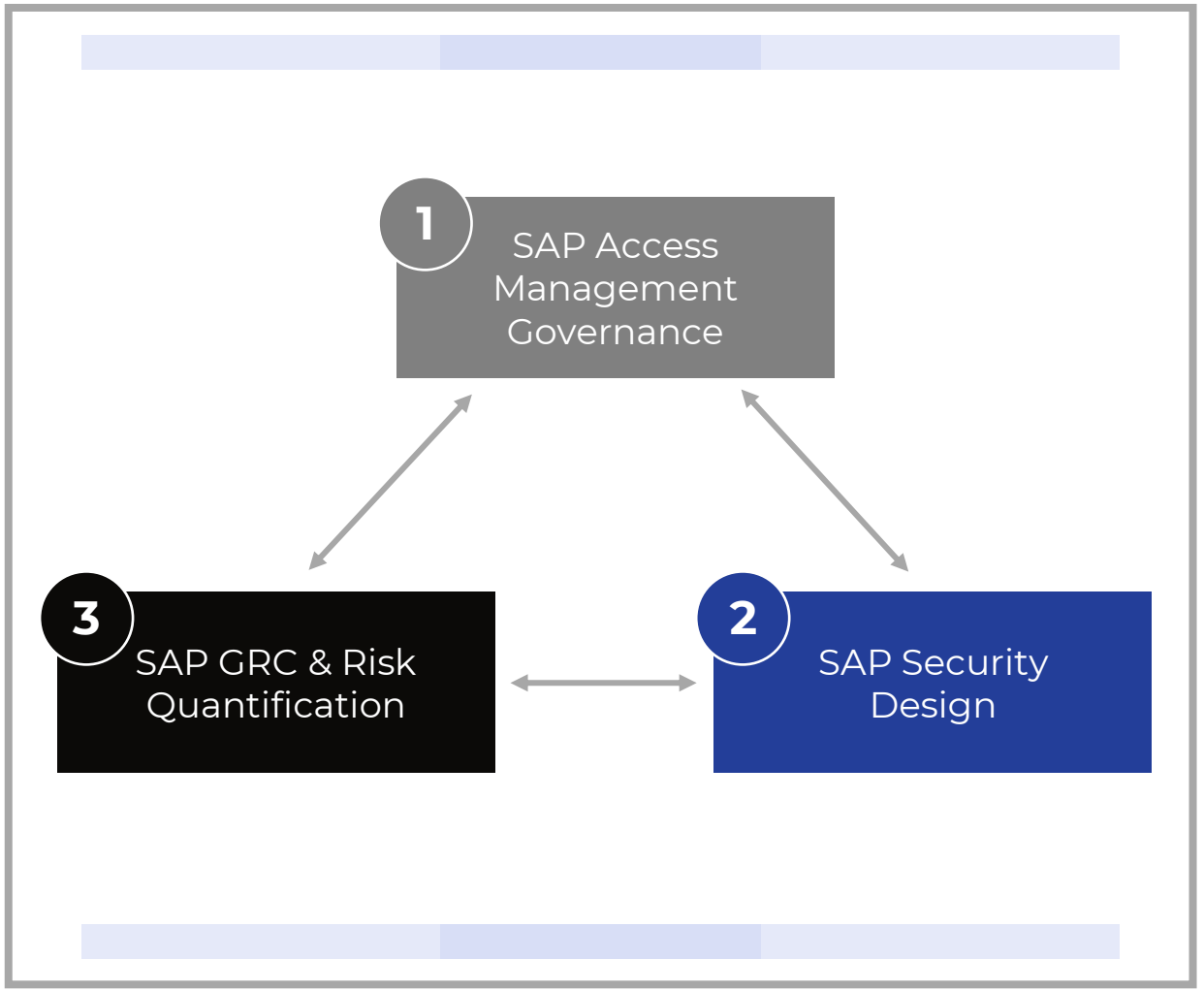
The following steps provide a brief overview of an approach for building security and SOD management processes. The GRC / security support team provides timely assessments to system implementors to ensure that technical roles are risk-free and that the user assignment minimizes as much risk as possible.



Ongoing Security Maintenance

The SAP Access Management Governance & Strategy should consider:

- Global Role Template Standards
- Role Naming Conventions
- Change Control
  - Adding Transactions to Roles
  - New Fiori App Requests (Note: We often see an uptick in this as the organization starts to recognize the capabilities of Fiori)
  - Role Owner Changes
  - Role Design Changes / New Roles
  - Impacts to Risk Quantification



Ongoing Control Maintenance

The below should be considered and managed to ensure automated Risk Quantification monitoring controls as well as your organization continue to stay compliant:

- Changes to org structure
- Personnel changes (e.g., control owner)
- Changes to the risk environment
- New Systems, New Functionality, Process changes

Wrap Up

Where to Find More Information

Key Points to Take Home

Q&A

Where to Find More Information

Introducing Pathlock Cloud's Continuous Controls Monitoring - Revolutionizing Compliance and Risk Management

- Blog post from Kyle Benson detailing the new Pathlock CCM solution (March 2024)

System Integrator or Security Specialist: Who Should Be Responsible for Implementing S/4HANA Security and Controls?

- Blog post from Mohammed Abdullahi, an SAP Security SME with Protiviti (January 2024)

How to De-Risk Your S/4HANA Upgrade Strategy

- Steve Apel, a Director at Protiviti, discusses the intricacies of S/4HANA migration from the Pathlock Innovation Series (December 2023)

Managing Risks Along Your SAP S/4HANA Journey

- Protiviti POV on How Internal Audit and Compliance Functions Can Support S/4HANA Projects (September 2022)

SOD Empowerment With SAP Access Violation Management By Pathlock

- Paper describing how organizations can handle SOD and mitigations most effectively when they use automated tools (March 2022)

The Total Economic Impact™ Of Pathlock's Access Violation Management (AVM) Solution

- Forrester's TEI study on how a Fortune 5000 enterprise saved over $1.8M by leveraging a part of Pathlock's capabilities (January 2022)

Key Points to Take Home

- Risk Quantification can add significance and give better visibility to SOD issues than typical substantive testing
- There is a significant difference between ‘potential’ SOD violations and ‘real’ financial impact
- Monitoring of known risks can start immediately to reduce risk and prove compliance
- Not every SOD in your rule set can be quantified – usually only financially relevant transactions are included, and many risks will never materialize in day-to-day business activities
- Include the Business and IT (and Audit if necessary) when implementing an Access Risk Management program to ensure proper scoping is performed up front and all expectations are met
- Automated processes for access risk and transaction monitoring can temper management pressure to resolve all conflicts during and after an S/4HANA implementation

Thank you! Any Questions?

Keri Bowman

LinkedIn.com/in/kbowman1/

John Scaramucci

LinkedIn.com/in/johnscaramuccijr/

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group with more than 800,000 members worldwide.