

How to Revolutionize and Harmonize Compliance Processes over SOD Access with Pathlock AVM

Vijan Patel, Managing Director, Protiviti
John Scaramucci, Associate Director, Protiviti

SAPinsider
Las Vegas

2023

SAPinsider

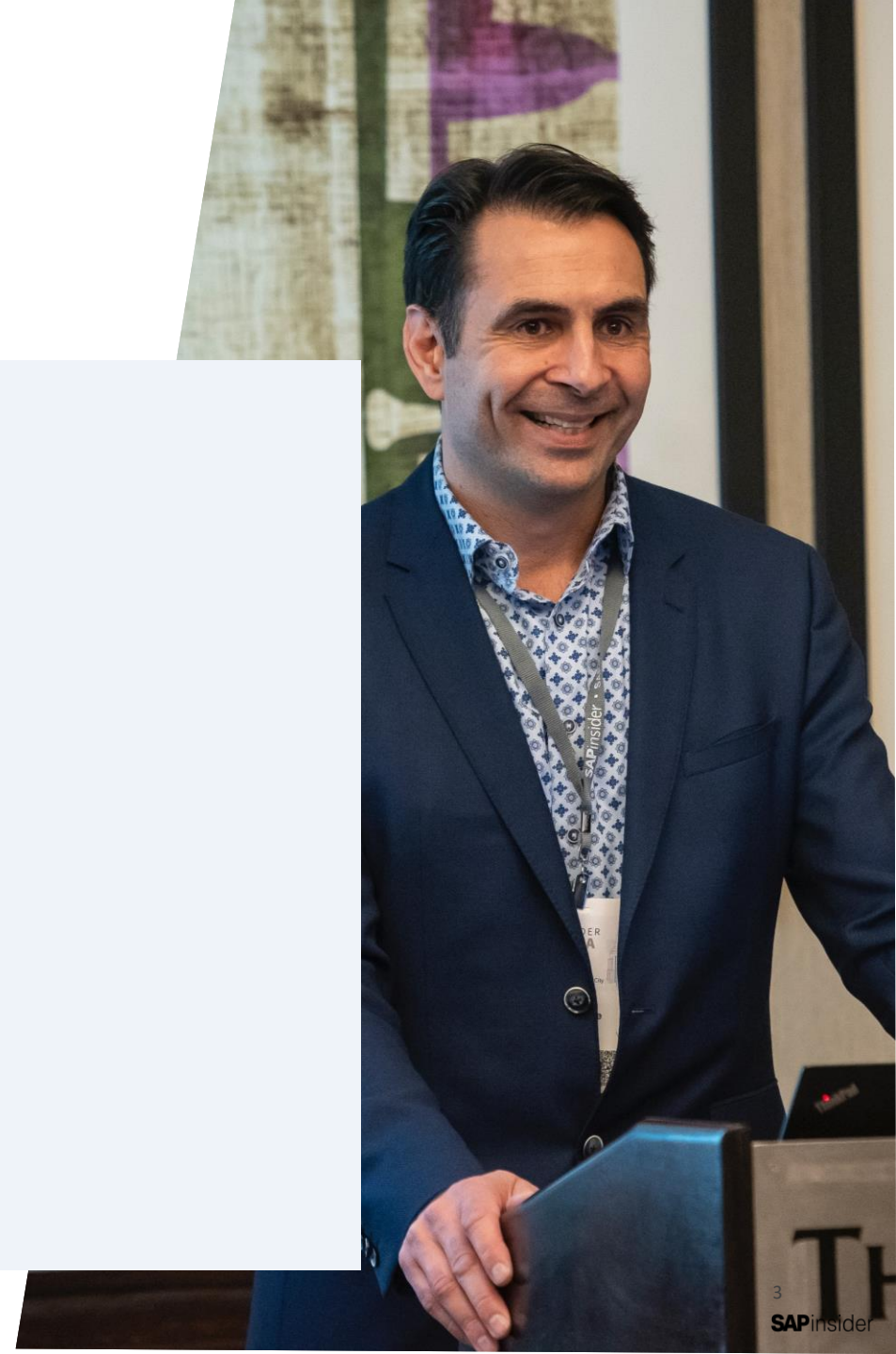


In This Session

- How AVM supports the security monitoring process
- Critical factors that drive the AVM implementation effort, timeline, and success
- Review SAP and cloud configurations needed for AVM integration
- How to deploy AVM as the repository of SOD mitigation and integrate expectations

What We'll Cover

- SODs Is Hard
- The Right Tool
- Too Much Data
- One Company's Journey
- Wrap-Up



Segregation of Duties (SOD) Is Hard

This section will explain the concepts and challenges of Segregation of Duties (SOD) management.

What Is Your (SOD) Problem?



**Company size and
(risk) culture**



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

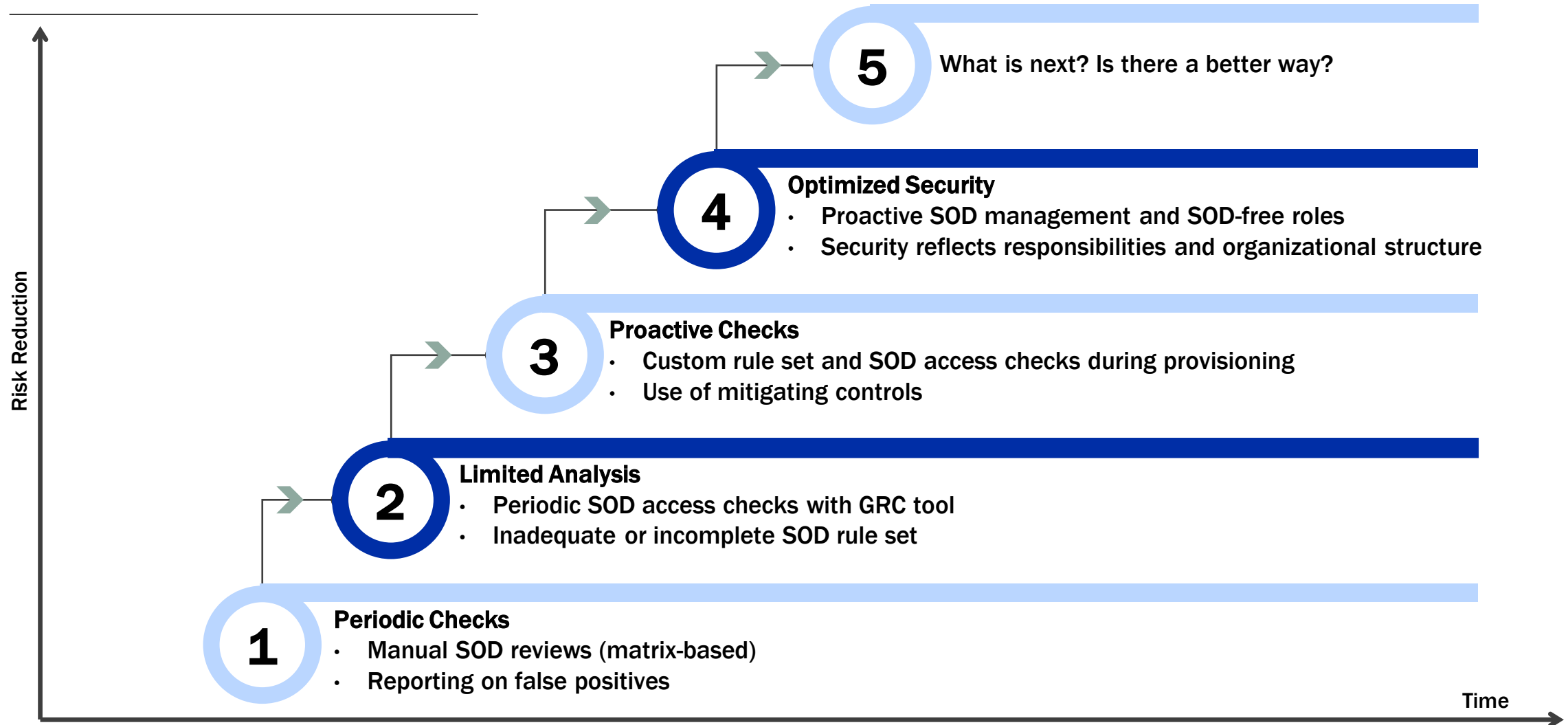


**Risk appetite and
regulations**



**Organizational
structure and
complexity**

SOD Risk 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

Is There a Better Way?

Provisioning with SOD Solutions

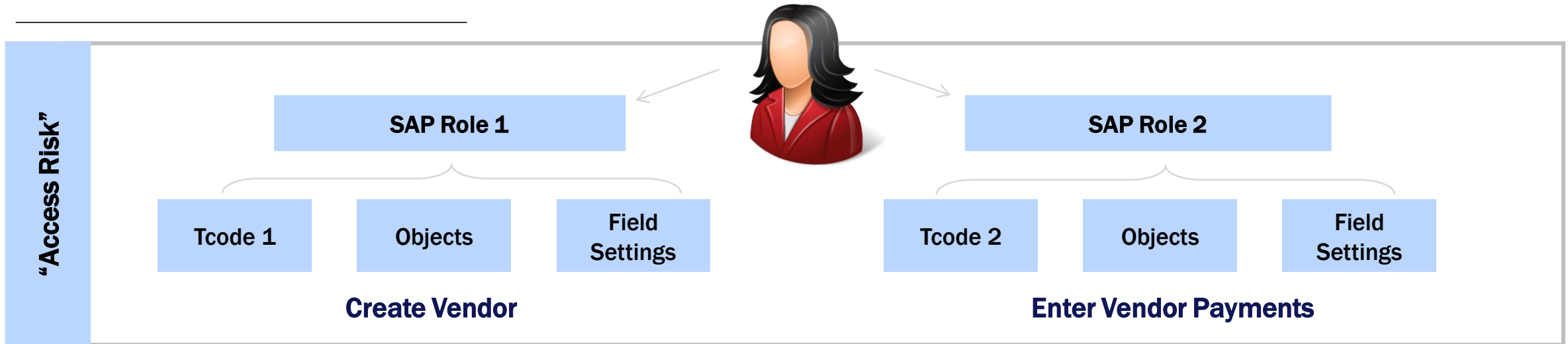
- Prevent and identify “potential” violations
- Occurrences are investigated if issues are identified (audit or fraud)
- Potential risks may be classified as “known” SODs
- No understanding if SODs are processed

Quantify and Mitigate Actual Violations

- Identify who conducted SOD issues (mitigated or unmitigated)
- How many times did they execute these SODs?
- For how much? What is the risk exposure?



What Is an Actual SOD Violation?



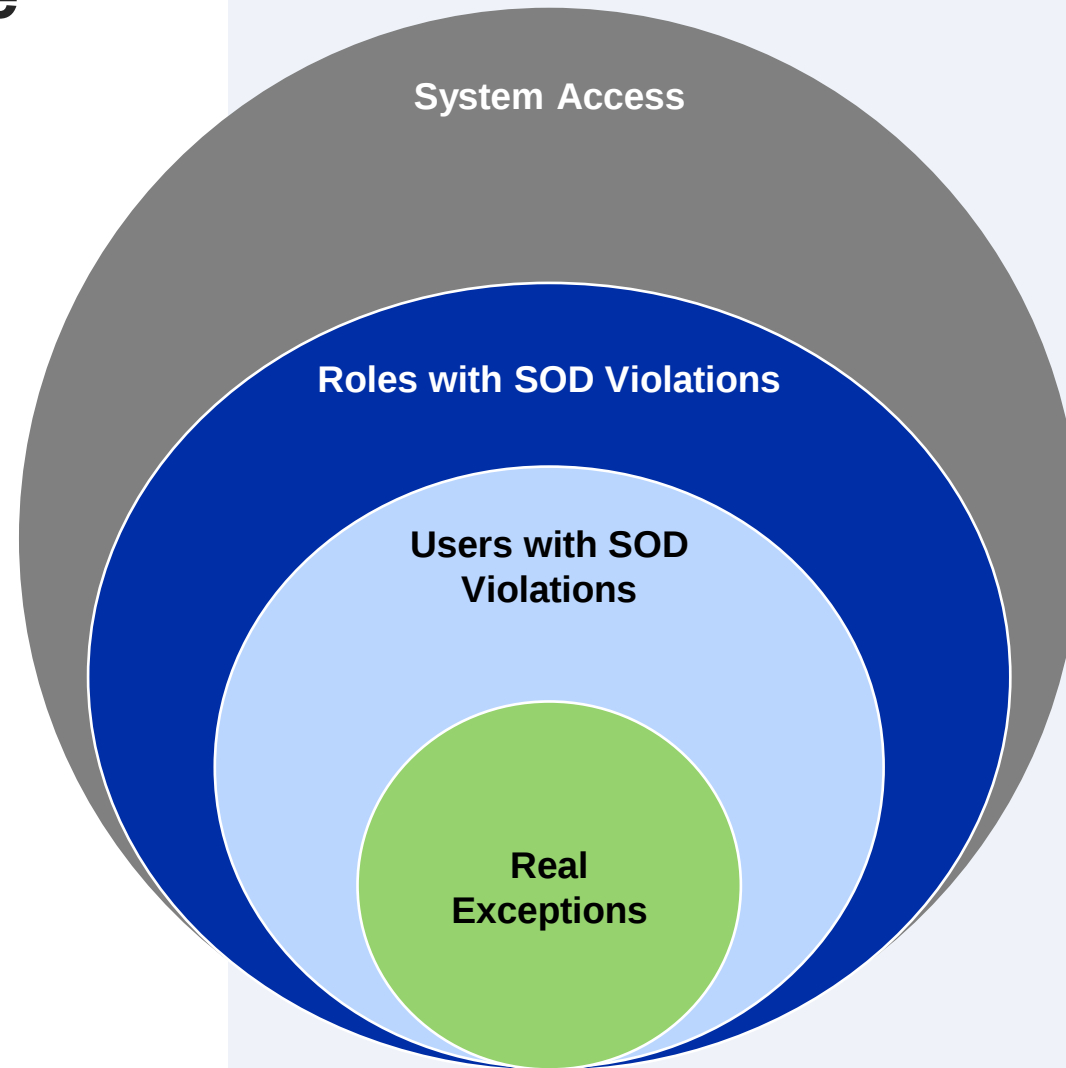
Notes:

- Sequence is important
- Access may not be captured
- Mitigating Controls may not find every violation

Quantifying SOD Risk Exposure

Why focus on the Real Exceptions?

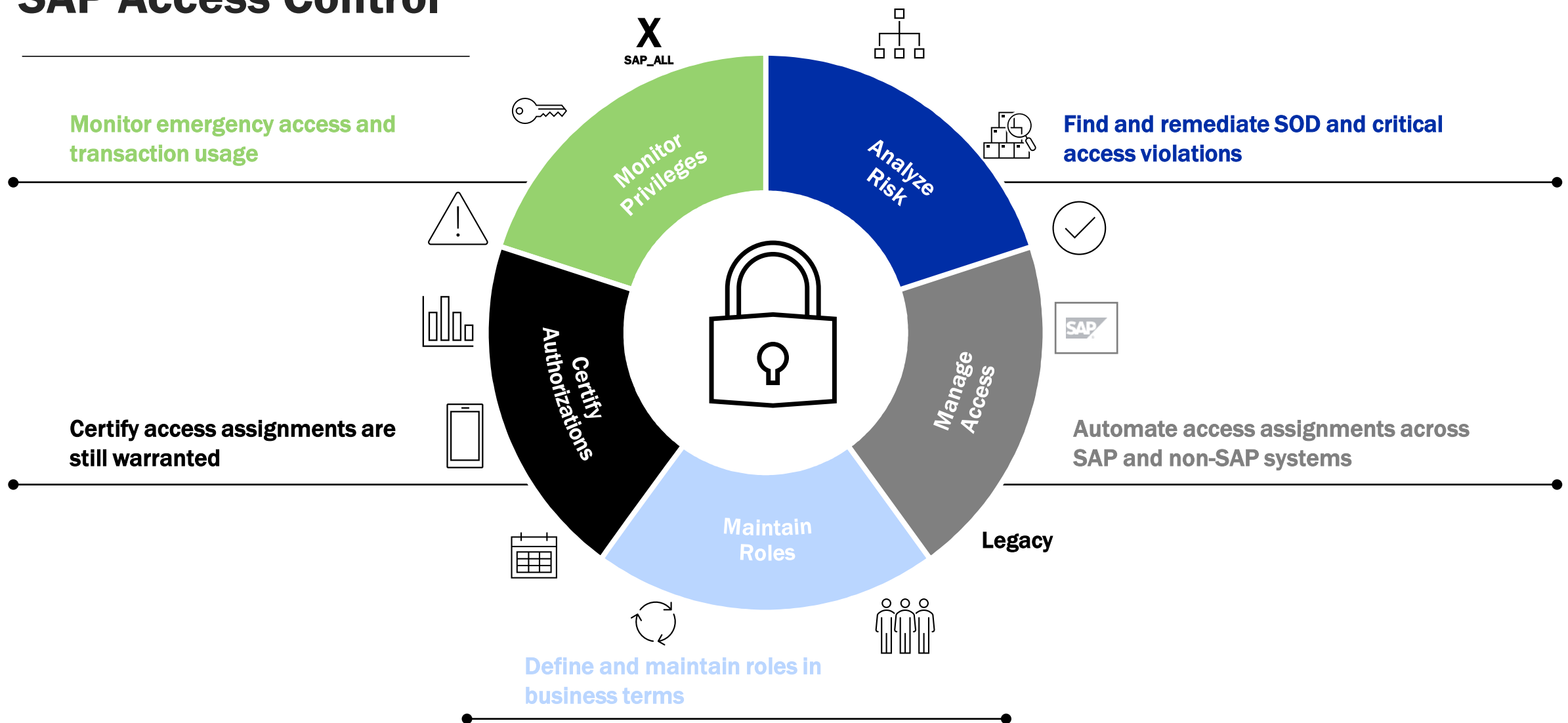
- Identify *actual occurrences* of SOD violations
- Understand *who* did it, *how many* times, and for *how much*
- In the *absence of controls* at the above layers, true comfort can still be obtained



The Right Tool (For Which Job?)

This section will share examples of leading automated solutions in the SAP Access Management space.

SAP Access Control



Extending GRC beyond Access Control

Get Clean

SAP Security Remediation

- Reduce overall number of Users with SOD Risks



- Reduce Unique User Risk



Although roles may be free of conflicts, many SOD access conflicts may still remain due to business requirements

Stay Clean

SAP Access Control

- Certify and monitor access
- Find and remediate SOD
- Automate assignments
- Define and maintain roles



Time and effort to mitigate SOD violations

No visibility to “did-do” and financial impact

SOD Transaction Monitoring

- Identify users that have actually performed conflicting transactions
- Provide visibility and control of risk exposure for remaining SOD violations
- Focus effort on truly high-risk areas
- Drive business transformation
- Implement a continuous monitoring solution like Pathlock AVM



Pathlock Access Violation Management

Without Access Control and AVM:

- Access is managed and reviewed independently by system
- No cross-system access analysis
- Segregation of duties violation goes undetected

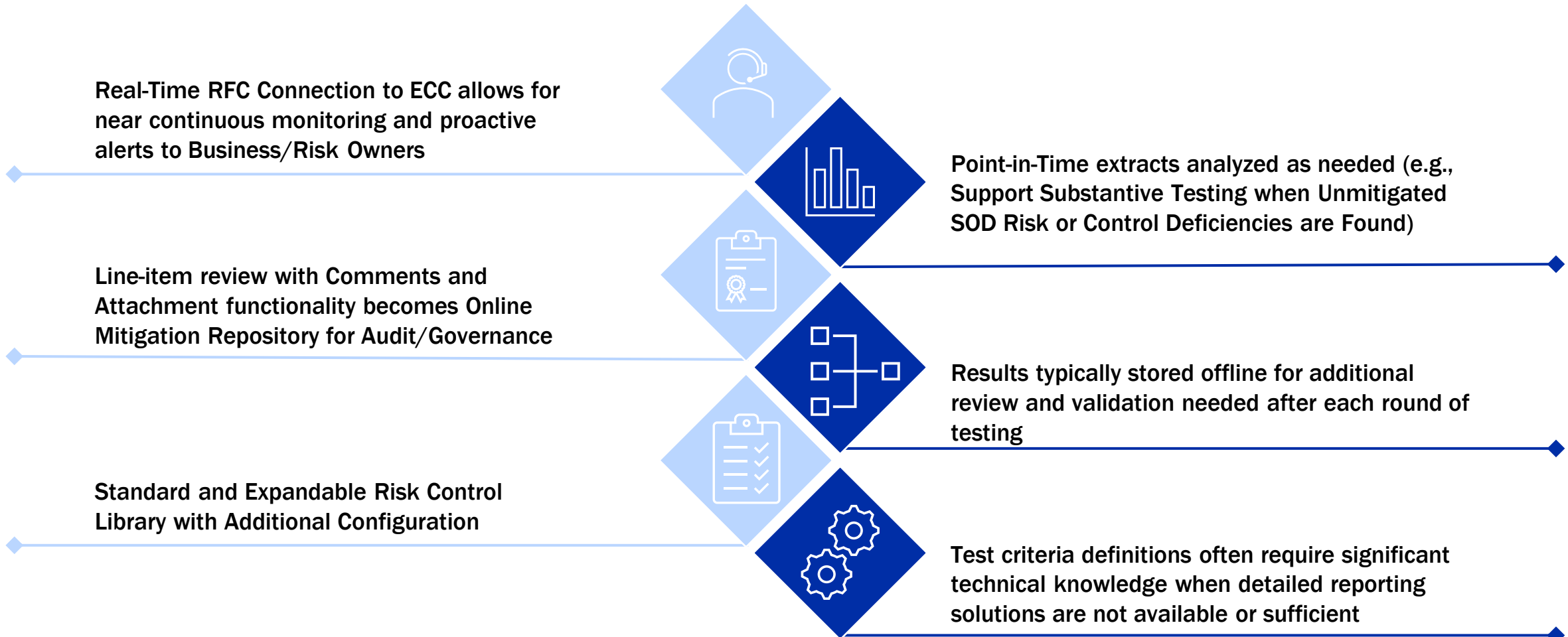
With Access Control and AVM-SI (System Integration):

- Reviewers receive real-time alerts when conflicts arise
- Multiple ERPs can be integrated with cross-system reporting
- Audit trail of approvals

AVM-RA (Risk Analysis) Transaction Monitoring across applications:

- Map hundreds of business functions across thousands of tables and views
- Translate data across all business applications
- Maintain as new versions are released and new applications adopted
- Remove invalid data
- Filter out immaterial exceptions

Solution Comparison (AVM vs Manual)



Too Much Data (And What to Do with IT)

This section will walk through common examples of results from SOD transaction analysis and how to engage the appropriate stakeholders.

Can-Do vs. Did-Do Results

Quantify
Financial
Impact of
Risk

		Potential Risk		100%	Material Segregation of Duties Issue		
Risks		"Can-Do" Access Conflicts		Activity Volume	"Did-do" Transaction Violations		
ID	Description	Users	SODs	Transactions	Users (% of can-do)	Exceptions (% of 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	221	4,581	22,224,544	1 (<0.01%)	8 <0.01%)	\$600
P005	Process purchase orders and payments	23	248	22,138,321	0 (0%)	0 (0%)	\$0

"Can-do" required reviewing 208 users when only 4 (2%) was needed

Smallest "can-do" SoD conflicts, but the largest "did-do" financial impact

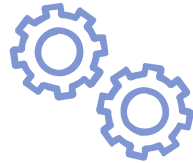
User not found by periodic "can-do" analysis because access changed

Time and effort wasted looking for exceptions that didn't occur

Leverage Results to Drive Action



Identify which risks to test or monitor using quantification analysis



Create a process to manage reported violations (e.g., which violations, who they are reported to, how they are mitigated)



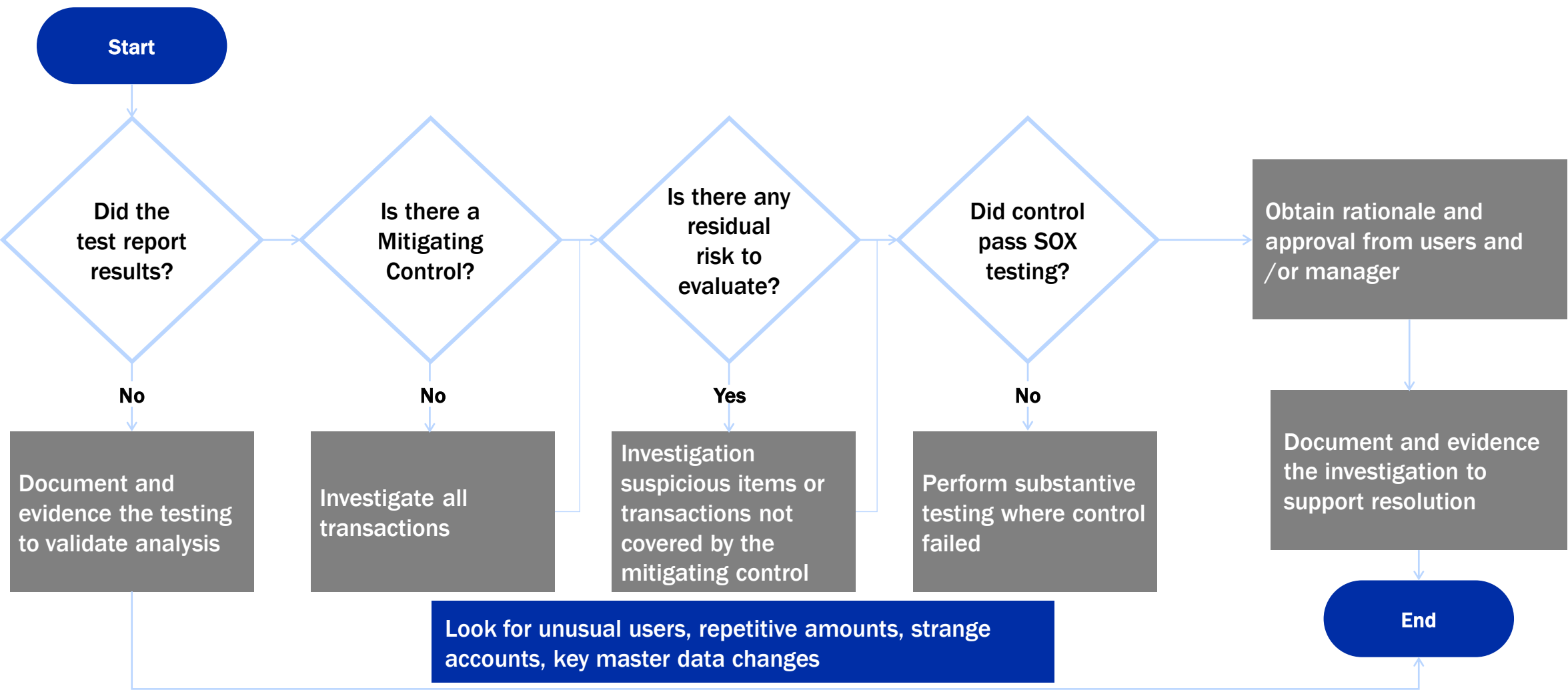
Transfer risk mitigation to the business owners rather than IT managed functions to realize true SOD risk and quantification.

This can lead the business to tighten security so that less violations exist within the landscape



Combine detailed examples with high level reporting to convey true risk exposure across the organization

Example SOD Review Process Flow

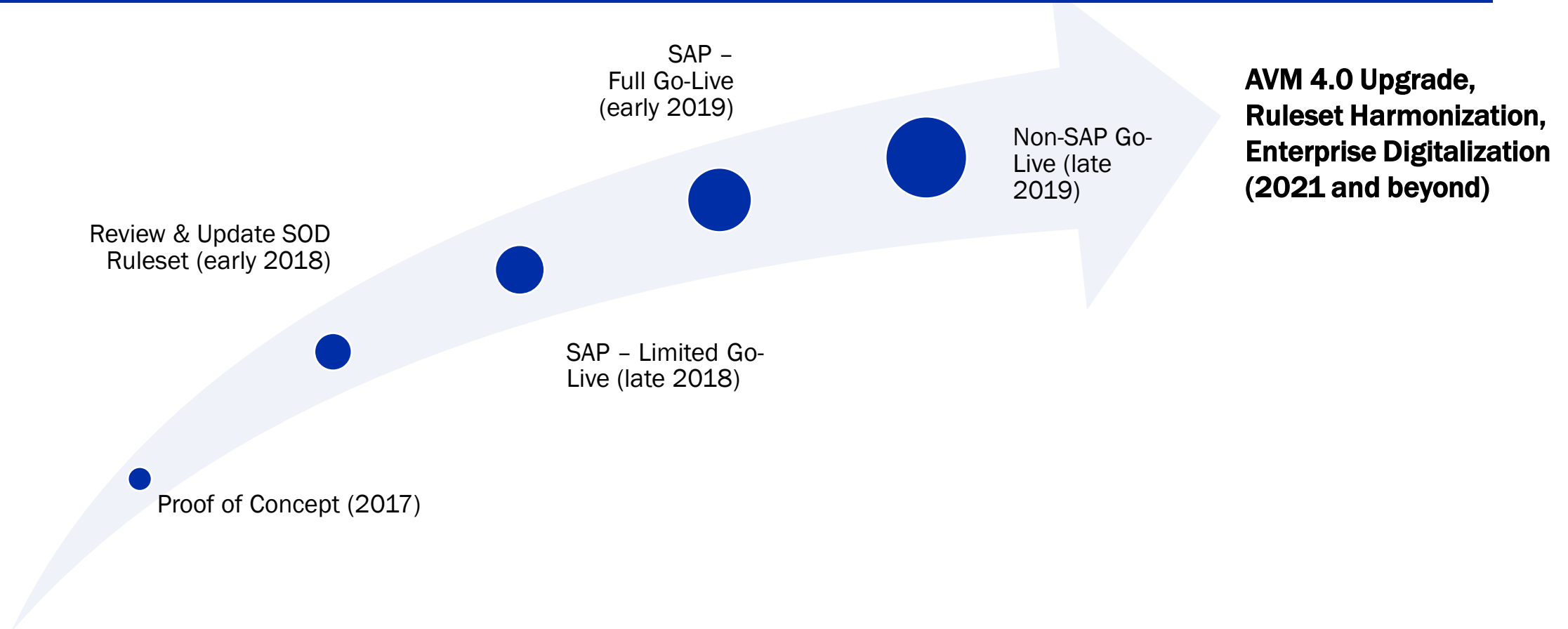


One Company's SOD Journey

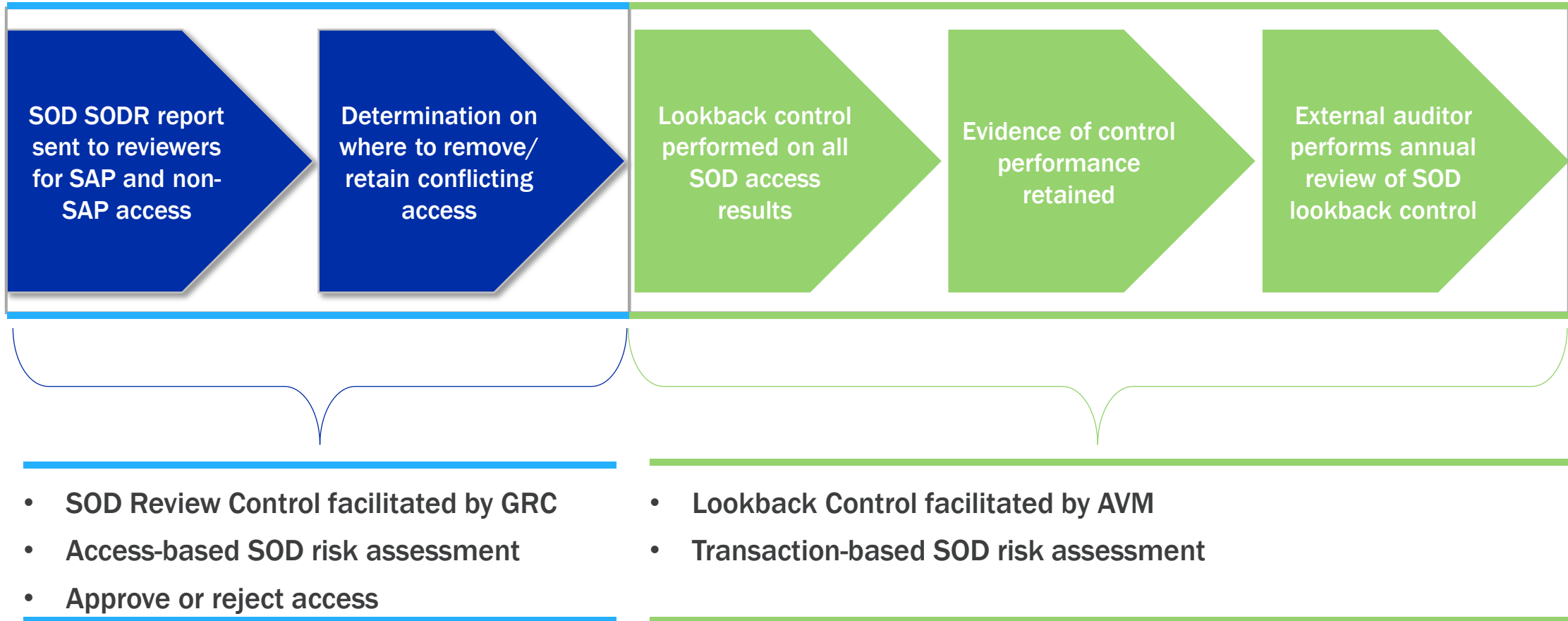
This section will explain how a Global Company moved from the decentralized and manual control processes that managed their Segregation of Duties (SOD) risks to a streamlined compliance model.

The Company's AVM Journey

Our client decided to implement AVM by Pathlock in order to automate their SOD lookback control process. AVM was configured to monitor ~50 SOD risks across 25+ ERPs, including cross-system.



SOD Controls Workflow



SOD Risks Examples

Risk ID	Business Process	Function 1	Function 2	System(s)
FI02	Finance / Accounting	Approve PRA Manual JEs	Create / update PRA manual JEs	SAP ECC
OC10	Order to Cash	Process Sales Order	Maintain Pricing Conditions	SAP ECC
PP02	Procure to Pay	Release Purchase Order	Maintain Vendor Master Data	SAP ECC
JR01	Procure to Pay	Approve Expenditure	Maintain Vendor Master Data	Non-SAP
X001	Procure to Pay	Release Purchase Requisition	Maintain Vendor Master Data	Non-SAP and SAP ECC (cross-system)
JX01	Procure to Pay	Release Purchase Requisition	Maintain Vendor Master Data	Non-SAP (cross-system)

A Leading Practice Backbone

SOD Rule-set Implementation Project Overview

Gap Analysis

- Protiviti took input from multiple sources, including the client's legacy rule-set, External Audit recommendations, and Protiviti's own leading practice rule-set, and developed a new proposed rule-set for S/4
- The proposed rule-set was inclusive of both S/4-based and non-S/4-based risks, therefore making it a holistic cross-system rule-set

Ruleset (Risk Layer)

- Protiviti then held a series of workshops with Global Process Owners and other business leads to determine the applicability of each of the proposed risks for S/4, as well as the associated risk criticality for those that were deemed to be in-scope
- After the rule-set was refined in this manner, final approval for the business risk layer of the rule-set was obtained from the SOD Governance Committee

Ruleset (Tech Layer)

- Protiviti worked with the S/4 functional and security teams to refine the technical layer of the rule-set, accounting for specific t-codes and Fiori apps within the S/4 system design
- Protiviti worked with the security team to incorporate incremental changes to the BPML and further refine the rule-set
- Protiviti worked with External Audit to review their observations on the rule-set technical data

Risk Analysis & Mitigations

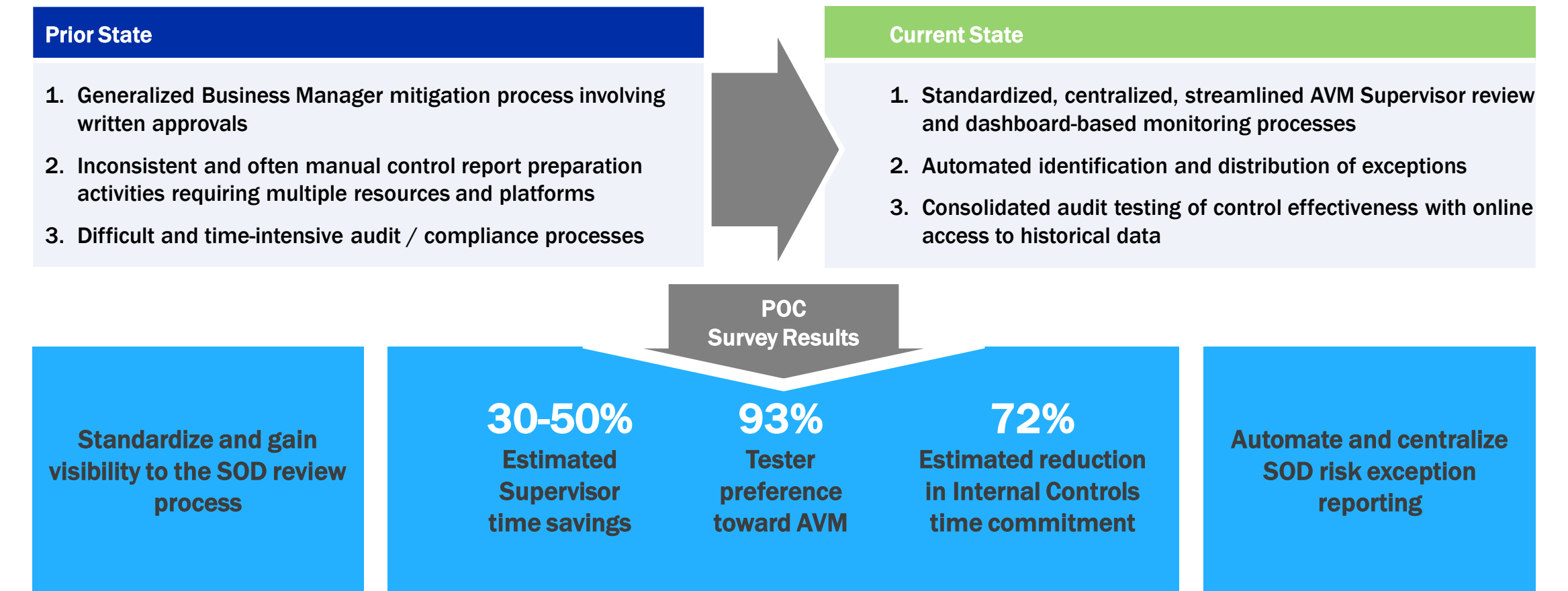
- Risk analysis results were shared with the security team to remediate master and single roles in order to eliminate SODs
- For high-risk conflicts that cannot be remediated, Protiviti will work with the client team to determine appropriate mitigating controls

Cutover & Go-Live Prep

- Protiviti team communicated the cutover plan and strategy with the client's GRC team
- Protiviti team will communicate any risk status changed to the client's SOD Governance Committee
- Protiviti team shared the GRC technical data to the client's GRC team for review and approval
- The S/4 GRC rule-set will be promoted to the GRC production environment upon approval

Benefits of AVM

The revolutionizing benefits related to **SOD Compliance** activities were highlighted and quantified through the results of a Proof of Concept survey of business managers.



Key Points to Take Home

- SOD quantification can give significant and better visibility to SOD issues

- 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

- Point in time assessments are very helpful, but they are only a short-term solution as it can be difficult to manually quantify the impact of SOD access

- Include the Business and IT (and Audit if necessary) when implementing an SOD Quantification process to ensure proper scoping is performed up front and all expectations are met

- An automated process for SOD monitoring can remove management pressure to remove all SODs during a redesign project

Wrap-Up

Monitor your target SAP system for actual SOD violation transactions using AVM.

Develop a process to review reported violations within AVM so that it becomes the repository of SOD mitigation, eventually replacing the need to for ineffective or inefficient manual controls.

Leverage the full reporting capabilities of the AVM solution to help the business avoid material weakness while better controlling SOD.

Where to Find More Information

The Pathlock Blog

<https://pathlock.com/blog/>

- Link to various posts on market trends and success stories from Pathlock's library. Also check out the Case Studies page.

"SOD Empowerment With SAP Access Violation Management By Pathlock" by John Scaramucci, Protiviti TC Blog

<https://tcblog.protiviti.com/2022/03/30/sod-empowerment-with-sap-access-violation-management-by-pathlock/>

- Paper describing how organizations are best prepared and empowered to handle SOD and mitigations effectively when they use automated tools.

"Effectively Managing SAP Security Risks in the Modern World" by Vijan Patel and John Scaramucci, Protiviti TC Blog

<https://tcblog.protiviti.com/2022/03/30/sod-empowerment-with-sap-access-violation-management-by-pathlock/>

- Paper describing how the global landscape has changed in light of COVID-19 and how critical it is for companies to practice good security hygiene.

Key Points to Take Home

- Pathlock AVM combined with SAP Access Control can give significant and better visibility to SOD issues
- 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
- Point in time assessments are very helpful, but they are only a short-term solution, as it can be difficult to manually quantify the impact of SOD access
- Include the Business and IT (and Audit if necessary) when implementing an SOD Quantification process to ensure proper scoping is performed up front and all expectations are met
- An automated process for SOD monitoring can temper management pressure to remove all SODs during a redesign project

Thank You! Any Questions?

Vijan Patel

[Linkedin.com/in/vijanjpatel/](https://www.linkedin.com/in/vijanjpatel/)

John Scaramucci

[Linkedin.com/in/johnscaramuccijr/](https://www.linkedin.com/in/johnscaramuccijr/)

Please remember to complete
your session evaluation.

SAPinsider



SAPinsider.org

PO Box 982Hampstead, NH 03841
Copyright © 2023 Wellesley Information Services.
All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 600,000 members across 205 countries.
