Excelitas' SOD Financial Analytics: Bridging the Gap between Audit Findings and Remediation

BichLoan Dang, IT Technical Lead, Excelitas Technologies

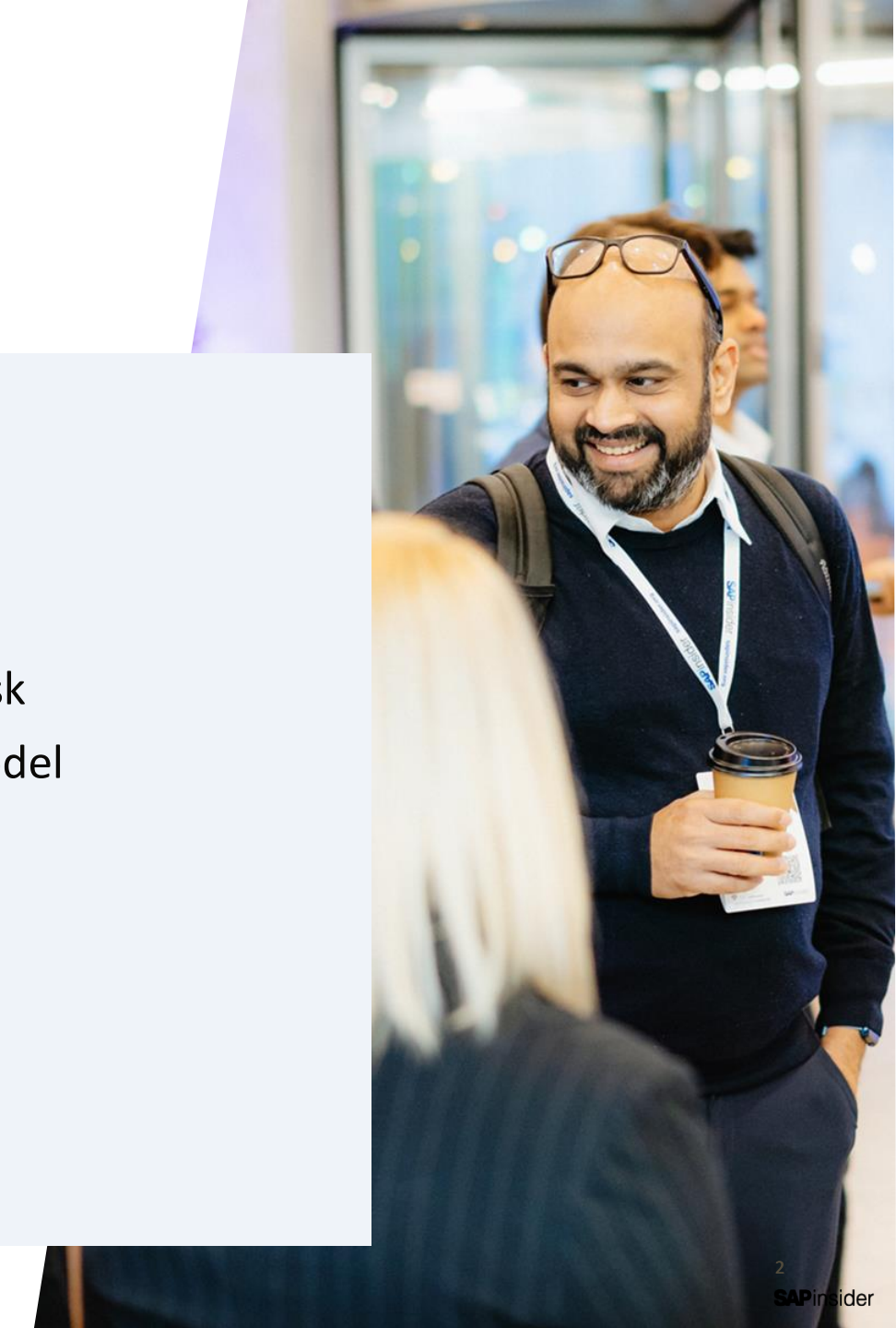
Las Vegas

2024

SAPinsider

What We'll Cover

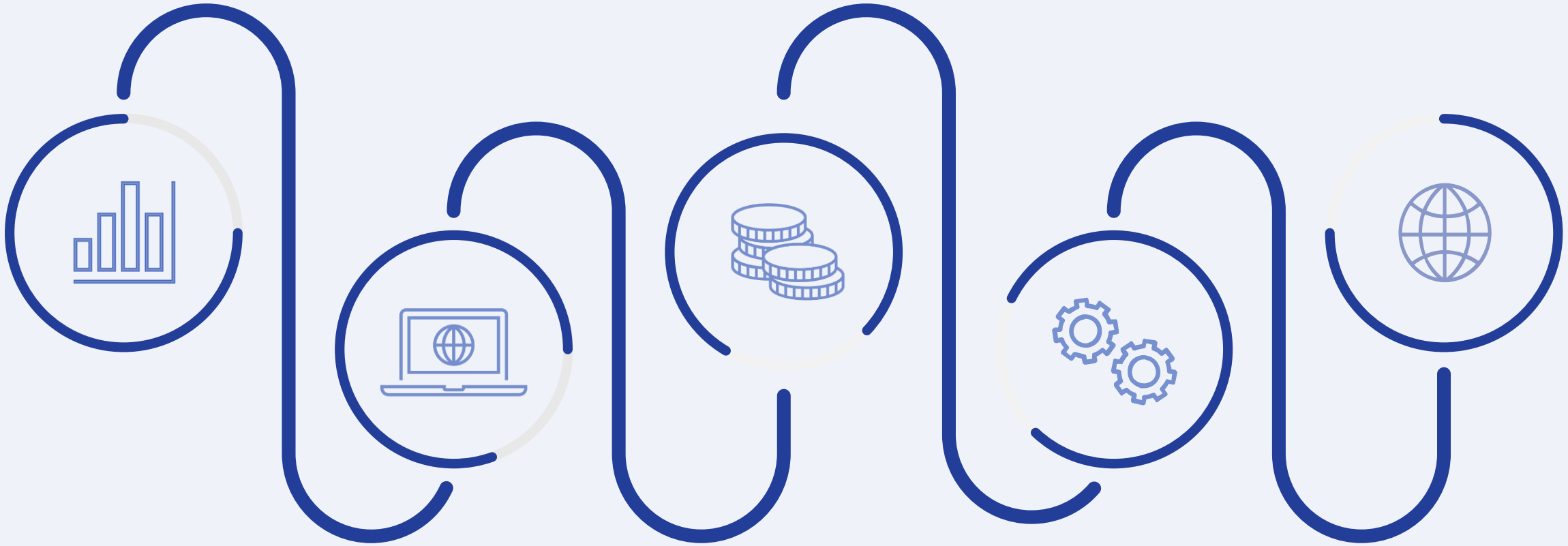
- Our Company and SOD Journey
- Assessing the Risk Universe
- Strategizing Remediation Efforts
- Quantifying Financial Impact of Access Risk
- Implementing a Best Practice Security Model
- Transforming the Organization
- Wrap-Up



Company Overview

Excelitas Technologies is a technology leader in delivering high-performance, market-driven photonic innovations to meet the illumination, optical, optronic, sensing, detection and imaging needs of customers worldwide. Serving a vast array of applications across automotive, consumer products, defense and aerospace, industrial, medical, safety and security, and sciences sectors, Excelitas Technologies stands committed to promoting our customers' success.

Our SOD Journey



Project Background

Challenges

Lack of change management controls with respect to user access security

Overprovisioning of access to users with minimal preventive checks in place

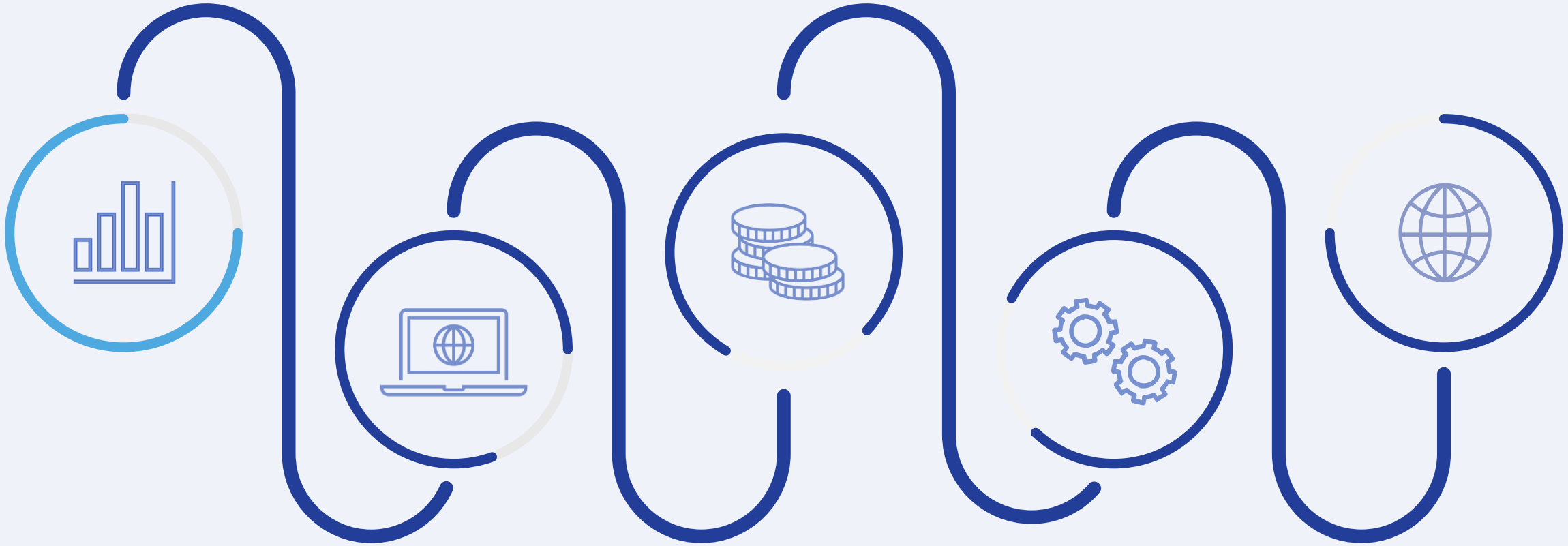
Control deficiencies noted aggregating to Significant Deficiencies in Program Change and Access to Programs & Data

Key Considerations

At the time, using SAP S/4 Central Finance for central processing and direct entries – more than just a dashboard

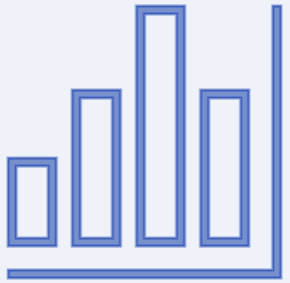
Key financial systems were SAP ECC, Microsoft Dynamics AX2009, and Salesforce, but majority of issues were found in SAP systems

Our SOD Journey



Phase 1 Assessment Project Overview

- Kicked off in July 2022
- Assessed current state security across critical financial systems using automated tools
- Analyzed for role-level and user-level Segregation of Duties (SOD) conflicts and Sensitive Access (SA)
- Reviewed results with key stakeholders to develop remediation plans
- Leveraged an agile approach to address areas of greater risk with prioritization
- Created a timeline of quick wins and remediation strategy

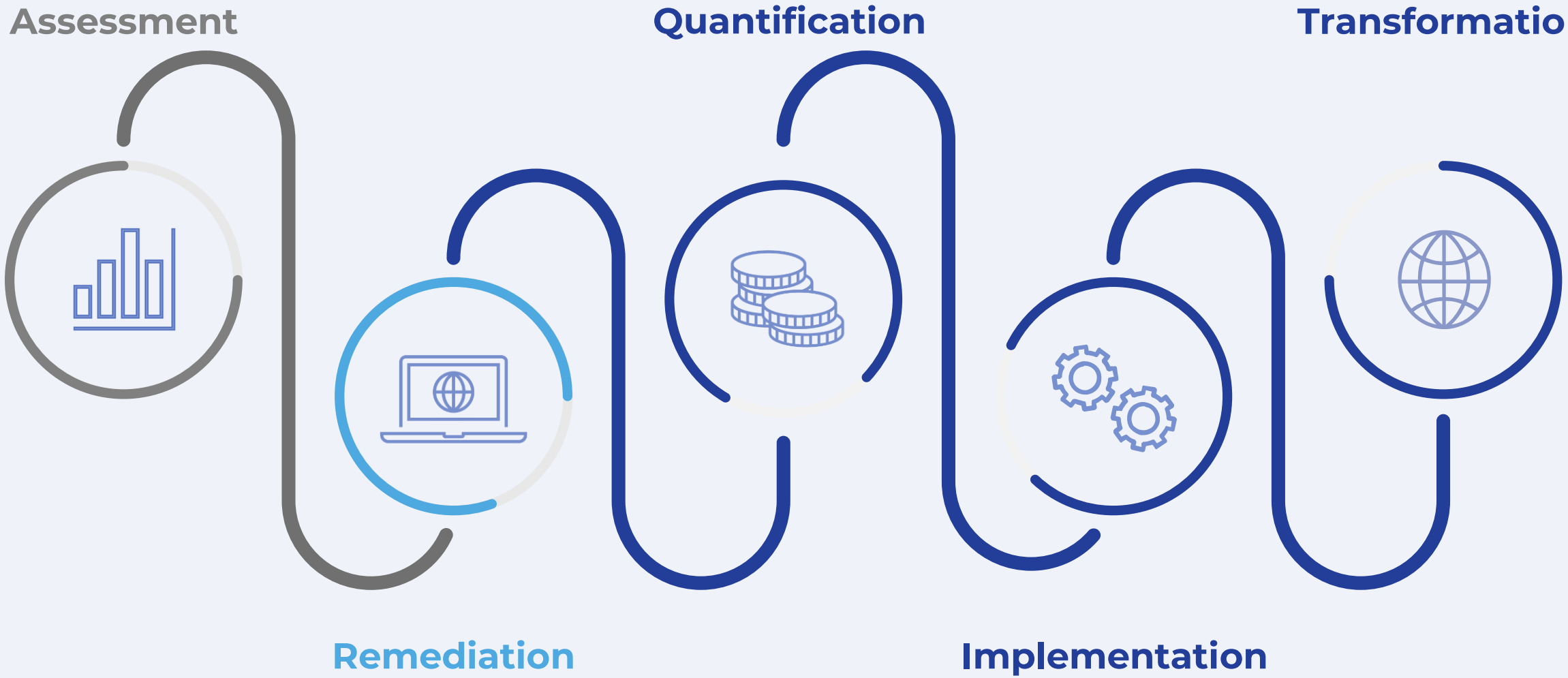


Remediation Approach Options

Based on assessment findings, the following options were considered for SAP Security remediation efforts:

Options	Details	Summarized Approach	Pros (+)	Cons (-)
 **Targeted Remediation**	Remediate roles and/or users with the highest priority risks	• Achieve identified Quick Wins • Remove IT sensitive access from day-to-day roles • Establish an approach for Elevated Access Management • Remediate inherent high SOD conflicts from roles where possible	• Quicker turnaround • Lower cost initially • Lower amount of disruption to the business	• Difficult with large number of roles with excessive access • Limited reduction in SOD violations and risk • Role architecture may not be consistent
 **Role Redesign**	Net new security roles are designed and built for all users based on business requirements	• Develop initial role design based on tcode usage and stakeholder input • Build roles and perform functional unit testing and SOD analysis • Conduct user acceptance testing • Finalize user mapping, transport finalized roles, and hypercare	• Role architecture is consistent and scalable • Easier to maintain • No inherent SOD risks within technical roles • Architecture can be shared across instances	• High level of business involvement and coordination • Costlier than remediation to achieve fuller coverage

Our SOD Journey



Strategic Remediation Roadmap

Short Term

Quick Wins

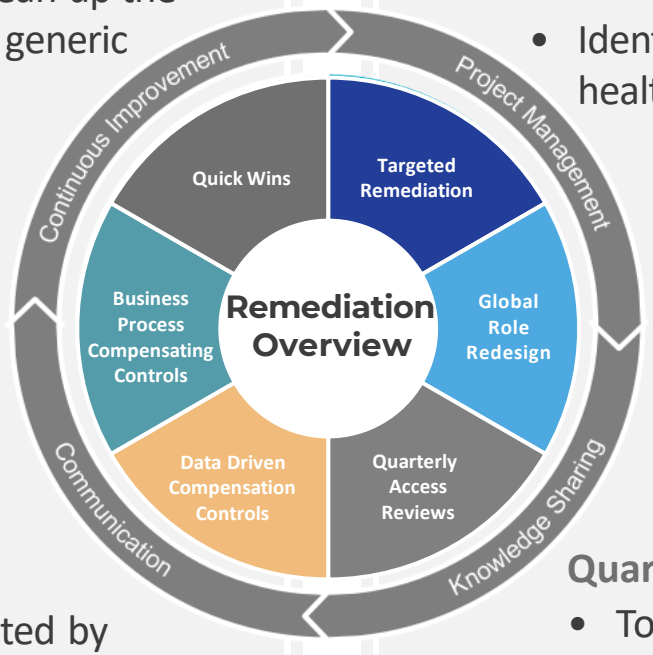
- Focus on impactful areas that will begin to clean up the overall security of each system (e.g., remove generic accounts, powerful roles, inactive users)

Business Process Compensating Controls

- Technical remediation or redesign will only resolve 70% of user SOD
- Begin identifying controls (automated or manual) that will mitigate access

Substantive Testing or Data Driven Compensation Controls

- Substantive testing of user SOD will be expected by external audit with remediation efforts ongoing
- Use of automated SOD quantification tools will lower effort and cost of testing



Long Term

Targeted Remediation (Non-SAP Systems)

- Identify and address targeted high-risk issues
- Identify key risk areas that will improve the overall health of the system's security

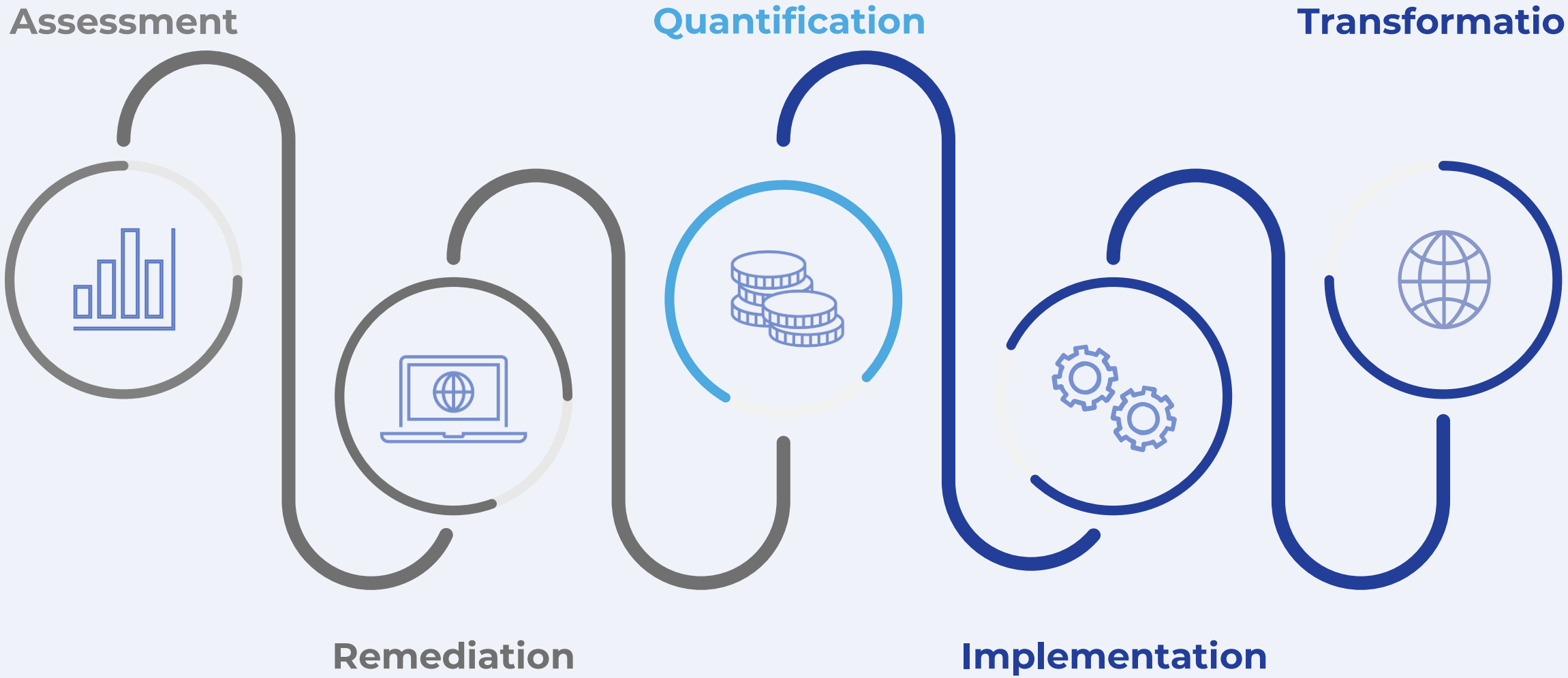
New Global SAP Role Design

- New security roles for S/4 users based on business requirements & compliance
- Significantly reduce access risk
- Clarify SOD and access review processes
- Improve efficiency and scalability of SAP security administration & maintenance

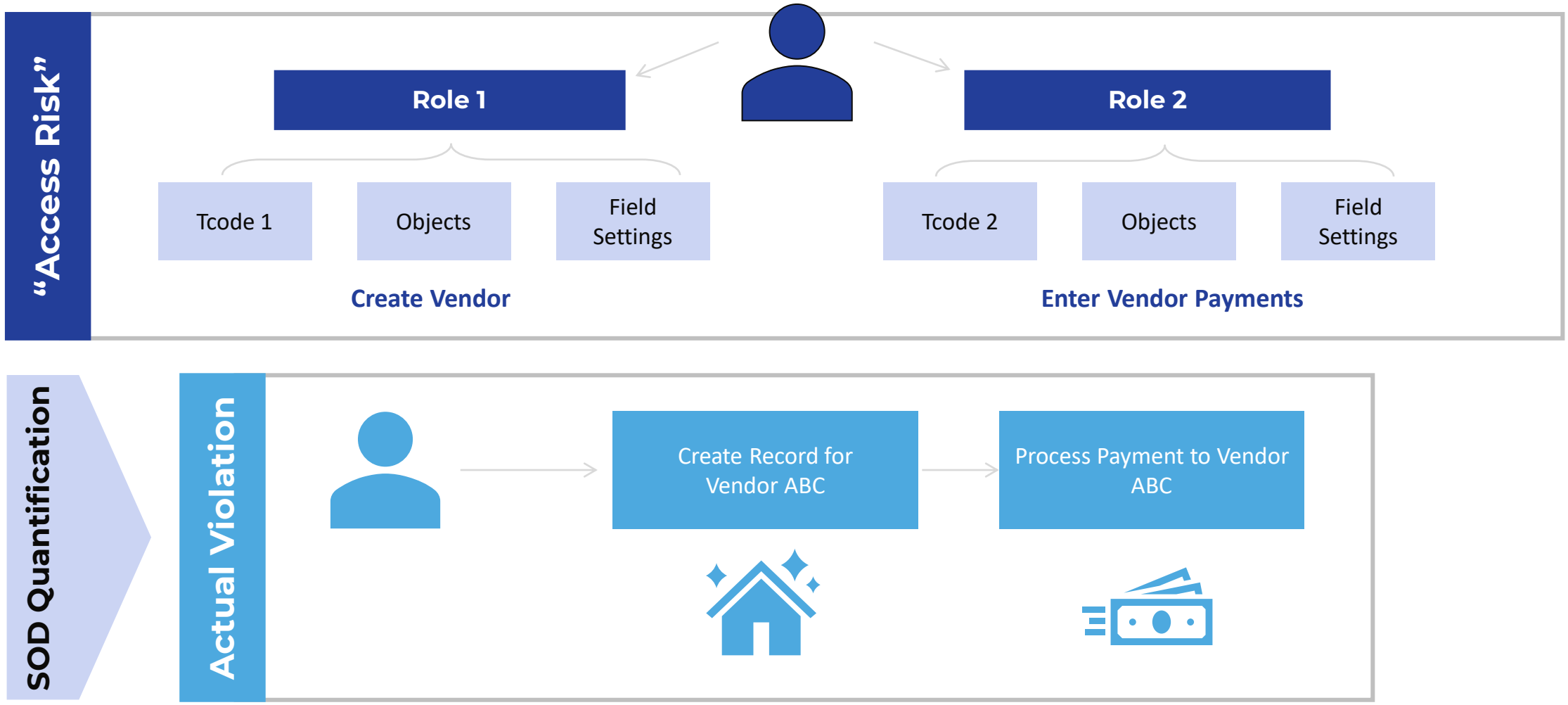
Quarterly SOD Access Reviews

- To be SOX compliant, external audit will require quarterly access reviews of financial systems
- Implementation of GRC tool(s) will enable periodic SOD reviews and other governance

Our SOD Journey



SOD Risk Example



Isolate Actual Risk Exposure

"Can-Do" Access Risk

100s of users across many different countries had access to conflicting functions.

Tested 100% of the Population

"Did-Do" Occurrences

###

transactions

$$$

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

Quantified Financial Impact

SOD Quantification Project Overview

User access to numerous Segregation of Duties (SOD) Risks was identified as part of the Phase 1 assessment.

Management action plan was to remediate security for end users and have a user access management process in place in 2023, however due to timeline restrictions and external audit concern substantive testing related to SOD had to be performed.

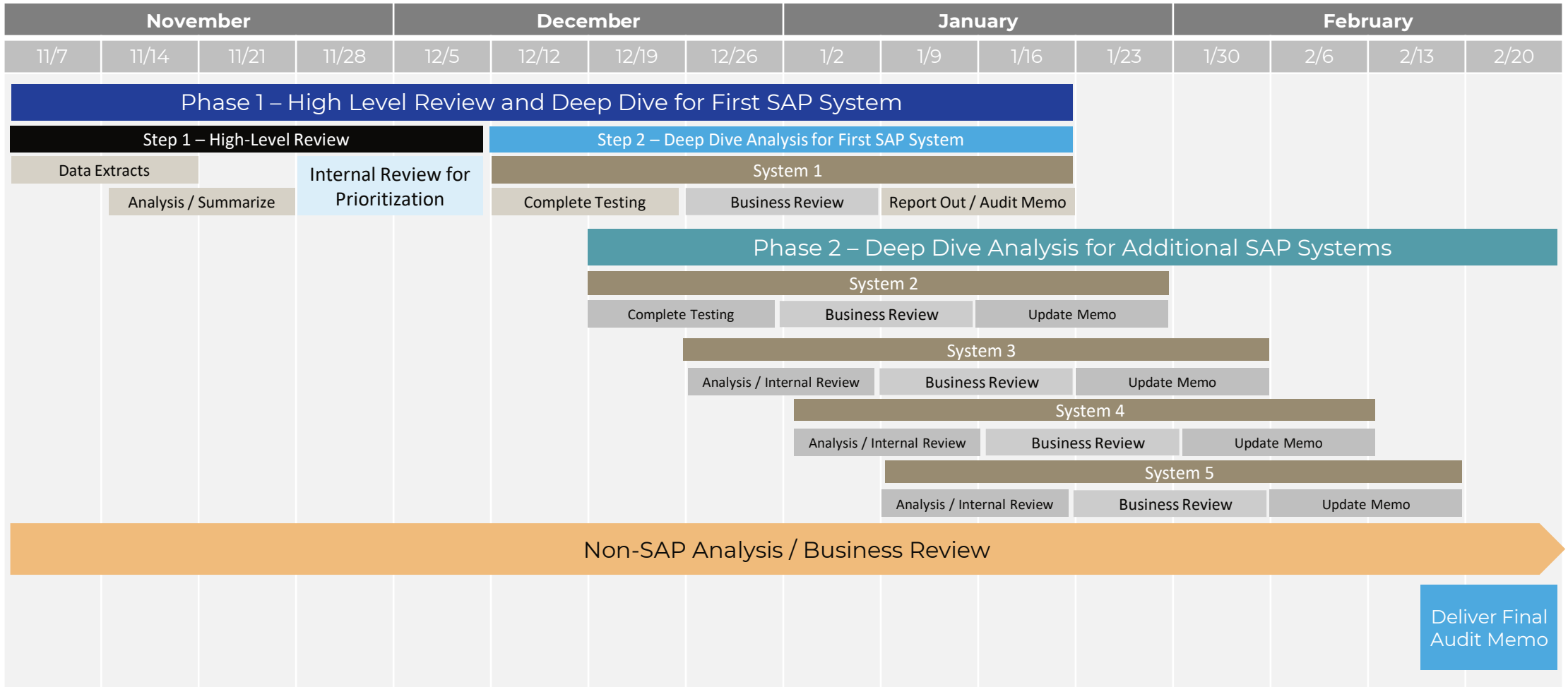
Outcomes:

- Identified Actual SOD Violations to Key SOD Risks ("Did-Do Analysis")
- Filtered results based on user activity and materiality
- Reviewed individual transactional line items with local management
- Provided a memo with findings to external audit

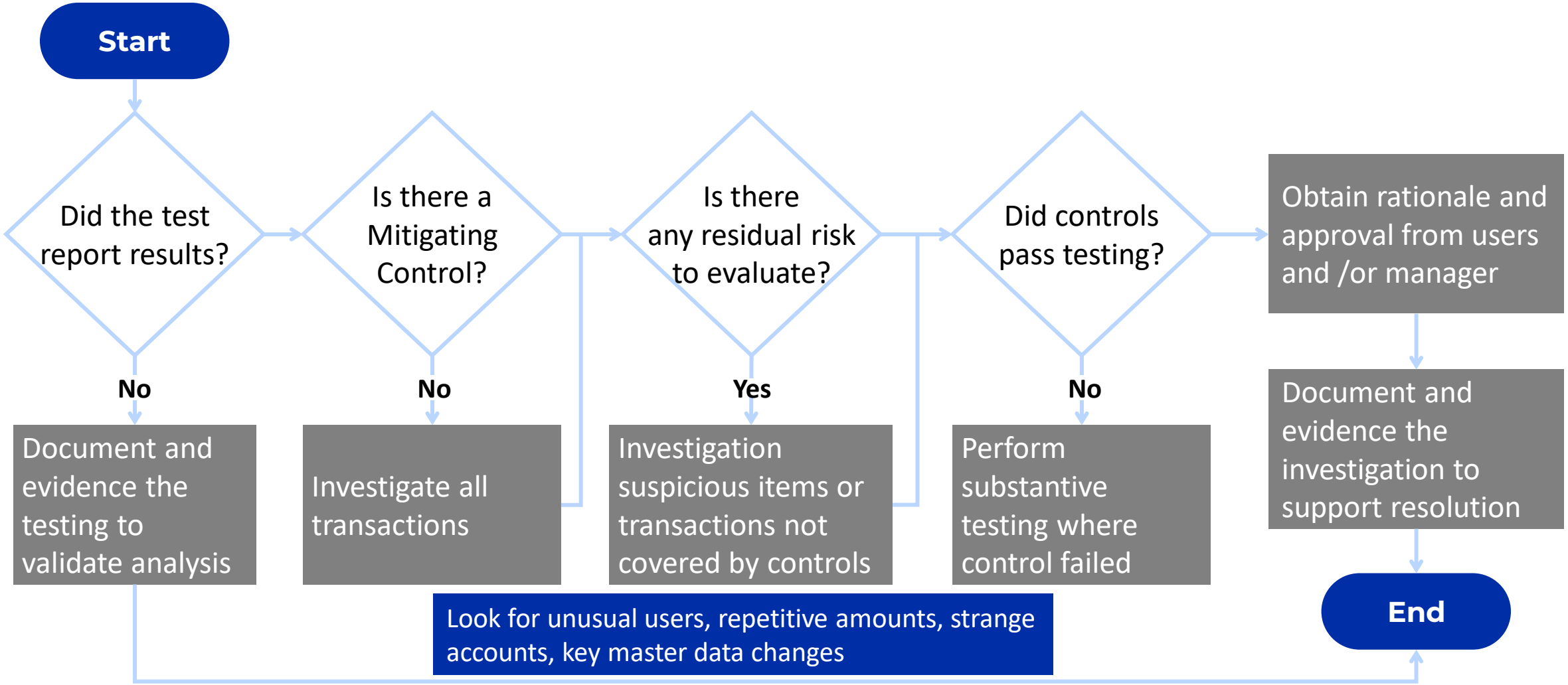
Scope:

- Only High SOD Risks
  - SAP Automated Analysis: 33 SOD Risks
  - SAP Manual Testing: 28 SOD Risks
- 5 SAP Production Instances (1 CFIN and 4 ECC)
- FY2022 Tested Once (Year End was not included)
- Ad-hoc Analysis for Non-SAP Systems

Approach and Timeline



Example SOD Review Process



Our SOD Journey

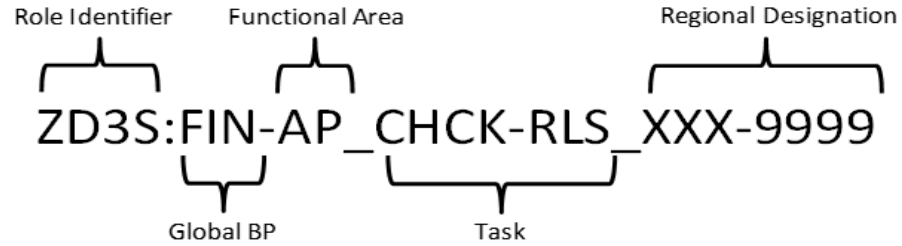
Leading Practice SAP Security Design Principles

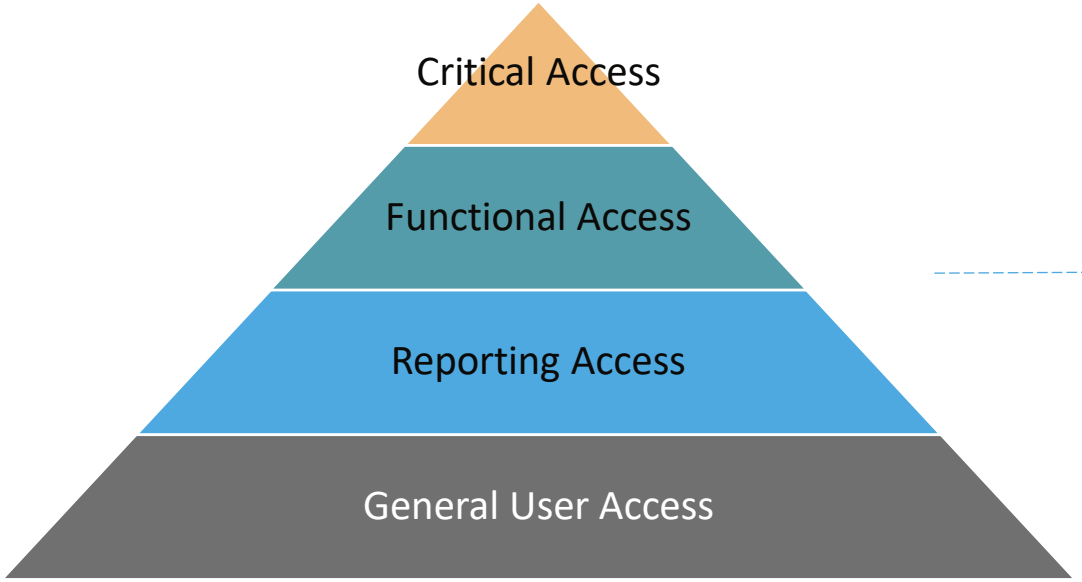
1. Segregation of Duties (SoD) Conflict Free Design (Task Role Level)
2. Least Privilege Access when designing and provisioning access
3. Consistent Role Naming Convention
4. Minimize duplication of transaction codes
5. Tiered Role Architecture
6. Separate access in roles between Display vs. Update transactions
7. Separate access for emergency/critical activities (Firefighter) and non-dialog users

Implementation Security Design Assessment

Standardized Naming Convention

- Evaluated requirements and developed security role naming convention aligned to the business based on Leading Practices



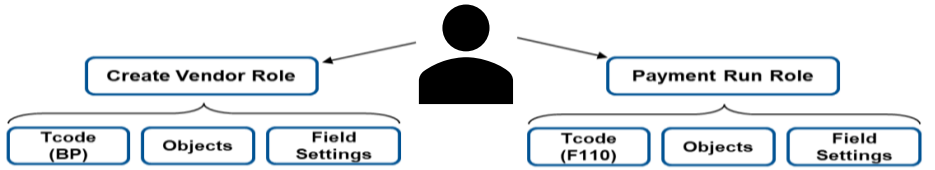


Tiered Access Architecture

- Developed Role Design Principles using leading practice with Fiori App and GUI transactions
- Evaluated requirements and developed security architecture and role naming convention aligned to the business

Segregation of Duties

- Reviewed Leading Practice SOD Ruleset with key stakeholders
- Executed Role-level SOD analysis post-build and remediated inherent conflicts



Task-Based Role Methodology

A task-based role design includes building each role to perform a single function/task (Ex: Creating a role for Vendor Master Maintenance, one for Sales Order Creation, etc.). All transactions related to a task are grouped together.

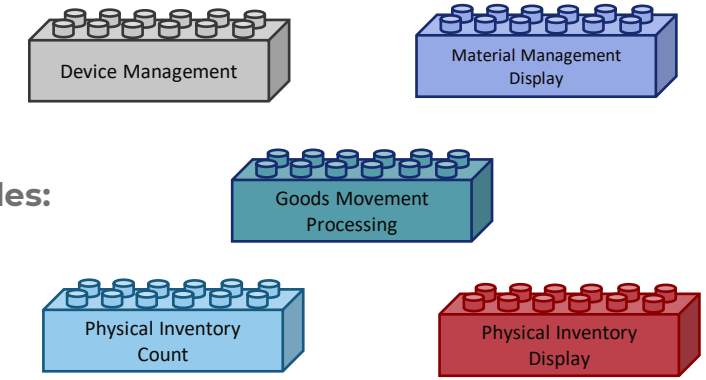
Task Roles

- Grouping of functionality (e.g., tcodes, Fiori apps) to accomplish a single task
- Highly granular roles
- Specific to one application (e.g., S/4, MDG, BW)

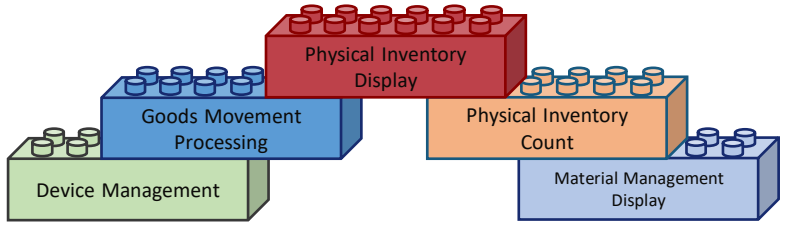
Business Roles

- Groupings of technical roles to provide all required access for a given user's job responsibilities
- Large, business driven roles
- Can include technical roles from multiple applications

Examples:



Ex: Warehouse Manager Role



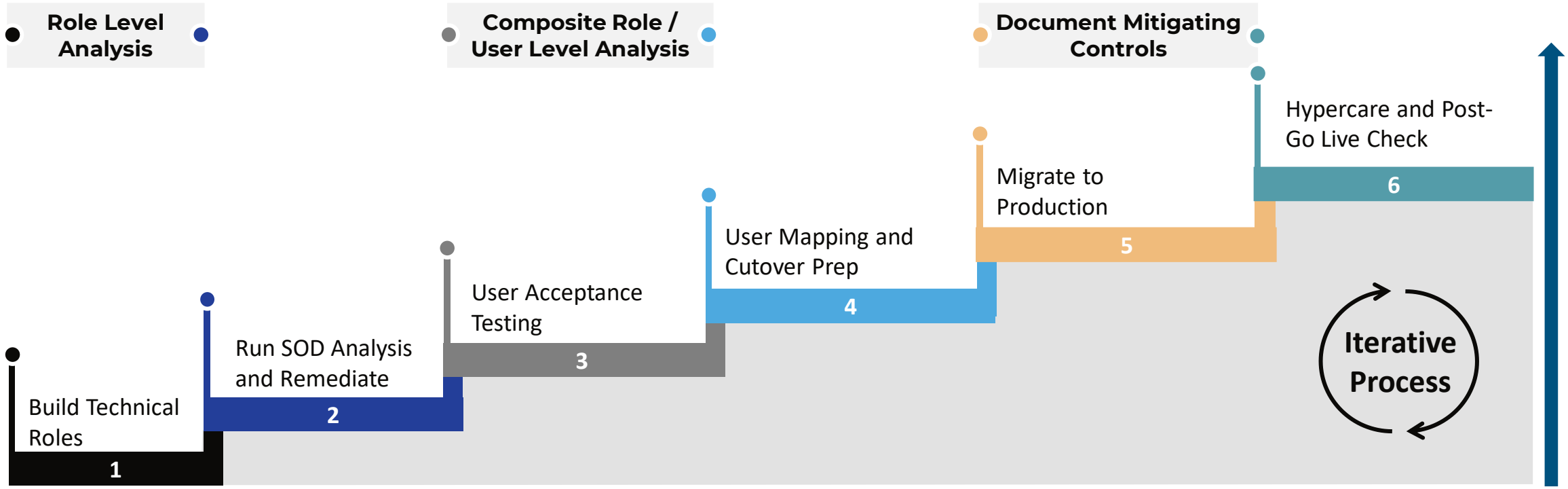
Advantages of Task-Based Methodology:

✓ Minimizes transaction duplication in roles to only transactions that perform cross-functional tasks (FB01 for AR, AP, GL Posting)

✓ Allows for flexibility in user access assignment such that users can be assigned only the specific tasks they require to perform their jobs

Pre-Implementation SOD Review Process

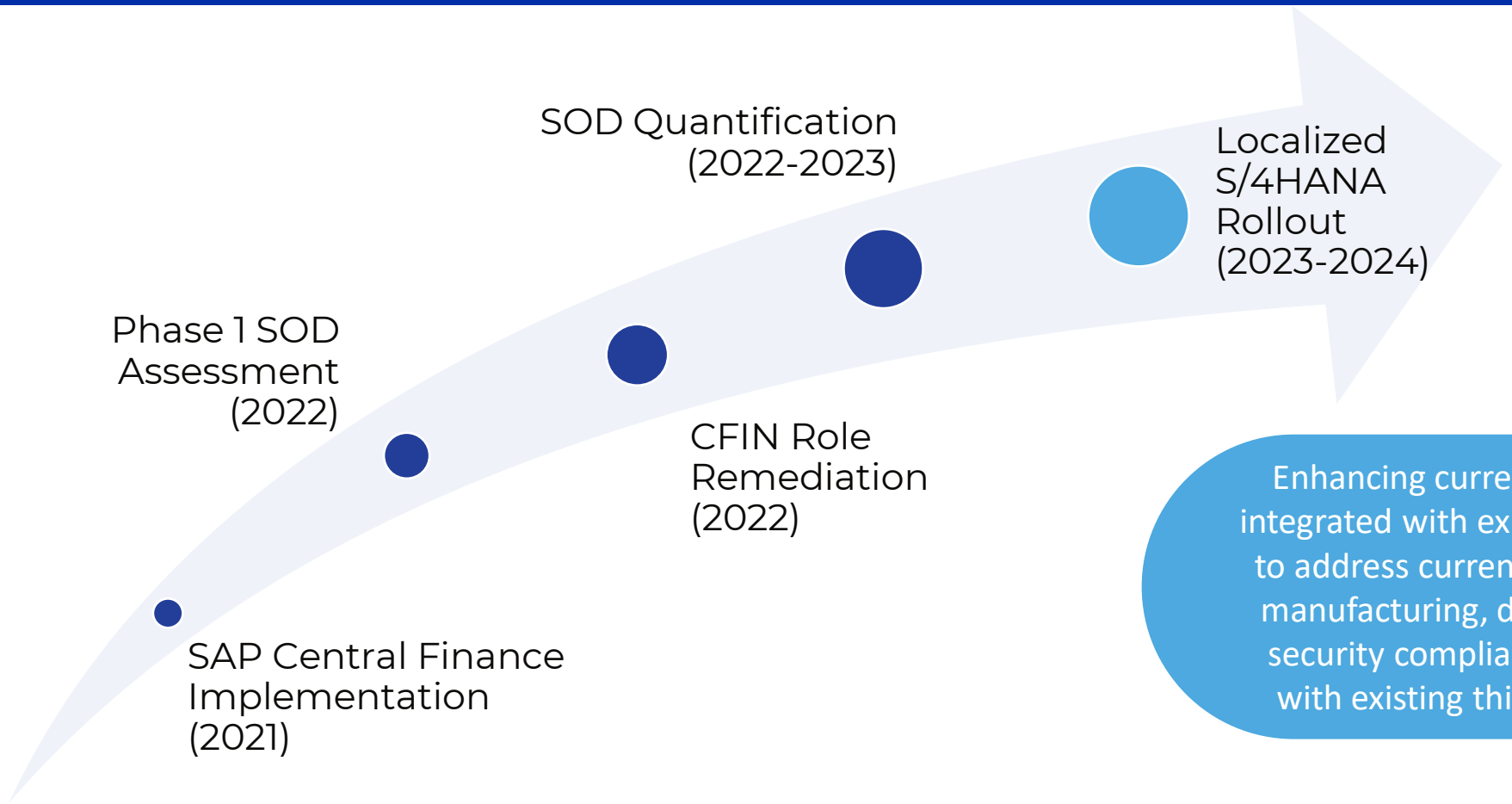
The following steps provide a brief overview of the approach when building security. The security support team provides timely assessments to system implementors to make sure that the roles are risk free, and that the user assignment minimizes risk as much as possible.



Our SOD Journey

S/4HANA Roadmap

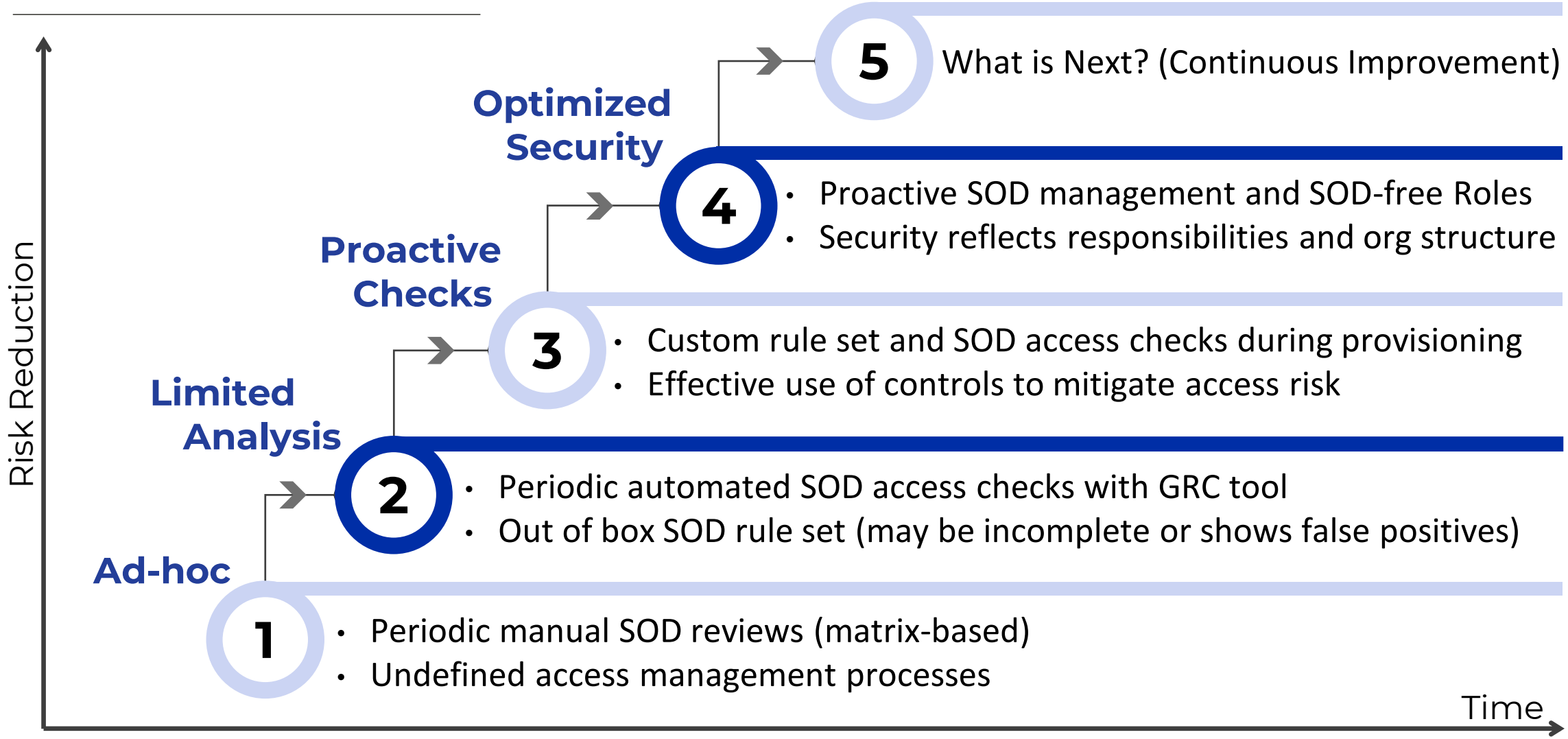
Excelitas has embarked on IT Technology Transformation initiative for simplified & uniform business process execution with enhanced user experience and single source of truth



“Project Evolution”

Enhancing current S/4HANA Instance integrated with existing CFIN for local site to address current and future needs for manufacturing, distribution, financials, security compliances and integrations with existing third-party applications

Access Management Maturity



Wrap Up

- Where to Find More Information
- Key Points to Take Home
- Q&A

Where to Find More Information

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)
- https://sapblog.protiviti.com/2024/01/24/system-integrator-or-security-specialist-who-should-be-responsible-for-implementing-s-4hana-security-and-controls/

Designing SAP Application Security

- Protiviti Whitepaper on Leveraging SAP Access Monitoring Solutions During SAP Implementations, Upgrades, or Security Redesign Projects (September 2022)
- https://www.protiviti.com/sites/default/files/2022-09/designing-sap-application-security-protiviti.pdf

Managing Risks Along Your SAP S/4HANA Journey

- Protiviti POV on How Internal Audit and Compliance Functions Can Support S/4HANA Projects (September 2022)
- https://www.protiviti.com/sites/default/files/2022-09/pov-internal-audit-role-sap-hana-protiviti.pdf

Subscribe for Additional SAP Insights

- https://learnmore.protiviti.com/SAPInsightssubscription

Key Points to Take Home

- **Quantify the Risk:** SOD quantification can give enhanced visibility to SOD issues
- **Apples and Oranges:** Understand the difference between ‘potential’ SOD conflicts and ‘real’ financial impact
- **Prioritize Intelligently:** Removing excessive access, such as unused transactions, can be a quick win in reducing SOD access
- **Plan Strategically:** Develop a roadmap to remediation of SAP access deficiencies while performing mitigating activities to buy yourself time.
- **Take Action:** Monitoring of known risks can start immediately to reduce risk and prove compliance
- **Build Governance:** Specialized knowledge is required to understand details of SAP security, business processes, SAP table structures, compliance risk and organizational hierarchy
- **Secure Sponsorship:** Representation from executive leadership to ensure the right messaging is heard and communicated to the broader organization

Thank you! Any Questions?

BichLoan Dang

linkedin.com/in/bichloan-dang-3872674/

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.