

# How a Major Retail Chain Successfully Managed Multiple Integrators to Embed Compliance Objectives into Their S/4HANA Implementation

**Liz Zuber**

Associate Director - SAP Solutions, Protiviti

SAPinsider  
Las Vegas

---

**2023**

**SAP**insider



## In This Session

---

In this session we will share how our Retail customer kept ***compliance*** at the forefront of their S/4 transformation journey by identifying, documenting, and providing guidance regarding GRC, Security and Controls throughout their implementation.

We will also discuss how our customer integrated ***multiple 3<sup>rd</sup> party providers*** to achieve a successful SAP S/4HANA implementation.



# What We'll Cover

---



**Implementation Program Overview**



**Compliance Workstream Overview**



**Collaboration with Other Partners**



**Wrap-Up**



# Program Overview

---

**Review specifics around the implementation program detailing key principles, scope and timelines.**

**Introduce the various 3<sup>rd</sup> parties involved in the program and how the core responsibilities were split.**

# Program Overview

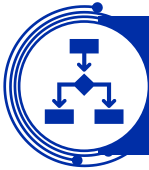
---

- **Greenfield SAP S/4HANA Implementation**
- **Key Guiding Principles**
  - **Compliance**
  - **Automation**
  - **User Experience**
  - **Standardize Processes**
  - **Scalable**
  - **Document Key Decisions**



# Scope

A core objective of this program was to simplify the technology portfolio. S/4HANA was chosen to replace multiple local applications.



## Processes

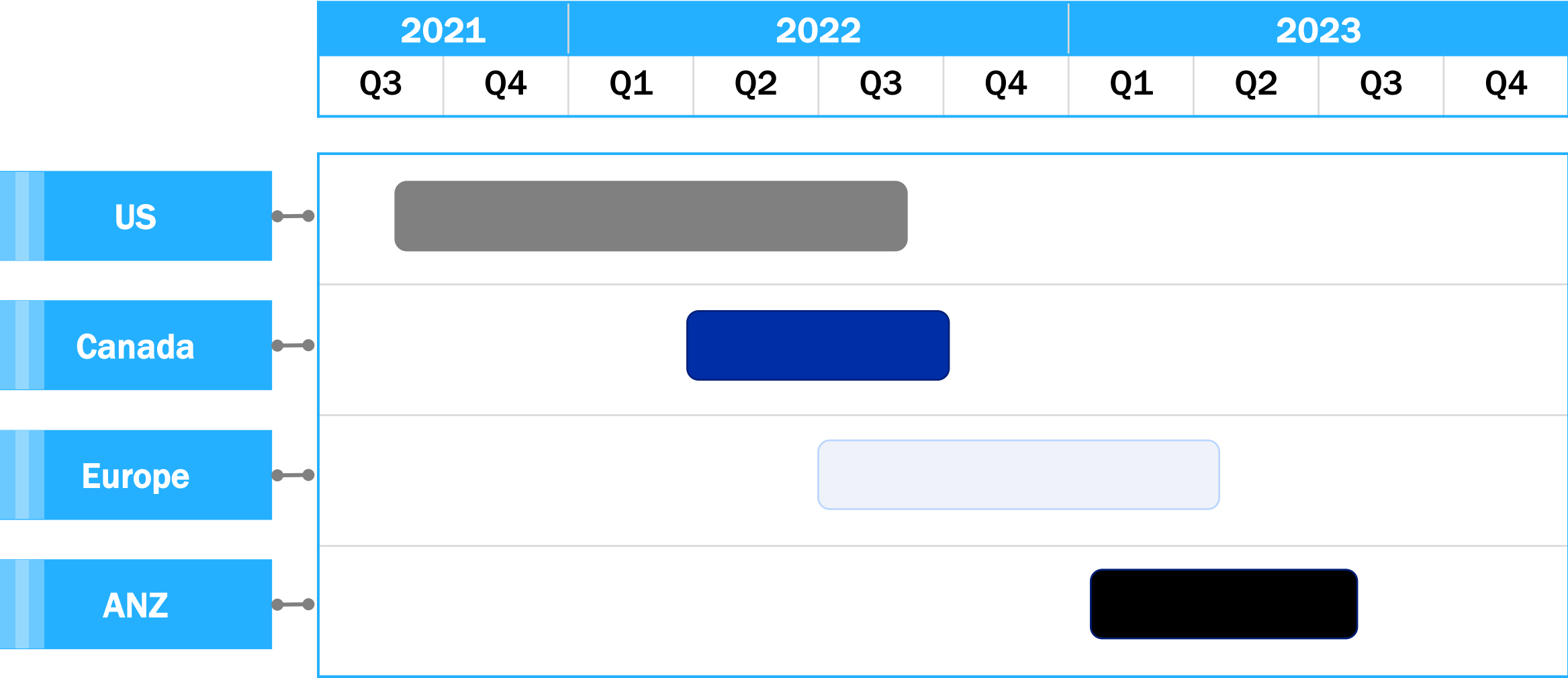
- Finance & Accounting
- Retail Management
- Inventory Management
- Direct Procurement
- Supply Chain
- Manufacturing
- Global Trade Management
- Governance, Risk & Controls
- HR



## Technologies

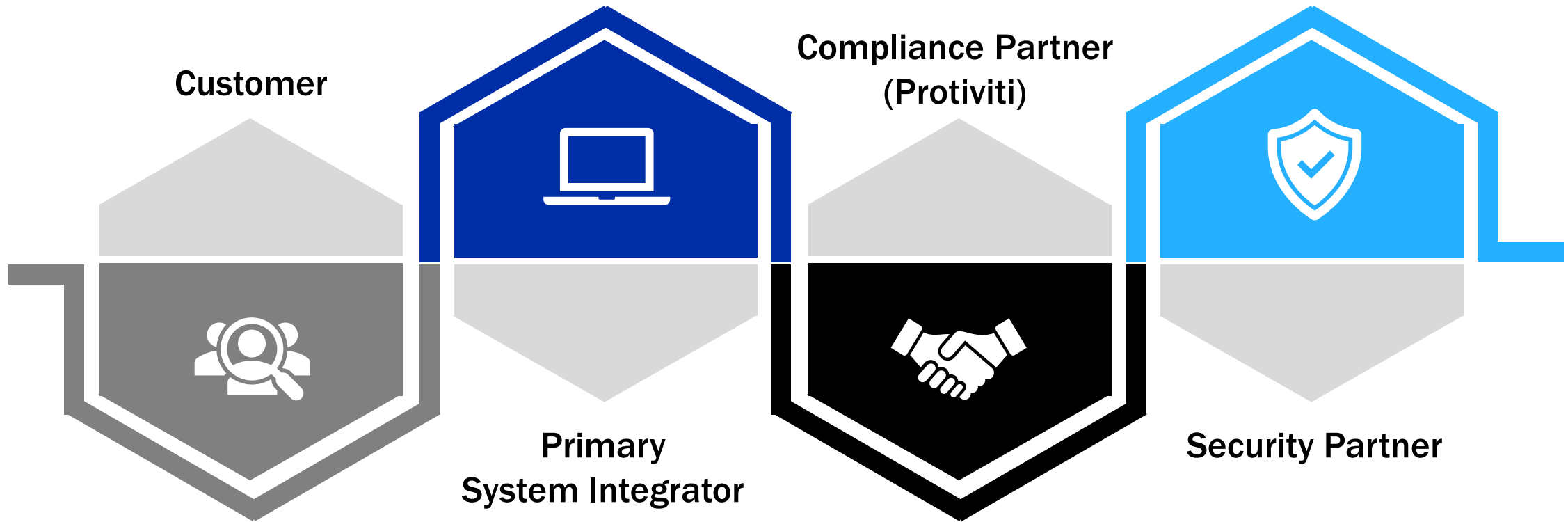
- SAP S/4HANA
- SAP GRC
- SAP CAR
- SAP GTS

# Phased Approach



# Multiple Partners - Defined

---





# Compliance Workstream

---

Overview of the compliance workstream focusing on key activities and ongoing maintenance required to ensure your organization continues to stay compliant:

- GRC
- Security
- Controls (Automated & CCMs)

# Compliance Overview

---

**GRC, Security and Controls should be considered from the beginning of your 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, etc.) that will help ensure your system stays compliant with regulations.**

**The compliance workstream consisted of the following core areas:**

- **GRC**
- **Security**
- **Controls (GRC Process Control & Automated Controls)**



# Compliance Overview - GRC

The objective of this workstream was to implement the SAP GRC Access Control tool to *enable* and **automate** key SAP S/4HANA security administration, **compliance monitoring** and **ongoing governance processes**.

In-Scope GRC Access Control Features:

Access Risk  
Analysis  
(ARA)

Emergency  
Access  
Manage-  
ment  
(EAM)

Access  
Request  
Manage-  
ment  
(ARM)

User Access  
Review  
(UAR)



# GRC Features Defined



## Access Risk Analysis (ARA)

### Key Activities

- Tailor ruleset to be specific to client's industry/risk profile
- Incorporate customizations (reports & custom transactions)
- Incorporate Fiori Apps

### Ongoing Maintenance

- Establish a process when new TCDs are introduced they are assessed for inclusion in the ruleset



## Emergency Access Management (EAM)

### Key Activities

- Design & Configure Firefighter
- Define EAM Strategy
  - Request/Approval Processes
  - Activities to be managed via EAM
- Log Review Workflow

### Ongoing Maintenance

- Establish a process to manage changes to FFIDs (roles, IDs, etc.), FF Owners, FF Workflow Design, etc.

# GRC Features Defined, Cont.



## Access Request Management (ARM)

### Key Activities

- Design Provisioning Workflows
- Configure Provisioning Workflows
- Determine approval attributes, role approval criteria, administrators

### On-going Maintenance

- Process Changes



## User Access Review (UAR)

### Key Activities

- Design UAR Workflows
- Configure UAR Workflows

### Ongoing Maintenance

- Process Changes (e.g., Template, Emails, Workflow, etc.)
- Role Owner Changes



# Compliance Overview – Security

The objective of this workstream was to design a custom set of SAP security roles that are **compliant** with SoD (Segregation of Duties) policies and are aligned with business users' responsibilities for the SAP production environment.

## Key Security Principles



- Task-Based Role Architecture
- Role Assignment Policy:
  - End users based on least access needed for job functions; and
  - Firefighter IDs based on functional area.

# Key Security Activities



## Plan & Design

- Develop SAP access management strategy and governance structure.
- Design conflict-free SAP task-based roles (e.g., PO Processing) based on SoD policies.



## Build & Test

- Work with Security Partner to build S/4 task-based roles.
- Document Unit Testing Efforts.
- Assist the Business with System Integration & User Acceptance Testing.



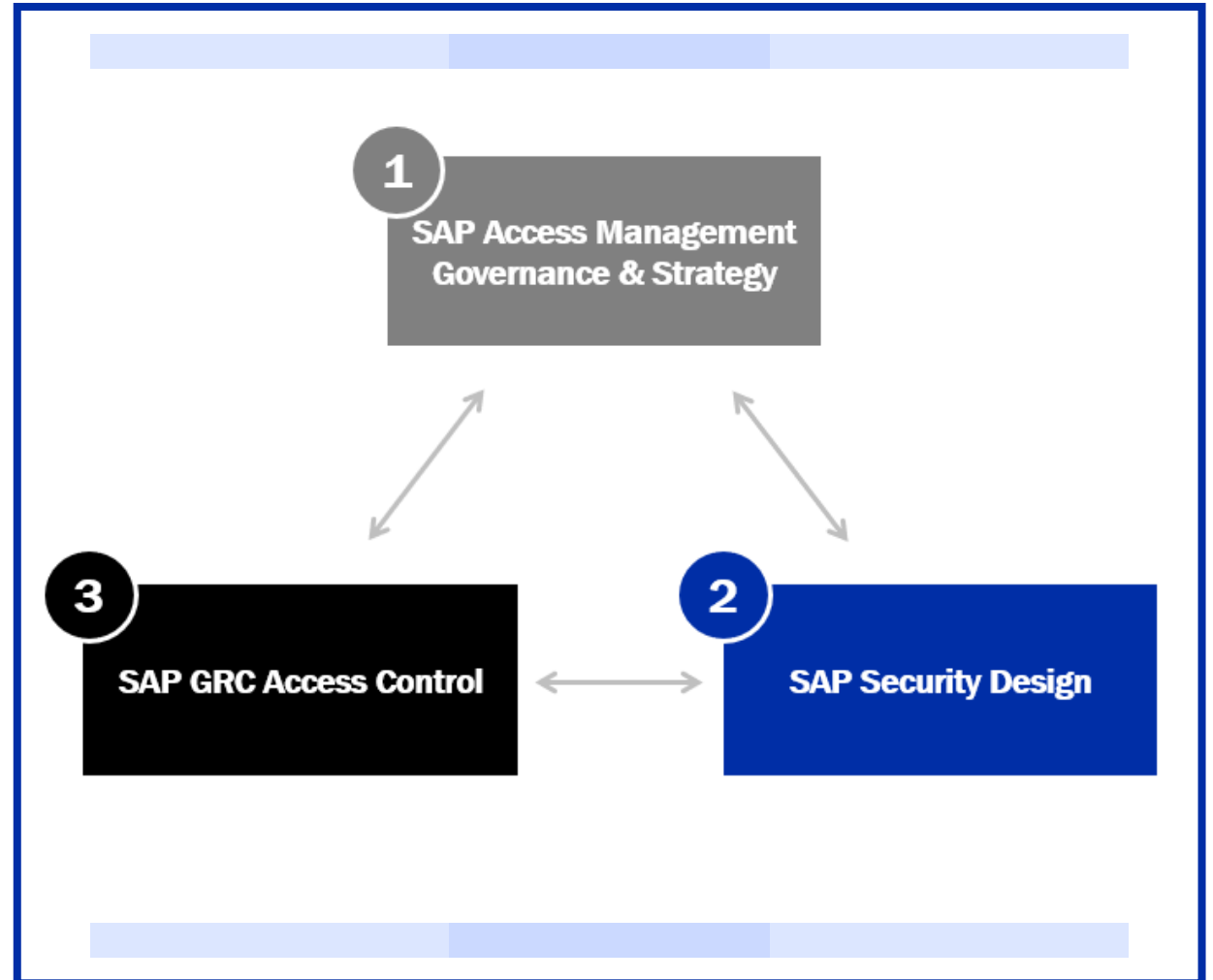
## Go-Live

- Provide support during Go-Live and stabilization period.
- Transition GRC and security monitoring and maintenance support to SAP Operations/Security Support.

# 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



# Compliance Overview – Process Controls

---



## What is SAP Process Control?

- Part of the SAP GRC Suite
- Supports the lifecycle of the Internal Controls Framework
- End-to-end management of compliance initiatives



- **Automated Controls**
  - SAP Configurations (e.g., 3-way Match)
  - Workflows (e.g., JE Approvals)
- Process Control (**Continuous Control Monitoring (CCMs)**) – automated monitoring of controls which can be used to cover any gaps in Automated Controls

# Compliance Overview – Automated Controls

The objective of this workstream was to ensure proper automated controls are designed to mitigate financial reporting risk for in-scope processes.

## Key Activities:



**Control  
Documentation**

**Control  
Rationalization**

**Control  
Automation**

**Control  
Optimization**



# Compliance Overview – Process Control (CCMs)

The objective of this workstream was to implement the SAP PC tool to enable continuous control monitoring (CCM) around SAP S/4HANA.

## Key Activities:



**GRC System  
Configuration &  
Validation**

**Business  
Blueprinting**









**CCM  
Implementation  
& Testing**

**Training & Go-  
Live Support**

# Ongoing Control Maintenance

---

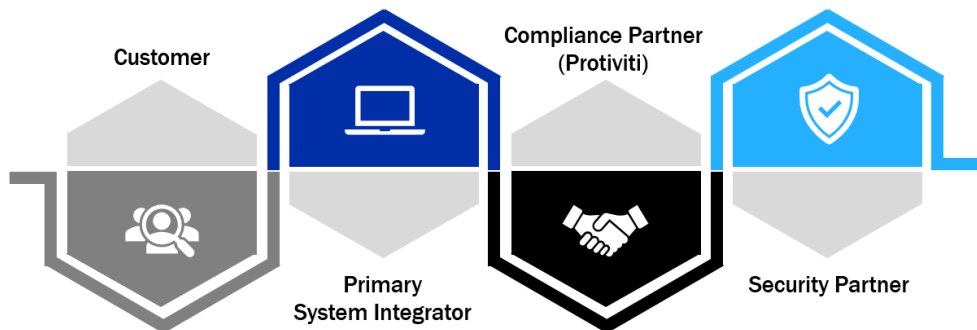
The below should be considered and managed to ensure your organization continues to stay compliant:

-   Changes to org structure
-   Personnel changes (e.g., control owner)
-   Changes to the risk environment
-   New systems, new functionality, process changes

# Collaboration with Other Partners

---

- Key collaboration points throughout the implementation timeline.
- Overview of integration between various compliance workstreams: PMO, GRC, Security & Controls.
- Key lessons learned when integrating multiple partners on an implementation project.



# Key Collaboration Points

## Prepare

- Integrating with the various partners and establishing roles & responsibilities
- Consolidating Project Plan(s)

## Explore

- Ensuring compliance was considered and prioritized as a part of design strategy (e.g., Automated Controls)
- Security and Controls teams participating in key design workshops

## Realization

- Supporting testing efforts with the business and troubleshooting errors
- Maintaining security role design for on-going changes
- Consolidating Cutover Plan(s)

## Cutover & Deploy

- Consolidating transports required for go-live
- Develop and deliver compliance-related training

## Hypercare

- Issue Resolution and Troubleshooting

# PMO Integration

---



- **Attended regular touchpoints with the Primary System Integrator's PMO to align the Compliance Workstream timeline and tasks to the overall project timeline**
- **Attended Bi-Weekly Leadership Calls**
- **Time/Budget Tracking**
- **Managed Project Documentation Repository (SharePoint)**
- **Project Scope Alignment**
  - **Notified the proper individuals if any project changes were discussed that would impact compliance efforts**



# GRC Integration

---



- Participated in System Integrator-led blueprint design sessions to provide feedback on GRC integration points
- Led design workshops with the various stakeholders (customer & primary SI) to define any custom deviations the customer needed from the standard set-up/workflow
  - SoD Ruleset Design, Custom Transaction Code Review, EAM Workflow, ARM Workflow, UAR Workflow, etc.
- Supported testing cycles

# Security Integration

---



- Participated in System Integrator-led blueprint design sessions to provide feedback on security.
- Led design workshops with the various stakeholders to confirm role design aligned with business users' key responsibilities.
- Designed a custom set of SAP security roles, following a least privilege methodology, that were compliant with SoD policies and shared design with the security partner to build in the system.
- Supported various testing cycles/hypercare and updated design and/or authorization restrictions as needed.

# Controls Integration

---



- Participated in System Integrator-led blueprint design sessions to provide feedback on controls.
  - Suggested automated controls should be “designed in” to the SAP system as much as possible to mitigate Financial Reporting risks.
- Led discussions with the various stakeholders (customer & primary SI) to confirm and validate the proposed automated controls along with the proposed CCMs.
- Supported testing cycles.

# Key Lessons Learned for Integration

---



- **Establish a RACI matrix for all project tasks**
  - **Ensure complete coverage of all tasks from start to finish**
  - **Customer should be responsible for facilitating agreement between all parties on RACI model**
  - **If it is not clear who owns a task, don't make assumptions**
- **Ensure regular communication cadence**
- **Establish a project governance group responsible for monitoring all 3<sup>rd</sup> party relationships**
  - **This group should meet regularly with leadership from each partner to ensure alignment and all pending issues are resolved**

# Wrap-Up

---

**Compliance was considered a priority workstream from the beginning.**

**Protiviti was brought in as a SME and secondary system integrator.**

**Multiple 3<sup>rd</sup>-party providers meant collaboration was required.**

**Key lesson learned include protectively addressing risks/issues related to integration.**

**Additionally, ensure roles and responsibilities are clearly defined.**



# Where to Find More Information

---

- Managing Risks Along Your SAP S/4HANA Journey
  - <https://www.protiviti.com/sites/default/files/2022-09/pov-internal-audit-role-sap-hana-protiviti.pdf>
- Designing SAP Application Security
  - <https://www.protiviti.com/sites/default/files/2022-09/designing-sap-application-security-protiviti.pdf>
- Controls and Automation for Finance: SAP's Game Changers Podcast
  - <https://sapblog.protiviti.com/2022/07/27/controls-and-automation-for-finance-saps-game-changers-podcast/>
- Achieve Seamless, Efficient SAP GRC Access Control Operations through Managed Services
  - <https://sapblog.protiviti.com/2022/08/02/achieve-seamless-efficient-sap-grc-access-control-operations-through-managed-services/>

# Key Points to Take Home

---

- **Compliance requirements should be integrated throughout the transformation process.**
- **Leverage a custom SoD and critical risk ruleset tailored to your industry and risk profile.**
- **Enhance current processes by implementing automated controls.**
- **Don't be afraid to bring in additional SMEs when your Primary SI has specific skillset gaps.**
- **Ensure all project dependencies are defined and monitored for a successful go-live.**

# Thank You! Any Questions?



**Liz Zuber**

[Liz.Zuber@protiviti.com](mailto:Liz.Zuber@protiviti.com)

<https://www.linkedin.com/in/lizzuber/>

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.

---