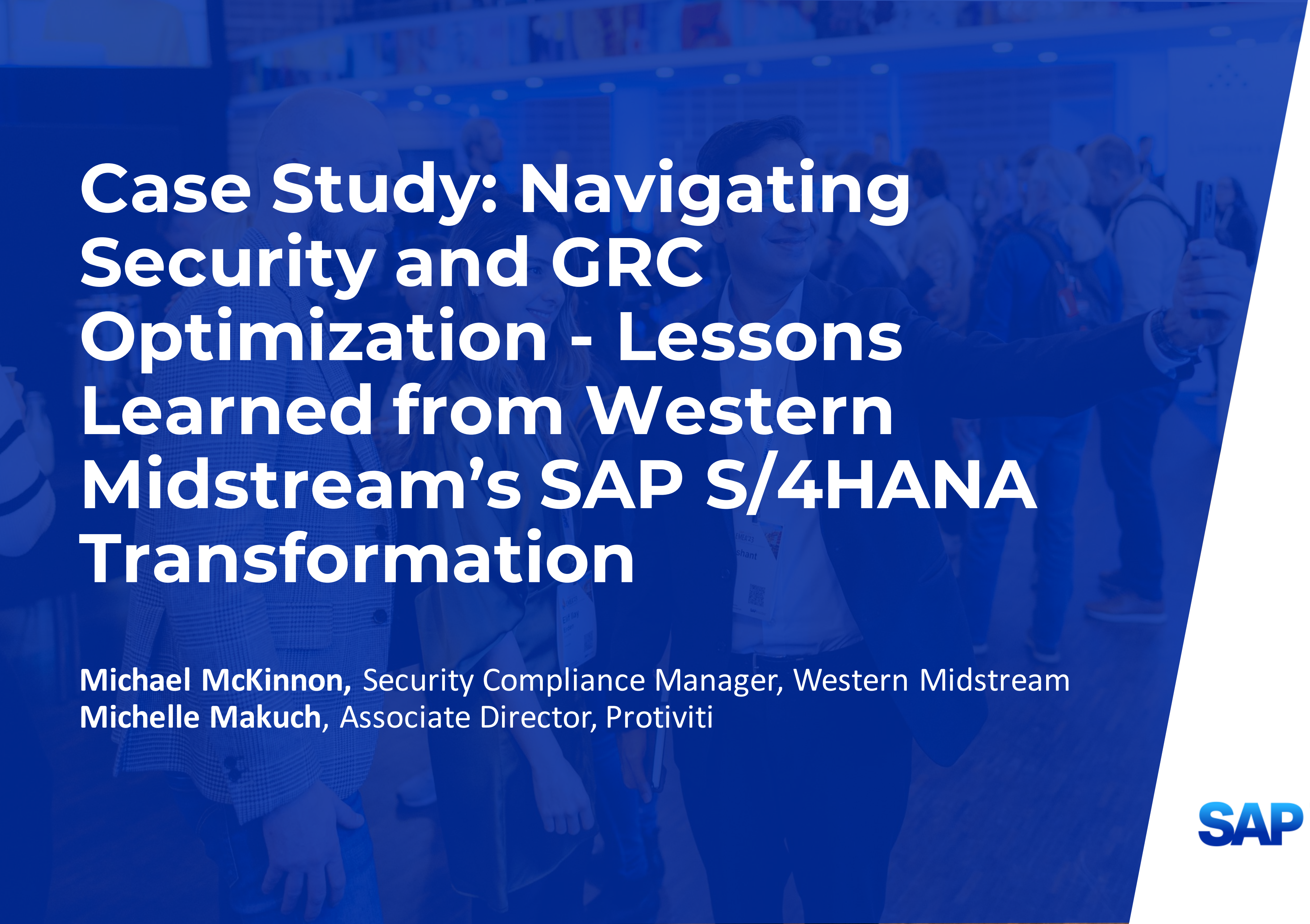


Case Study: Navigating Security and GRC Optimization - Lessons Learned from Western Midstream's SAP S/4HANA Transformation

Michael McKinnon, Security Compliance Manager, Western Midstream
Michelle Makuch, Associate Director, Protiviti

Las Vegas

2024

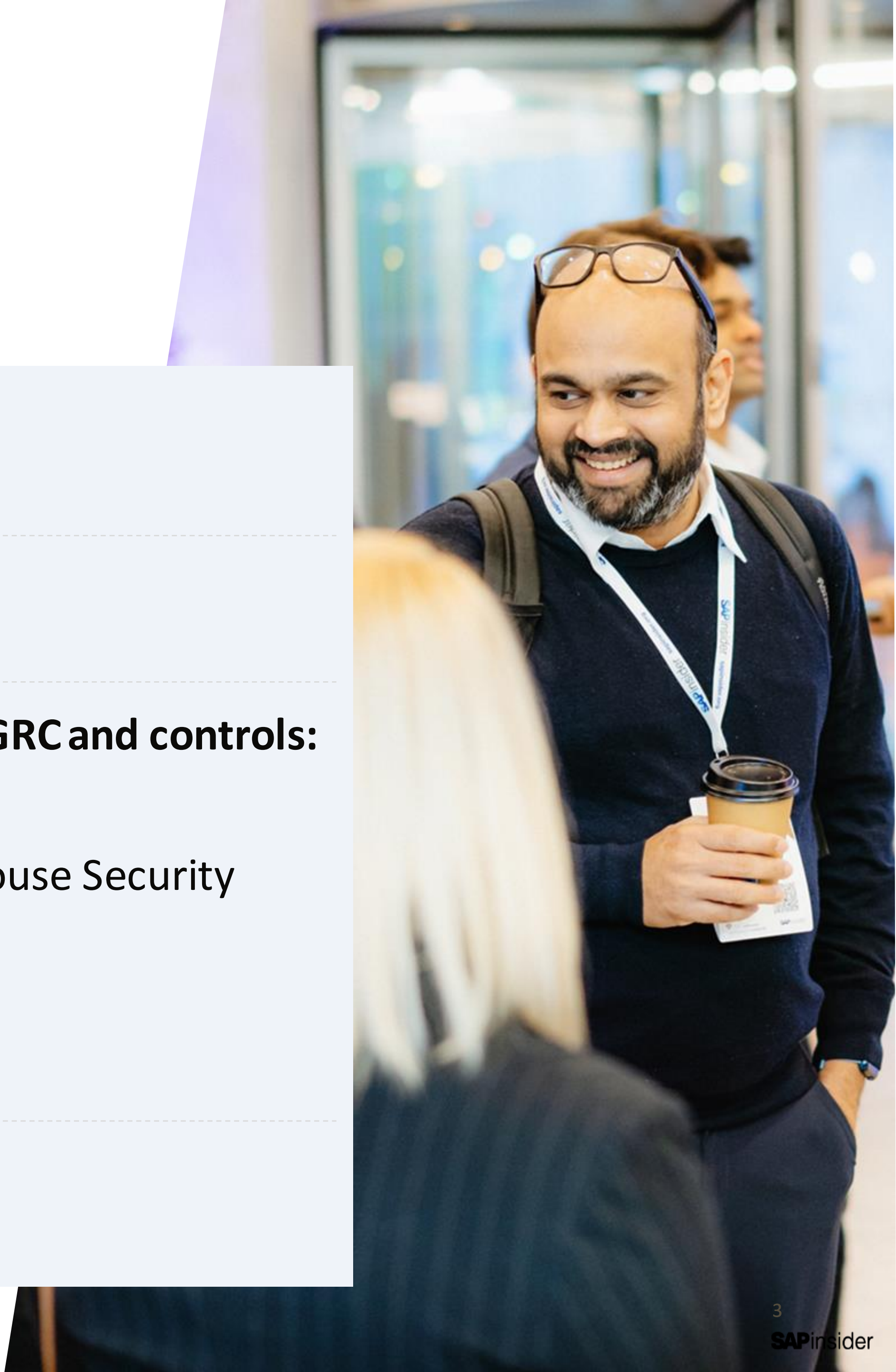
SAPinsider

In This Session

Gain key insights on how a midstream energy service provider:

- Successfully redesigned security task roles and business roles for all core business processes in S/4HANA and Fiori
- Designed and implemented security for SuccessFactors, Ariba and Business Warehouse
- Implemented GRC Access Control, including user provisioning at the business role level
- Performed benchmarking of system configurations against best practices to maximize the implementation of automated controls throughout the transformation

What We’ll Cover



Company Overview of Western Midstream

SAP Transformation Project Overview

Approach and lessons learned for security, GRC and controls:

- S/4HANA and Fiori Security Design
- SuccessFactors, Ariba and Business Warehouse Security Design
- GRC Access Control Implementation
- S/4HANA Automated Controls Assessment

Wrap-Up

Company Overview

Western Midstream (WES) is a midstream energy service provider based in The Woodlands, TX. It was founded by Anadarko Petroleum Co. (APC) in 2017 and eventually spun off into a standalone business in 2019 after Occidental Petroleum (OXY) acquired Anadarko. WES focuses on gathering, processing, and transporting natural gas and crude oil to end-use markets.

As a midstream service provider, Western Midstream helps deliver essential energy and inputs that improve the quality of life across the globe. WES focuses on ensuring the reliability and performance of our systems, creating sustainable cost efficiencies, enhancing our safety culture, and protecting the environment.

SAP Transformation Project Overview

The WES SAP Transformation project was business value driven and formed part of a broader Business Transformation Program.

Primarily Operations and Maintenance sponsored, the SAP Transformation aimed to enhance business processes and bring visibility to data to enable better business decisions and streamline business processes.

WES replaced a highly customized SAP R/3 environment designed and implemented for an integrated oil company with an SAP environment now designed specifically for a midstream business.

SAP Transformation Project Overview

- SAP S4 HANA
- SAP R3P Payroll
- Fiori
- Success Factors
- Ariba
- SAP GRC
- SAP Field Glass

- Business Warehouse (*SAP Data Sphere*)
- Signavio

S/4HANA and Fiori Security Design

The objectives of the S/4HANA and Fiori Security Design included:

- Designing and implementing **new end-user security roles** in S/4HANA and Fiori to support production security access at go-live as well as future access needs
- Enabling a **least privilege access** approach, reducing excessive access and restricting sensitive access
- Minimizing **Segregation of Duties (SOD) conflicts**
- Streamlining the **alignment of roles** to the organization

S/4HANA and Fiori Security Design Approach

The S/4HANA and Fiori Security Design included designing end-user Production access roles for all business processes in scope for the transformation project and for Information Technology. The high-level approach used during each project phase is described below:

Design

- Analyzed transaction code and Fiori app **requirements provided by functional teams**; extracted legacy ECC usage data as an additional reference
- Created a preliminary **task role design** based on **best practice** templates and **conducted design workshops** with all teams to review, including data restriction and business role requirements

Build

- Updated role design per workshop feedback and performed **task role build** and **technical unit testing**
- Executed **Segregation of Duties (SOD) analysis** with updated WES GRC ruleset to ensure **conflict-free task roles**
- Built **Spaces and Pages** for Fiori launchpad access

S/4HANA and Fiori Security Design Approach (cont.)

Test

- Conducted **functional unit testing on task roles** as part of System Integration Testing; testing was performed by WES business users
- Conducted **User Acceptance Testing** at the **business role level**; pre-testing was performed by the system integrator followed by business user testing

◒

Cutover

- Finalized role design and **obtained role owner approval**
- Conducted **user mapping to new business roles** and obtained role owner approval
- Migrated **roles to Production** and **assigned through GRC Access Control** per approved user mapping

◕

Go-Live & Hypercare

- Validated **user role assignments** in Production and executed **user-level SOD analysis**
- Supported **Production cutover and hypercare stabilization** period
- Finalized **documentation of security strategy** and design elements for future use

●

SuccessFactors, Ariba and Business Warehouse Security Design

The objectives of the SuccessFactors, Ariba and Business Warehouse (BW) Security Design included:

- Designing and implementing **new end-user security roles and groups** in **SuccessFactors** and **Ariba** to support production security access at go-live and as well as future access needs
- Designing and replicating **task-based Business Warehouse roles** for in-scope transactions/reports and incorporating into the appropriate Business Roles
- Enabling a **least privilege access** approach, reducing excessive access and restricting sensitive access

SuccessFactors, Ariba and BW Security Design Approach

The approach for SuccessFactors, Ariba and Business Warehouse Security Design consisted of Design, Build, Test, Cutover and Go-Live & Hypercare phases similar to the S/4HANA and Fiori security approach with key differences highlighted below:

SuccessFactors

- Designed and configured **Role-Based Permissions** per security requirements for Employee Central and Onboarding functionality in scope
- Created **source and target groups** to control access to specific data/populations; created **permission roles** and assigned the roles to groups

Ariba

- Designed and built **business roles and groups** in accordance with security requirements and feedback from design workshops
- Performed **user to group / business role mapping** and assigned roles to users

Business Warehouse

- Replicated and **adjusted the existing end-user Production roles** in upgraded environment for the reports in scope for the transformation
- Performed **SU25 upgrade steps** and incorporated changes to the replicated roles
- Incorporated **dynamic data restrictions** in roles

Security Design Lessons Learned

Security Design Lessons Learned

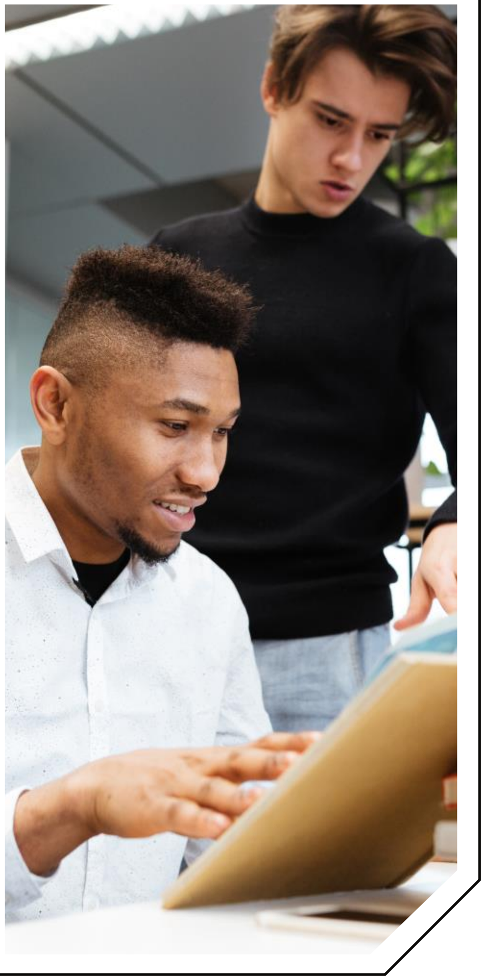
Incorporate the **security workstream early in the project** so it is considered in functional design and development decisions.

Document **access requirements** as an **output of functional design** sessions.

Consider the overall **strategy on access to data** within your organization when developing access approach.

Seek **leadership alignment** with access approach to ensure **consistent messaging** to the project team and user community.

Develop and communicate a **clear strategy on the use of Fiori** (vs. GUI access).



Security Design Lessons Learned (cont.)

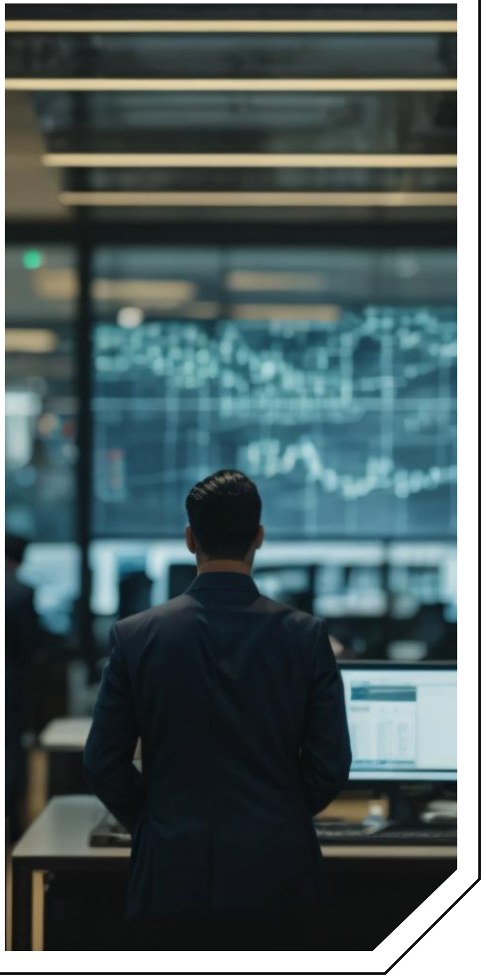
Minimize acceptance of changes past the security design phase of the project. Implement **rigorous change approval requirements** to facilitate this goal.

Identify and plan for **areas of complexity** during the design phase that will require **increased effort for security development and testing**.

Ensure awareness and coordination for any **integration-related dependencies** between S/4HANA security and other systems.

Consider security requirements for **reporting environments** (i.e., BW) to account for data restrictions in alignment with S/4HANA access approach.

Establish **clear role ownership by the business** to better ensure accountability for ongoing role change management, SOD management and user access reviews.



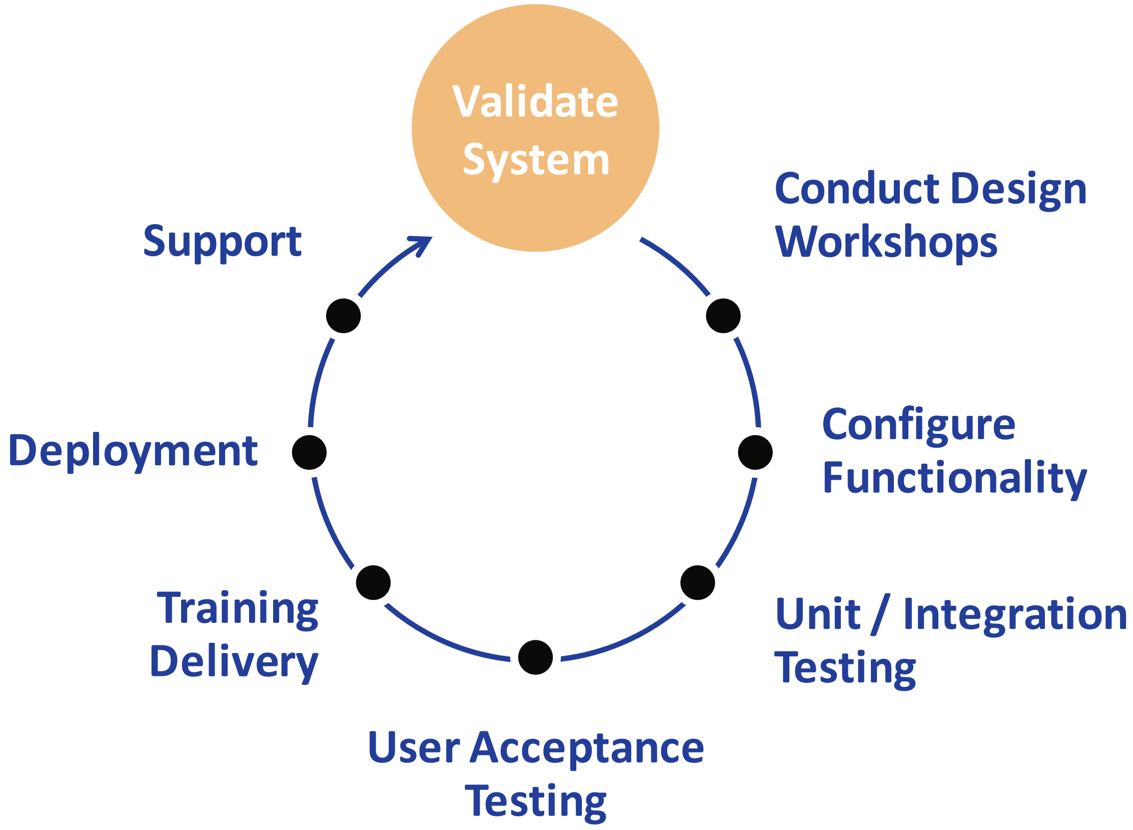
GRC Access Control Implementation

The objectives of the GRC Access Control Implementation included:

- Upgrading the GRC Access Control systems to the **latest version**
- Implementing Access Request Management (ARM) to **automate and simplify the access provisioning process**
- Implementing User Access Review (UAR) to **streamline user access reviews** that **automatically deprovision** access

GRC Access Control Implementation Approach

As part of the transformation project, the GRC Access Control Implementation approach included the phases depicted to configure, test and implement **GRC Access Control 12.0** as an **embedded** component on the S/4HANA stack.



GRC Access Control Implementation Approach Highlights

1 Designed and implemented **Access Risk Analysis, Firefighter, Access Request Management** and **User Access Review** functionality

2 Designed a **customized, leading practice SOD ruleset** which included custom transactions, Fiori apps and new S/4 transactions with **sign-off from Business owners**

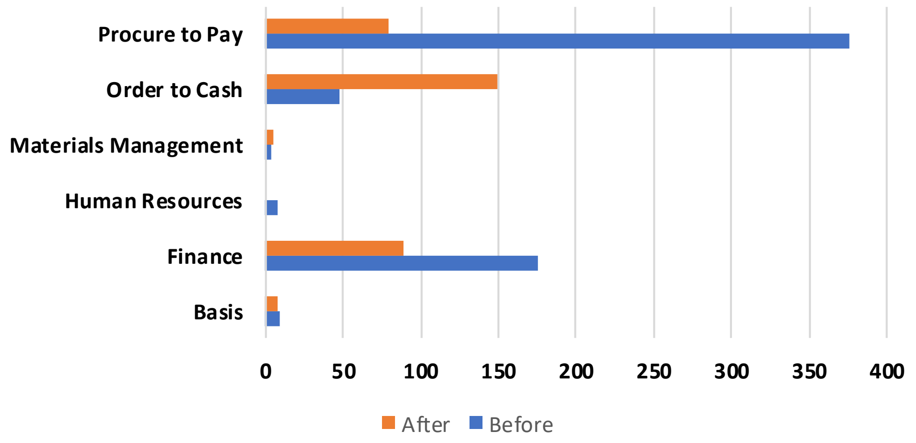
3 Configured **Business Roles** through Business Role Management to **simplify the user provisioning process**

4 Built **HR Trigger integration** through SuccessFactors to **automate birthright provisioning** and **user terminations**

5 Built **custom program** to populate HR personnel number in user master record to **enhance user experience** for time entry

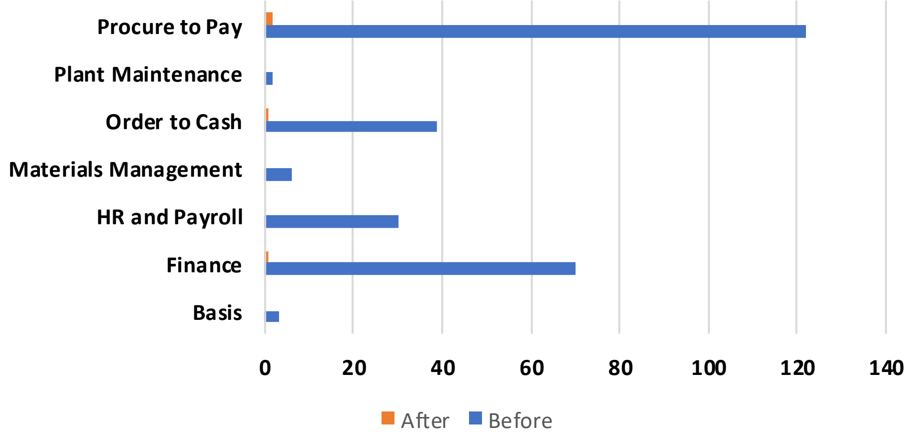
GRC Access Control - Segregation of Duties Key Metrics

Unique User Level SOD Violations



Business Process	Before	After	% Reduction
Basis	9	8	11%
Finance	175	89	49%
Human Resources	8	0	100%
Materials Management	3	5	-67%
Order to Cash	47	149	-217%
Procure to Pay	376	79	79%
Total	**618**	**330**	**47%**

Unique Role Level SOD Violations



Business Process	Before	After	% Reduction
Basis	3	0	100%
Finance	70	1	99%
HR and Payroll	30	0	100%
Materials Management	6	0	100%
Order to Cash	39	1	97%
Plant Maintenance	2	0	100%
Procure to Pay	122	2	98%
Total	**272**	**4**	**99%**

GRC Access Control Implementation Lessons Learned

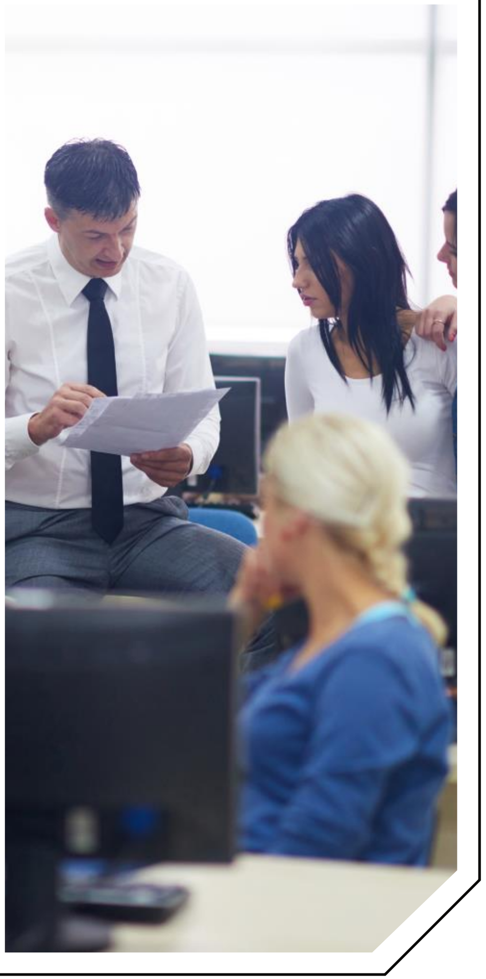
Consider **impacts of embedding GRC** within the S/4 system (ex. security role design, workflow engine considerations)

Firefighter approach for Fiori with 3rd Party SSO should be properly tested – web-based Firefighter vs Fiori through SAP GUI

Review pros and cons when **determining GRC data source** (HR vs LDAP)

Involve training and change management teams early in the project to properly plan future state onboarding process and access request process for end users

Ensure coordination with all key parties and integration teams when implementing **HR Triggers integration with SuccessFactors**



S/4HANA Automated Controls Assessment

The objectives of the S/4HANA Automated Controls Assessment included:

- Performing **benchmarking** of high criticality S/4HANA and Ariba **system configurations** against best practices to maximize and affirm the **inclusion of automated controls** as part of the implementation
- Validating the **resolution of identified automated controls gaps** prior to go-live
- Developing a **configurable controls baseline** that for future assessments and audits

S/4HANA Automated Controls Assessment Approach

The automated controls assessment included discovery and planning, focused on creating a preliminary list of leading practice and high criticality SAP S/4HANA controls. This was followed by several rounds of configuration validation in SAP and Ariba to inform the internal controls effort through the lifecycle of the implementation.

Discovery

- Reviewed relevant **business process design and implementation documentation** (business process flows, RICEFWs, functional specifications, etc.)
- Identified list of preliminary leading practice high **criticality SAP S/4HANA and Ariba controls**

System Integration Testing

- Validated SAP S/4HANA and Ariba configurations identified during Discovery within the SIT (System Integration Testing) environment to determine (1) **controls currently established**; (2) **opportunities to leverage automation**; (3) non-applicable controls (e.g., functionality not used)
- Held follow-up discussions with business process leads to confirm **configurations align with defined business requirements**
- Summarized and communicated **configuration changes** to system integrator

S/4HANA Automated Controls Assessment Approach (cont.)

The automated controls assessment included discovery and planning, focused on creating a preliminary list of leading practice and high criticality SAP S/4HANA controls. This was followed by several rounds of configuration validation in SAP and Ariba to inform the internal controls effort through the lifecycle of the implementation.

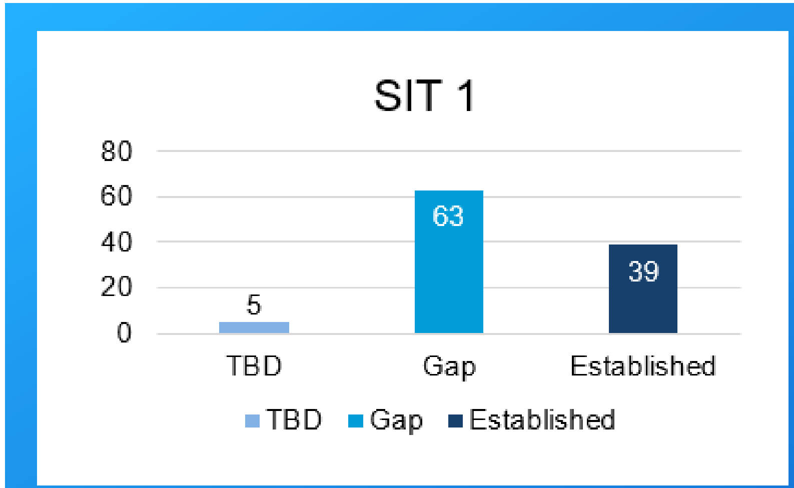
User Acceptance Testing

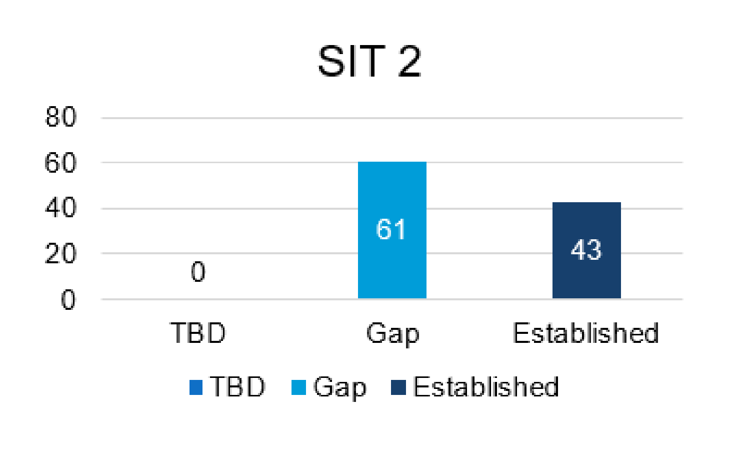
- Validated SAP S/4HANA and Ariba configurations within the UAT (User Acceptance Testing) environment to **determine whether configurations reflect controls and requirements** agreed upon during SIT
- Summarized and communicated **configuration changes** to system integrator
- Re-validated SAP S/4HANA and Ariba configurations pre-go-live to confirm that configuration changes were in place to support a **fully established control environment** for deployment

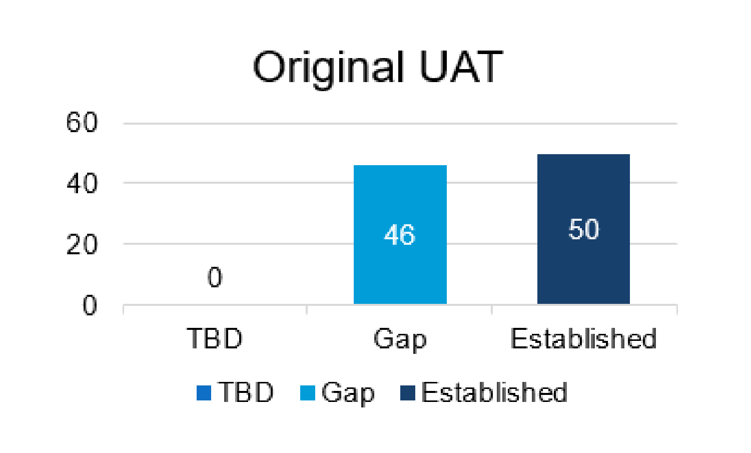
Go-Live & Hypercare

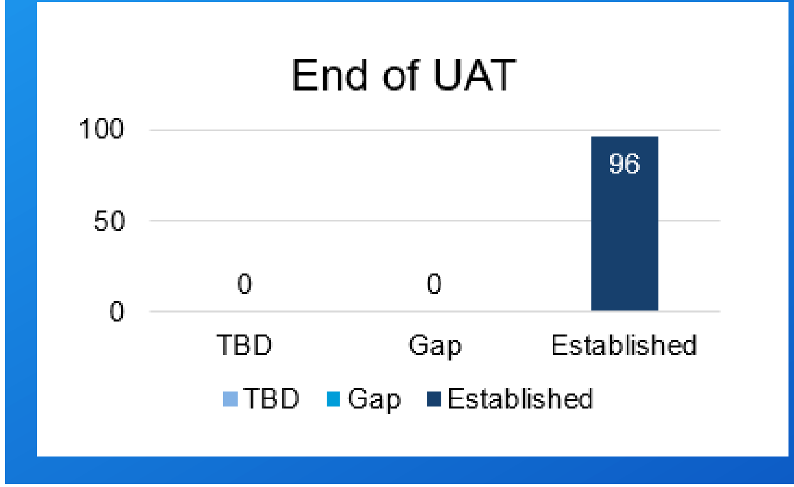
- Validated SAP S/4HANA and Ariba configurations within the PRD (Production) environment to determine whether **configurations and controls remained established**

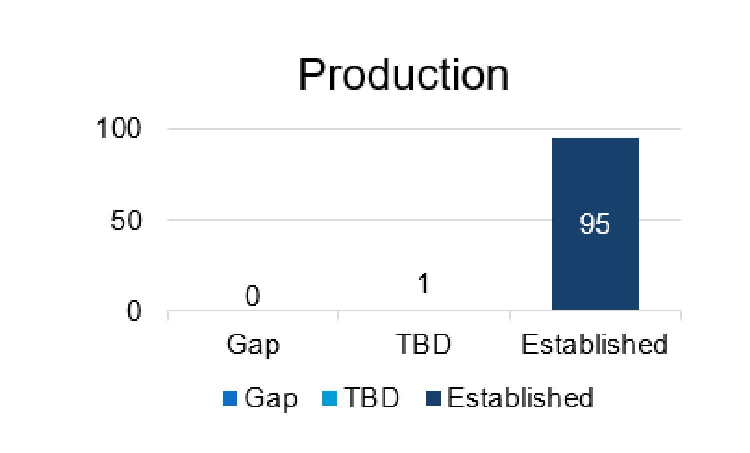
S/4HANA Automated Controls Assessment – The Journey to "Established"


SIT 1


SIT 2


Original UAT


End of UAT


Production

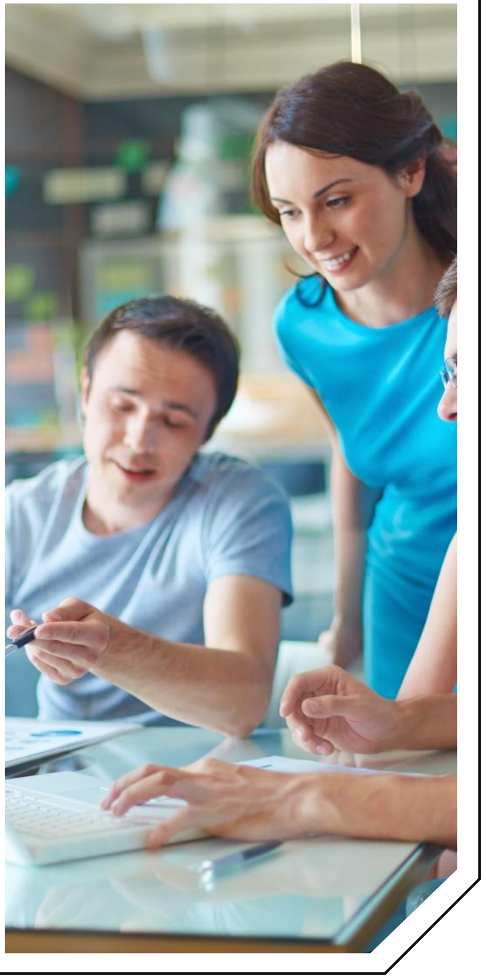
S/4HANA Automated Controls Assessment Lessons Learned

Establish a **controls workstream** as part of the SAP S/4HANA implementation program with a team that has **S/4 technical and risk management skills**

Define **inclusion of control requirements during SIT and UAT** testing cycles

Control requirements should be **documented and approved** within business process definition documents

Business process leads should be included in control discussions through the program to understand new/updated controls at go live, **minimizing the risk of control operating deficiencies**



Wrap Up

Where to Find More Information

Blog post describing the importance of security and controls within an implementation and selecting a partner with experience in developing strategic SAP security and access governance initiatives.

System Integrator or Security Specialist: Who Should Be Responsible for Implementing S/4HANA Security and Controls? - SAP Blog (protiviti.com)

Blog post on the importance of incorporating security best practices in Fiori Spaces and Pages design to create an intuitive user experience that supports a least privilege access model.

Mastering the Fiori Frontier: Crafting Secure, Intuitive Spaces and Pages in SAP S/4HANA - SAP Blog (protiviti.com)

Blog post on the importance of the Program Risk Management process and development of an effective governance structure for SAP S/4HANA projects.

Risk Management Essentials for SAP S/4HANA Projects - SAP Blog (protiviti.com)

Subscribe for Additional SAP Insights

learnmore.protiviti.com/SAPInsightssubscription

Key Points to Take Home

- Incorporate the security workstream early in the project so it is considered in functional design decisions
- Stress the importance of stakeholder involvement and engagement in design discussions
- Minimize acceptance of design changes past the design phase to prevent re-work that may cause delays in later phases
- Consider all integration points when designing the user access provisioning process
- Ensure contractual requirements for the system integrator to include your control requirements in the configuration and allocate time in the project plan to make the changes

Thank you! Any Questions?

Michael McKinnon, Western Midstream

Linkedin.com/in/mlmckinnon

Michelle Makuch, Protiviti

Linkedin.com/in/michelle-makuch-4553201

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.