Mastering Compliance and Efficiency – IFF's Journey with SAP GRC Access and Process Control

Michael Strause, Director of Information Security Architecture, International Flavors & Fragrances, Inc.

Las Vegas

2024

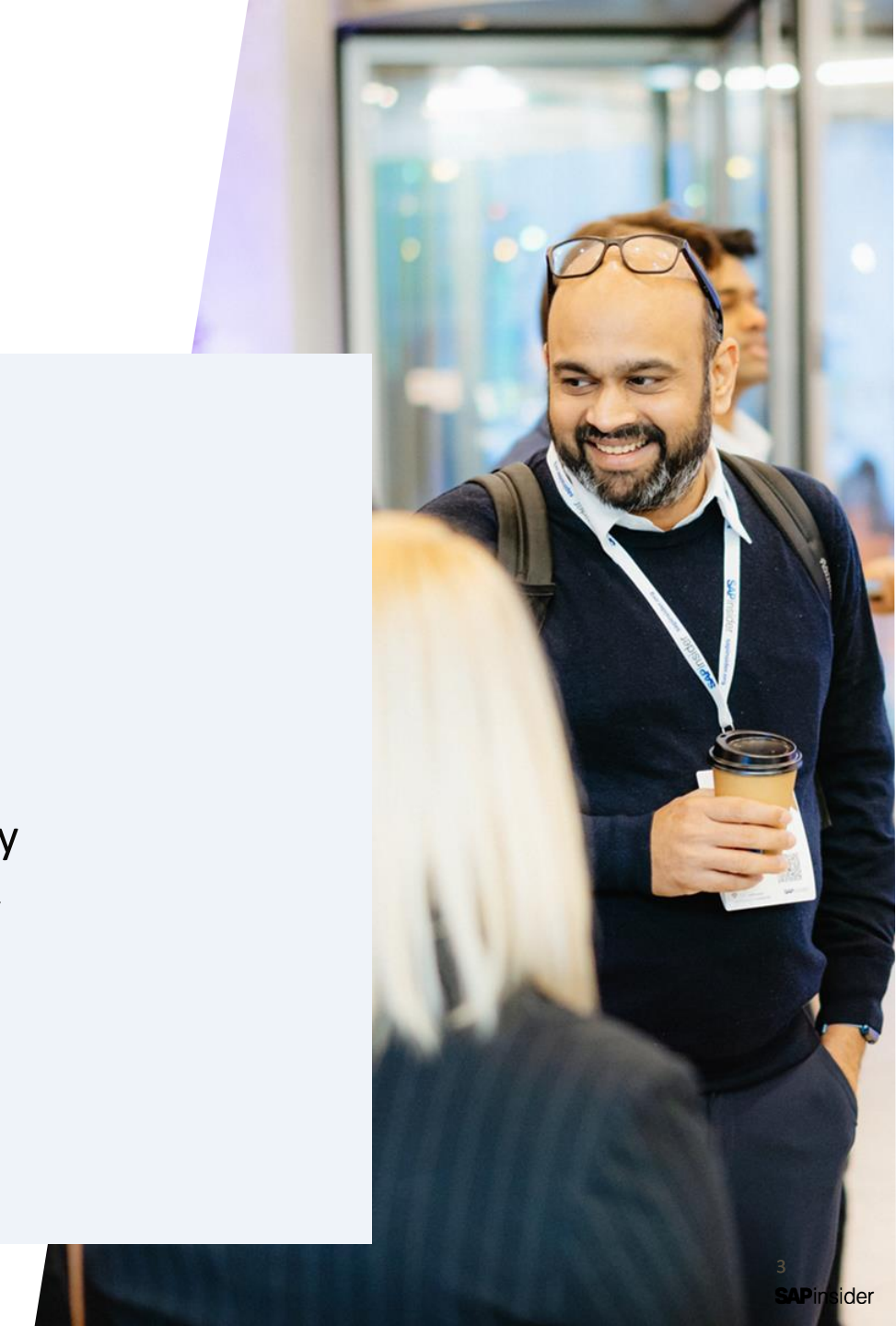
SAPinsider

In This Session

- Learn how International Flavors & Fragrances, a global manufacturing company, leveraged an SAP GRC implementation to help optimize and streamline business and compliance processes.
- From a GRC Access Control perspective, the organization was able to align 19 dependent target systems spread across five countries and thousands of users.
- From a GRC Process Control perspective, the organization was able to implement and streamline IT SOX controls across eight SAP S/4HANA and ECC environments.

What We'll Cover

- Company Background
- GRC Project Overview and Phases
- Phase 1
  - Standup New GRC Environment
- Phase 2
  - Enhance Access Control Functionality
  - Enable Process Control Functionality
- Future Phases and Roadmap
- Wrap-Up



Company Background

- Who is International Flavors & Fragrances?
- Large Scale M&A

Who is IFF?

International Flavors & Fragrances Inc. (IFF) is a global leader in food, beverage, biosciences, and sensorial experiences with over 400 locations and 25K technology users. Founded in 1889, IFF has grown by welcoming numerous brands into the IFF family. Most of these brands are fully integrated into our business, while others retained their unique business models and operate in harmony with the broader IFF brand.

IFF has an extensive and diverse portfolio of products to help create extraordinary sensorial experiences regardless of the category. We supply the food and beverage, home and personal care, and health and wellness markets with innovative solutions that allow them to create the products consumers know and love.

Project Drivers – Large Scale M&A

Revenue Increased from 5.1B to 12.44B

SOX Systems Increased from 4 to 19 SAP Landscapes

Headcount grew from 13.6K to 24.6K

IFF completes $26.2B merger with DuPont unit

Published Nov. 12, 2020 • Updated Feb. 1, 2021

Megan Poinski
Senior Reporter

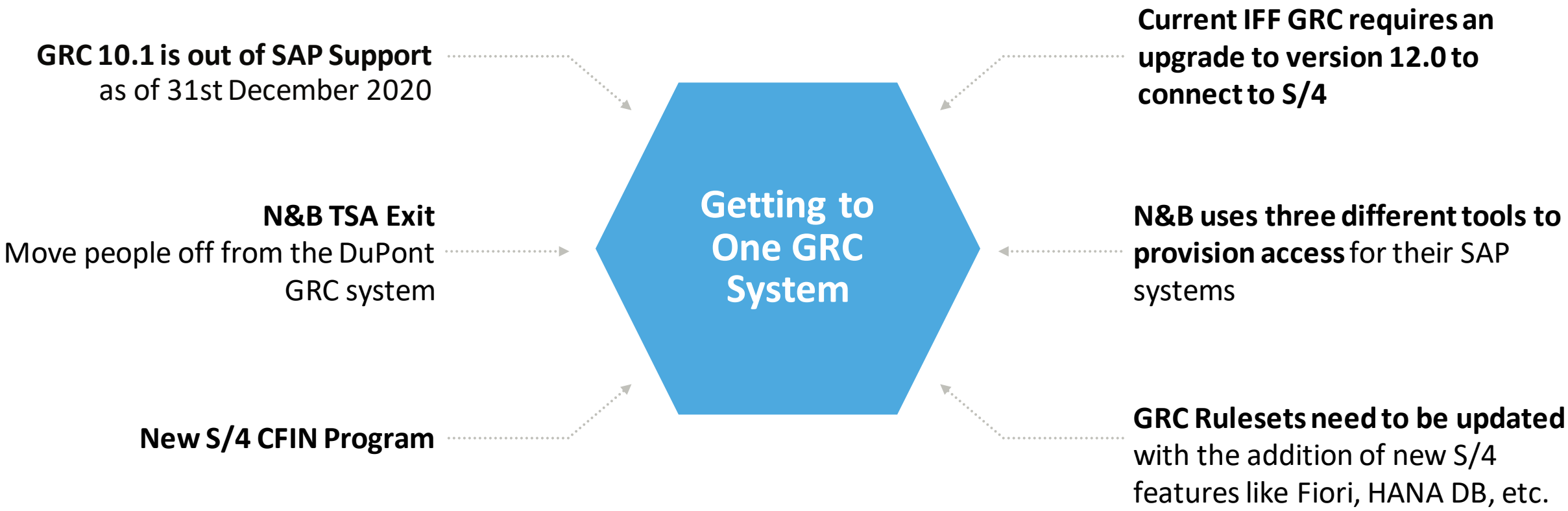
DUPONT IFF

NEW YORK--(BUSINESS WIRE)--Feb. 1, 2021-- IFF (NYSE: IFF) to complete the previously announced merger of IFF and DuPont's Nutrition & Biosciences ("N&B") business, pursuant to a Reverse Morris Trust transaction today. The combined company will continue to operate under the name IFF. Shares of the combined company's common stock will trade on the New York Stock Exchange under the symbol "IFF."

GRC Project Overview, Drivers, and Phases

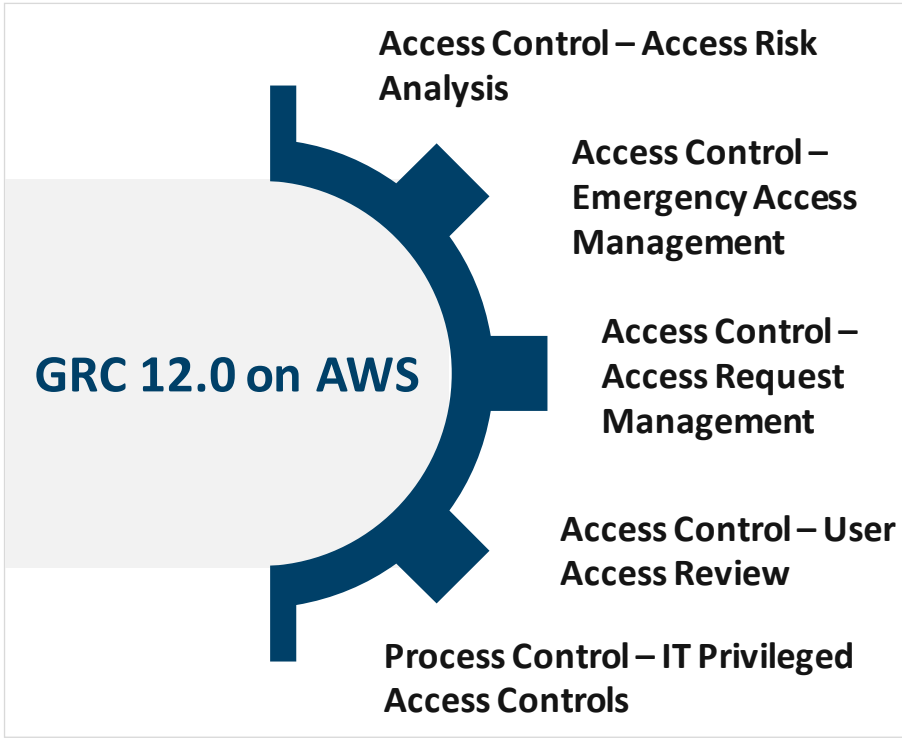
- Why Did We Upgrade GRC?
- Project Overview
- Our Complex SAP Landscape

Why Did We Upgrade GRC?



GRC Project Overview

Scope



20 Target Systems
connected over a period of 2 years (2021 to 2023)

~5300
Users onboarded to GRC 12.0

Deployed in over **400** locations in **66** countries globally

Project Team & Stakeholders

SteerCo
- CIO
- CISO
- Infrastructure
- PRO Sponsor

PMO
- Director (IFF)
- PM (IFF)
- PM/SME (PRO)

Execution
- Security Analyst (IFF)
- Functional Lead (PRO)
- Technical Lead (PRO)

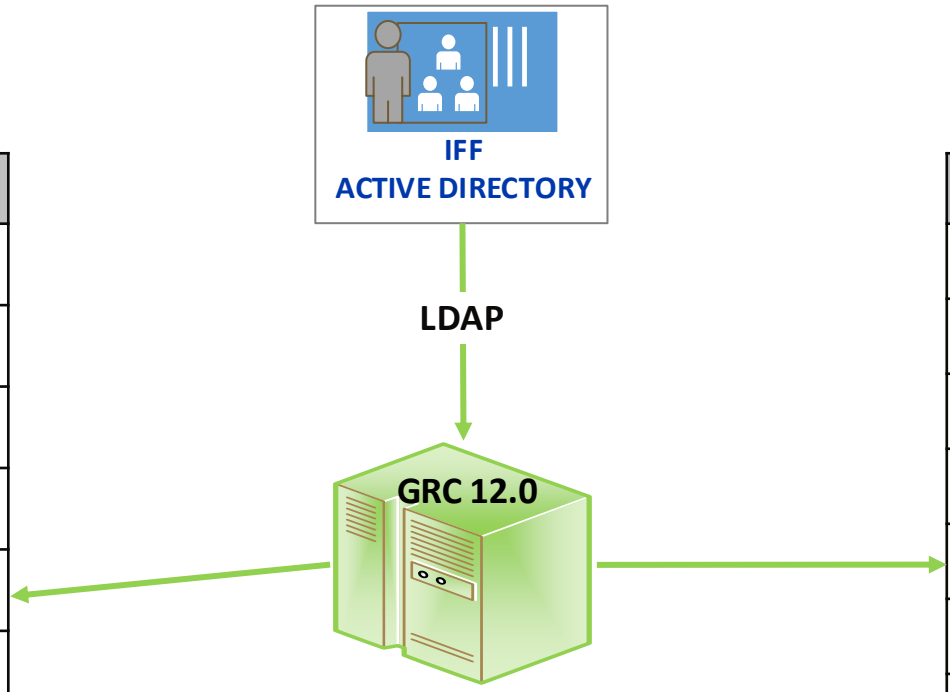
Corporate IT | **Enterprise Apps** | **Audit**

2021 Q3 | 2021 Q4 | 2022 Q1 | 2022 Q2 | 2022 Q3 | 2022 Q4 | 2023 Q1 | 2023 Q2 | 2023 Q3 | 2023 Q4 | 2024 Q1 | 2024 Q2 | 2024 Q3 | 2024 Q4

Phase 1 → Phase 2 →

Our Complex SAP Landscape

Landscape	System
N&B	ECC
N&B	ECC
N&B	SRM
N&B	APO
N&B	GTS
N&B	R/3 4.6C
N&B	BW
N&B	BW
N&B	HANA DB
N&B	IH



Landscape	System
IFF	ECC
IFF	GW
IFF	PLM
IFF	EPM
IFF	CFIN
IFF	GTS
IFF	SCM
IFF	CRM
IFF	BW
IFF	GRC 12.0

Phase 1 – Standup New GRC Environment

Below are the key features we attained through the implementation of a new GRC environment:

1. Unified Governance Environments
2. Standardization of Access Governance Processes
3. Integrated Segregation of Duties Ruleset
4. Customized User ID Management
5. Connection of Target Systems from Subsidiaries
6. Enhanced SOD Ruleset including CFIN Transactions

Phase 1: Stand Up GRC Environment (cont.)

	Key Feature	Approach	Benefits
1	**Unified Governance Environments**	Two different GRC 10.1 environments consolidated into one AWS cloud hosted GRC 12.0 environment	Simplified administration, reduced maintenance costs, and improved user experience with a unified governance framework
2	**Standardization of Access Governance processes**	Standardized and streamlined access governance processes, which differed across the two SAP GRC 10.1 environments, into unified processes in the new GRC 12.0 environment	Minimized risks, improved compliance, and streamlined user access management, ensuring consistent governance practices across the organization

Phase 1: Stand Up GRC Environment (cont.)

	Key Feature	Approach	Benefits
3	**Integrated Ruleset**	Integrated the Segregation of Duties (SOD) and Sensitive Access (SA) rulesets, which were initially distinct in two separate GRC systems, into one consolidated ruleset	Enhanced security, and improved audit readiness with a comprehensive and integrated SOD Ruleset
4	**Customized User ID Management**	Built customization around access provisioning, user termination, and search criteria to cater the requirements of different user ids for the same user in different SAP systems	Enhanced user experience and improved accuracy in access management by addressing the unique identity challenges within the SAP GRC 12.0 environment

Phase 1: Stand Up GRC Environment (cont.)

	Key Feature	Approach	Benefits
5	**Connection of Target Systems from Subsidiaries**	Successfully connected 20 target systems from three different subsidiaries / acquisitions (IFF, Danisco & Solae) to GRC 12.0	Enhanced consistency and centralized control over the access management process contribute to improved governance across subsidiaries
6	**Enhanced SOD Ruleset including CFIN Transactions**	Successfully connected new CFIN (IFF) system to GRC 12.0 and enhanced the SOD Ruleset to incorporate CFIN transactions	Increased accuracy in identifying and mitigating segregation of duties violations within the CFIN transactions

Phase 2 – Enhance Access Control Functionality

Below are the key features we attained by enhancing the existing GRC Access Control functionality:

1. Enhancement of User Provisioning Workflow
2. Efficient Handling of Non-SOX System Requests
3. Streamline NWBC UAR Experience
4. Implementation of Custom Fiori UAR App
5. Automated GRC Backend User Locking
6. Email Notification Enhancements
7. Identification of Cross-system SOD Conflicts
8. Implementation of Transactional Fiori Apps

Phase 2 – Enhance Access Control Functionality

	Key Feature	Approach	Benefits
1	**Enhancement of User Provisioning Workflow**	Enhanced user provisioning workflow by mandating inclusion of mitigated risk and enabling auto-population of RFD approvers at the approval stage, to ensure permanent retention of mitigated risks	Improved user experience by automating critical steps in the ARM workflow
2	**Efficient Handling of Non-SOX System Requests**	Enhanced ARM workflow by building a custom API-based rule, directing requests for Non-SOX systems to an alternative path where Risk Analysis is not mandatory	Increased efficiency, reduced processing time, and improved agility in handling Non-SOX system requests within the ARM workflow

Phase 2 – Enhance Access Control Functionality (cont.)

	Key Feature	Approach	Benefits
3	**Streamline NWBC UAR Experience**	Revitalized the NWBC UAR by streamlining processes, eliminating extra steps (e.g., save and then approve), and implemented daily reminders for reviewers to mitigate any potential delays in completion	Enhanced user experience, faster completion of UAR reviews, and reduced delays through a more intuitive and reminder-supported UAR workflow
4	**Implementation of Custom Fiori UAR App**	Implemented a customized Fiori UAR app, designed to optimize and expedite the User Access Review (UAR) process	Improved user experience, faster completion of UAR tasks, and a more user-friendly interface, enhancing overall satisfaction and efficiency in access review processes

Phase 2 – Enhance Access Control Functionality (cont.)

	Key Feature	Approach	Benefits
5	**Automated Backend User Locking**	Developed a custom program utilizing ARM workflow to implement locking of users in the backend systems, in alignment with requests for user terminations	Enhanced security measures, streamlined user termination processes, and reduced manual intervention
6	**Email Notification Enhancements**	Revised the content of all email notifications and implemented custom formatting by aligning standard notifications with custom formats written in HTML	Enhanced clarity, improved readability, and professional appearance of email notifications, leading to better user understanding and responsiveness

Phase 2 – Enhance Access Control Functionality (cont.)

	Key Feature	Approach	Benefits
7	**Identification of Cross-system SOD Conflicts**	Identified new Segregation of Duties (SOD) conflicts between CFIN and 3 SAP ECC target systems (IFF, Danisco & Solae)	Improved risk analysis, reduced chances of compliance violations, and a more robust control framework that considers the complex interactions between the three systems
8	**Implementation of Transactional Fiori Apps**	Implemented two transactional Fiori apps for GRC Access Control, enhancing the overall user interface and experience within the GRC AC system	Improved accessibility, responsiveness, and user experience

Phase 2 – Enable Process Control Functionality

Below are the key features we attained by enabling the GRC Process Control functionality:

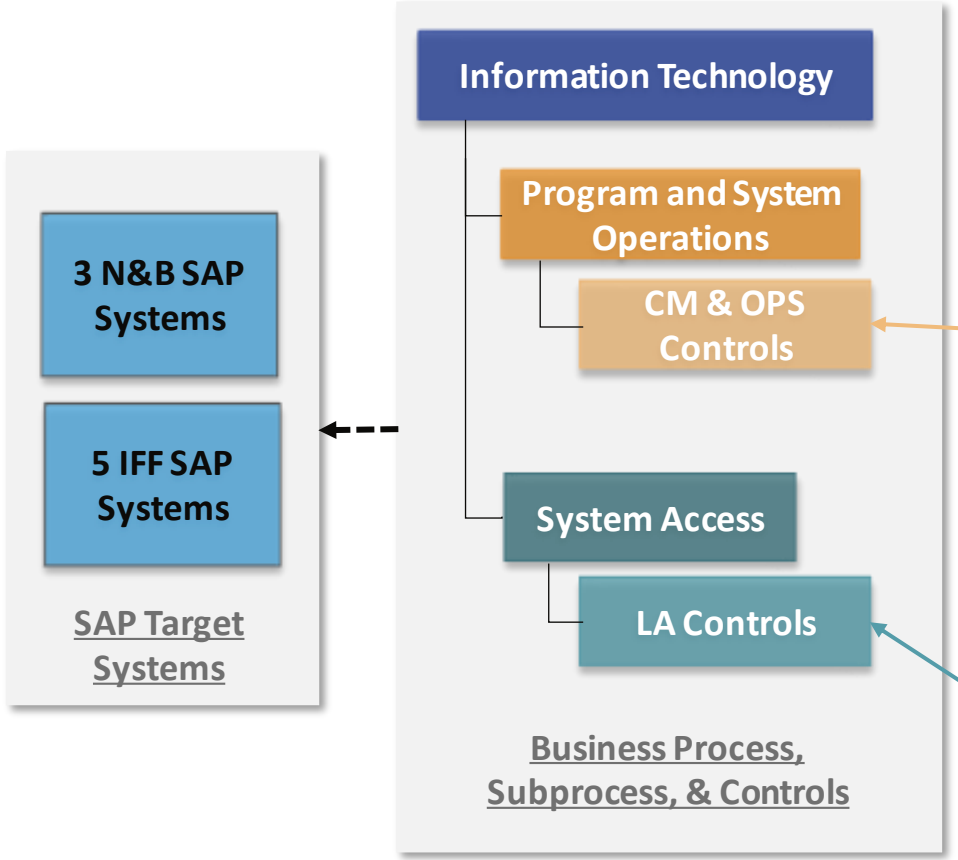
1. Automated IT SOX Controls with ABAP Report Sub Scenario
2. Automated IT SOX Controls with SOD Integration Sub Scenario

Phase 2 – Enable Process Control Functionality

	Key Feature	Approach	Benefits
1	**Automated IT SOX Controls with ABAP Report Sub Scenario**	Leverage standard SAP reports to automatically extract data from SAP environments and reduce time manually performing the tasks	Automatically generates list of users with access to critical SAP profiles that require further review across 8 SAP Production environments
2	**Automated IT SOX Controls with SOD Integration Sub Scenario**	Leverage existing GRC ruleset capability to add privileged access criteria and reduce time manually performing / testing IT SOX controls	Automatically generates list of users with access to approximately 77 different IT Basis and Security sensitive access transactions and authorizations across 8 SAP Production environments

Phase 2 – Enable Process Control Functionality (cont.)

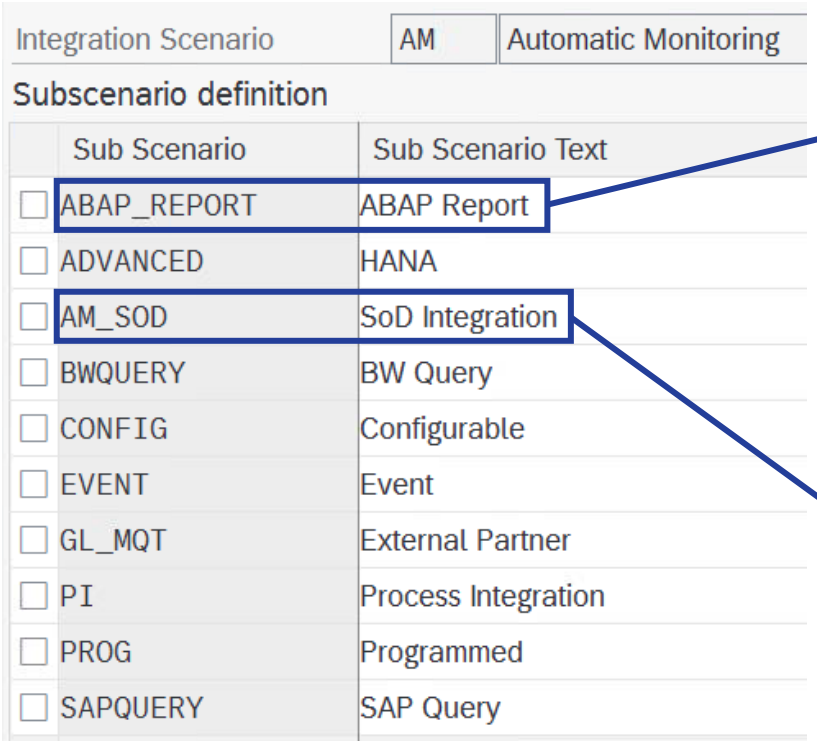
Automated monitoring of the below 7 IT SOX controls across 8 target SAP systems



Control ID	SOX Controls Description	Business Rule	Sub Scenario
CM.02	Access to system/client maintenance functions is limited to appropriate personnel.	BR_CM&OPS_ACPC	SOD Integration
CM.06	Access to import changes to production is restricted based on job functions	BR_CM&OPS_ACPC	SOD Integration
CM.07	Access to perform development/customizing functions in production or make an unauthorized change is prevented	BR_CM&OPS_ACPC	SOD Integration
OPS.04	Access to job scheduling function is appropriately restricted	BR_CM&OPS_ACPC	SOD Integration
LA.04 (A)	Access to privileged Profile Parameters Maintenance functions is limited to appropriate personnel	BR_LA04_ACPC	ABAP Report
LA.04 (B/C)	Access to privileged Profile Parameters Maintenance functions is limited to appropriate personnel	BR_LA04_ACPC	ABAP Report
LA.07	Access to User Maintenance functions is restricted to appropriate users based on job responsibilities	BR_LA07_ACPC	SOD Integration

Phase 2 – Enable Process Control Functionality (cont.)

Below is an outline of some steps you can follow to get these sub scenarios setup in your GRC environment:



Integration Scenario | AM | Automatic Monitoring

Subscenario definition

Sub Scenario	Sub Scenario Text
ABAP_REPORT	ABAP Report
ADVANCED	HANA
AM_SOD	SoD Integration
BWQUERY	BW Query
CONFIG	Configurable
EVENT	Event
GL_MQT	External Partner
PI	Process Integration
PROG	Programmed
SAPQUERY	SAP Query

1. Register report in SAP target system using tcode /GRCPI/OVERVIEW
2. Create report variant, if needed
3. Create Data Source using the above ABAP Report sub scenario
4. Create Business Rule and Link to relevant Control

1. Configure sensitive access criteria in GRC ruleset (critical actions or critical permissions)
2. Create Data Sources to enable data extraction
3. Create Business Rules & define filter criteria for potential exclusions (e.g., only dialog users, SAP system to be analyzed)
4. Link Business Rules to Controls and create a monitoring schedule

Addressing Key Hurdles and Future Phases

- Addressing Key Hurdles with Tailored Strategies
- Future GRC Roadmap for additional enhancements

Addressing Key Hurdles with Tailored Strategies

Challenges	Solution
GRC plugin install in some target systems had dependencies on additional components requiring updates	Target systems with component dependencies connected for access request creation only, with manual provisioning until dependent components can be updated
Different user id syntax across different subsidiaries / acquired companies	Custom solution built to map the different user IDs, which allowed system to recognize and change the Id based on system selected within Access Request
GRC Prod was on high availability OS whereas GRC Dev/QA were not, thereby causing performance issues and restricting ability to replicate network issues	OS version for QA environment updated to synch with Production thereby ensuring any future issues in Prod can be replicated to QA
Performing UAR in GRC AC for the first time was challenging for End users	Enhancing UAR for better user experience via NWBC customization and a custom Fiori app for UAR approval
SAP systems not connected to GRC where automated monitoring was not feasible had different reporting output	Developed Excel Macros to unify the reporting and approval process for manually extracted data related to the IT privileged access controls

Future GRC Roadmap

Extend PC functionality

- 2 additional IT controls that require GRC to be connected to Development and QA environments on target SAP systems
- Configure 55+ Business Process controls to enhance and automate the testing of SOX controls
- Align the IT and Business Process controls testing criteria across the company

Enhance NWBC Process

- Simplified role search based on a custom solution to restrict users from raising requests for more than one SAP landscape
- Custom solution for N&B systems default roles assignment policy
- Update HR Triggers process to extend current functionality to support new hires into GRC system

Implement Fiori Apps

- Fiori apps will give flexibility to access GRC via mobile/tablet
- All the customizations built in NWBC that are feasible will be extended to Fiori apps
- Implement three Transactional Standard Fiori apps (Access Request for Self, Access Request for Others and Mitigation Control) related to GRC Access Control

Wrap Up

- Where to Find More Information
- Key Points to Take Home

Where to Find More Information

Helpful Blogs:

- Mastering the Fiori Frontier: Crafting Secure, Intuitive Spaces and Pages in SAP S/4HANA
  https://tcblog.protiviti.com/2023/09/14/mastering-the-fiori-frontier-crafting-secure-intuitive-spaces-and-pages-in-sap-s-4hana/
- Enhancing the SAP GRC User Experience: Fiori Tiles in Access Control, Process Control and Risk Management
  https://tcblog.protiviti.com/2023/08/08/enhancing-the-sap-grc-user-experience-fiori-tiles-in-access-control-process-control-and-risk-management/

Helpful SAP Notes:

- Dependencies for GRC 12.0 Access Control plugins and other components in relation to Fiori and other target systems
  2654895 - FAQ: GRC Access Control 12.0 Installation Questions and Recommendations - SAP for Me
- Firefighter Logs not being triggered to Firefighter Controllers in SAP GRC
  2784131 - EAM: Firefighter Logs and Workflows intermittently missed - Possible reasons - SAP for Me
- Page load issue while accessing Fiori Launchpad
  3361852 - Access Approver Refresh reload was not working. - SAP for Me

Additional SAP Insights:

- Subscribe to SAP Insights featuring SAP blogs and monthly newsletters
  https://learnmore.protiviti.com/SAPInsightssubscription

Key Points to Take Home

- Getting in front of business in advance to understand pain points is critical
- Lookout for user experience early on to ensure user adoption, minimize push back and impact to key SOX processes (UAR)
- Reaching alignment on technical dependencies quickly and accelerating planning activities
- Ensure thorough testing is performed to uncover potential issues
- Train the user population and have recordings readily available

Thank you! Any Questions?

Michael Strause

https://www.linkedin.com/in/michaelstrause

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.