



The Evolution of a GRC Customer: Taking Control of Your GRC Destiny

James E. Roeske, CEO
Customer Advisory Group

SAPinsider
2023

A woman with blonde hair and glasses, wearing a black vest over a floral patterned top, is smiling and looking towards the right. She is seated at a conference table with a white coffee cup in front of her. Other people are visible in the background, also seated at tables.

In This Session

- **Learn how to shift from a GRC Initiative that's reactionary to one that is proactive and preventative with proper planning.**
 - Understand the typical journey and evolutionary path a GRC customer goes through to reach "continuous compliance" utilizing the full suite of SAP solutions for GRC
 - Learn how to define your current state of GRC evolution and map out a realistic plan for your destination of compliance
 - Gain real-world insight based on 250+ GRC customer projects, including key tips to enhance ROI and successful implementation strategies
 - Explore how solutions like SAP Access Control, SAP Process Control, and SAP Risk Management allow you to achieve short-term and long-term compliance goals

What We'll Cover

- **GRC Evolution – Times are changing, are you keeping up? Do you have a plan?**
- **Two different types of Evolution:**
 - #1. Evolution of SAP GRC Technology.
 - #2. Evolution of Customers GRC Requirements.
- **Where are you on the GRC Roadmap?**
- **The GRC Journey – “Think Big, Start Small and Work Smart”**
- **Wrap Up**



Changing Times!

The Past - Back in the old days, SOD Compliance was a foreign, difficult, and unappreciated thing that was left up to the “Security Administrator”.

The Present - Robust risk analysis functionality exists in the SAP GRC applications which brings to light many issues that customers were previously unaware of.

- The Auditors and Management say we need to get our SAP systems “clean” of Segregation of duties conflicts. But when I run Risk Analysis it tells me I have 2.5 Million SOD violations!

The Future - The definition of “Compliance” is ever changing, New Regulations, Audits become more detailed every year. They are looking at ALL systems in your entire landscape, processes, and all fraud/risk areas.

- I need to get my entire company’s landscape compliant. This means managing, mitigating, and eliminating Risk across my entire company! And Senior Management is watching!

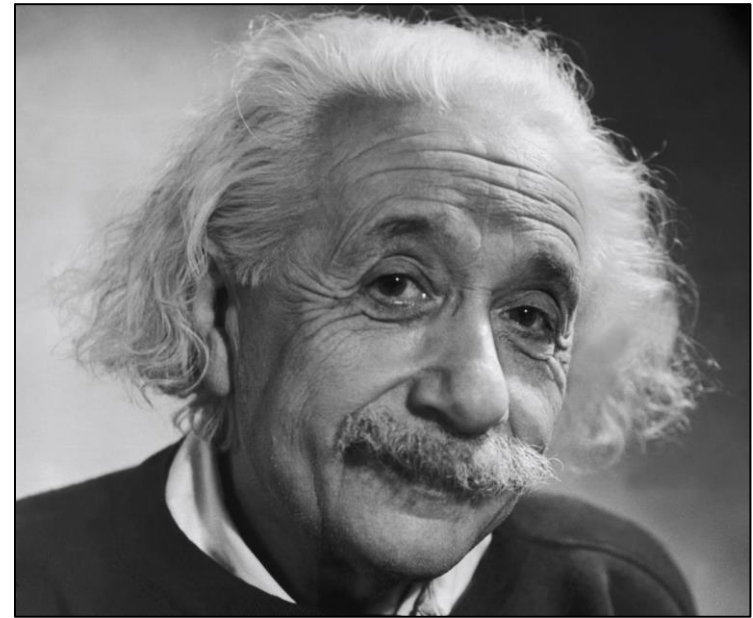


Compliance Road Map, Do I Need One?

- Aren't you glad that Albert is not your Corporate Compliance Officer or SAP Security Administrator!!!

**“I never think of the future –
it comes soon enough.”**

[Albert Einstein \(1879-1955\)](#)



- GRC requirements, compliance regulations, customer needs are constantly evolving. Planning for today and setting the correct foundation for the future of your GRC requirements are **ESSENTIAL** to success.

Customers Perception of GRC



Customers who don't have a plan, describe GRC processes as:

“Unpredictable” “Reactionary” and “Overwhelming”

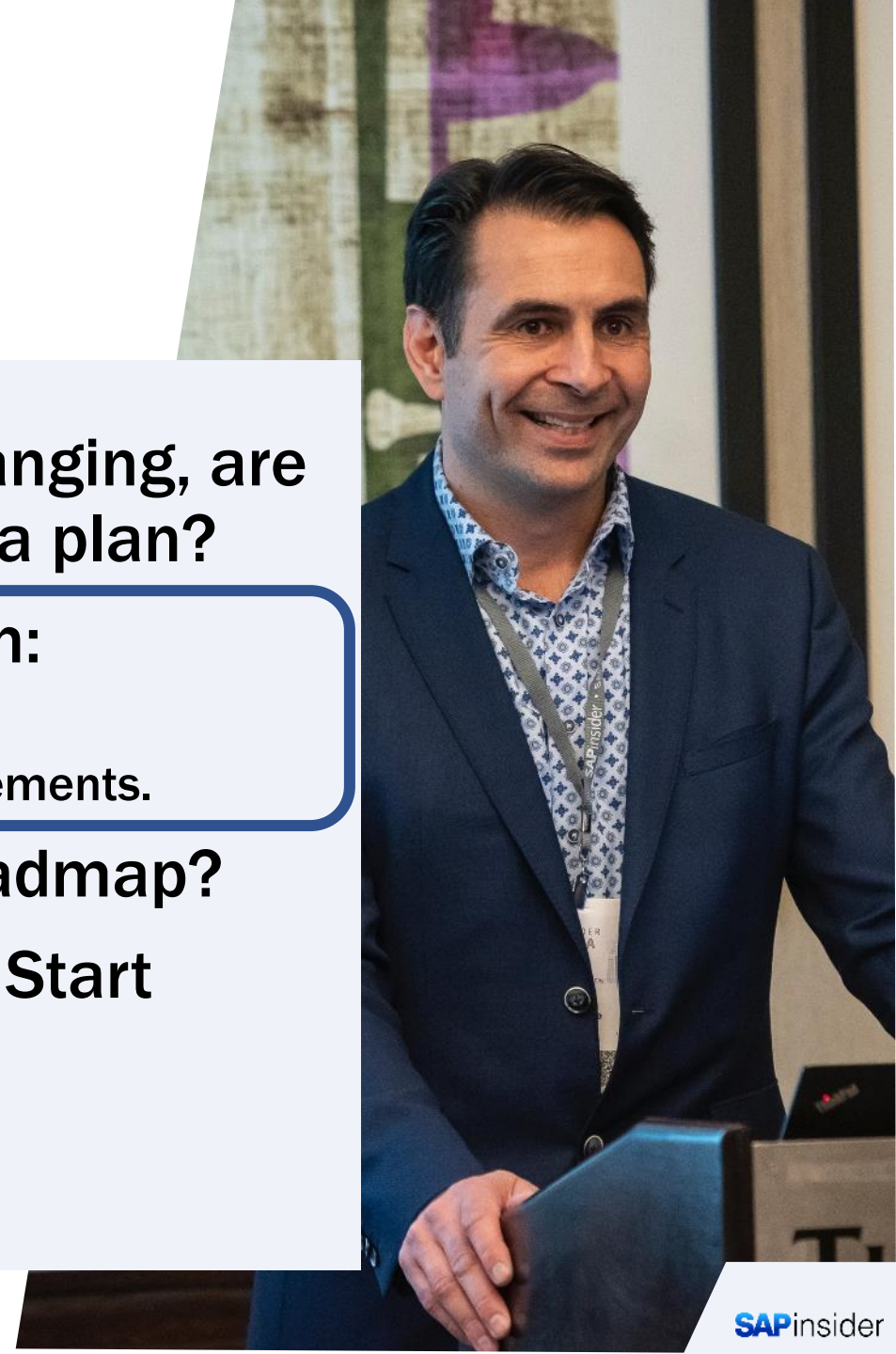


Customers who do have a plan and are continuing to evolve their GRC process and SAP GRC tools, describe GRC processes as:

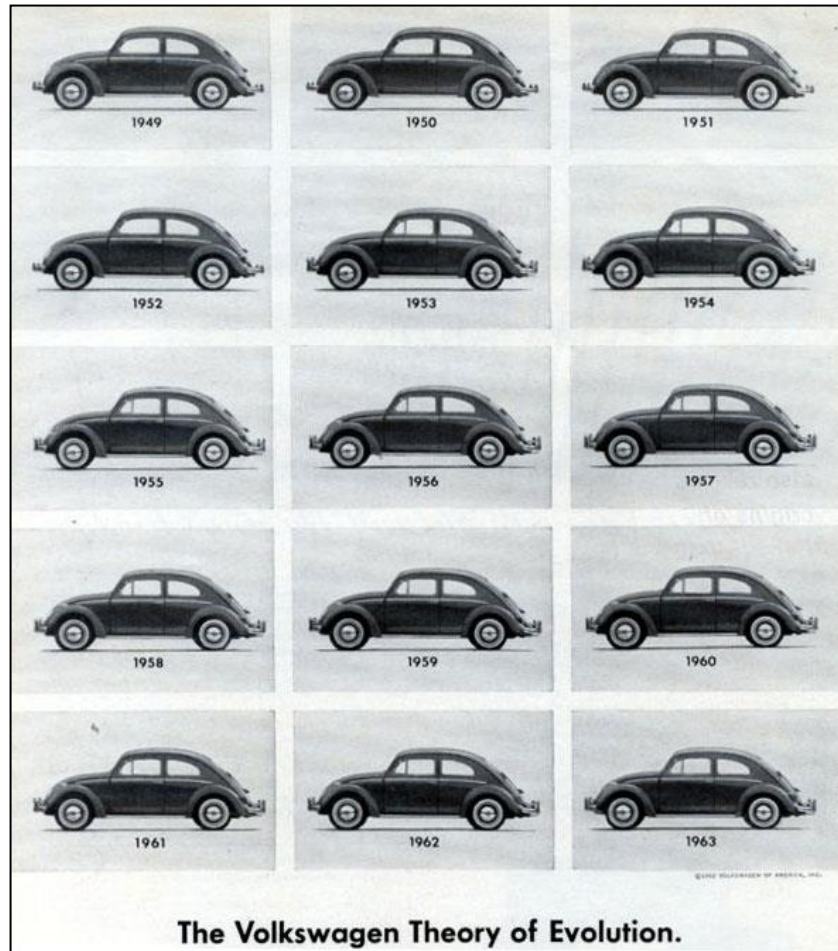
“Business Essential” “Controlled” and “Automated”

What We'll Cover

- GRC Evolution – Times are changing, are you keeping up? Do you have a plan?
- Two different types of Evolution:
 - #1. Evolution of SAP GRC Technology.
 - #2. Evolution of Customers GRC Requirements.
- Where are you on the GRC Roadmap?
- The GRC Journey – “Think Big, Start Small and Work Smart”
- Wrap Up



Is Your GRC Program's Evolution Like a VW Beetle or a Porsche 911?

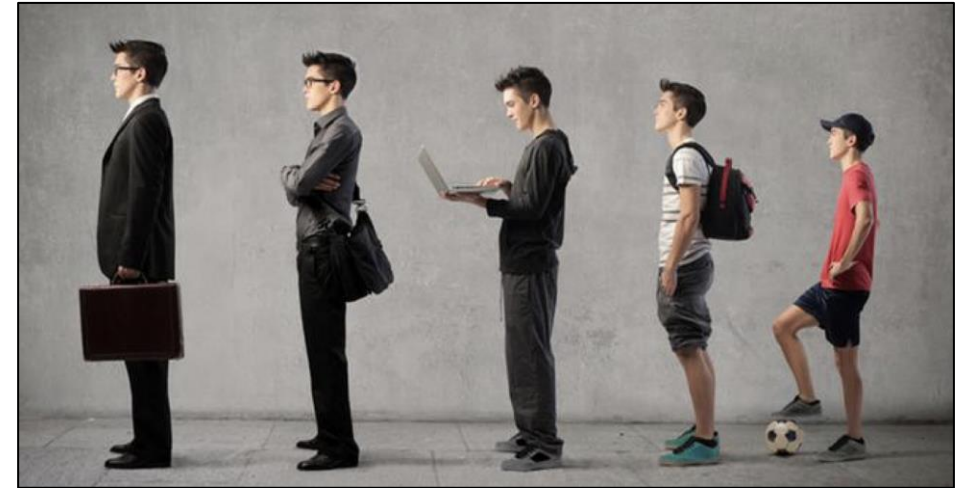


Two Things to Navigate while building a GRC Roadmap

#1: Evolution of GRC Technology



#2: Evolution of a Customer's GRC Requirements



#1. Evolution of SAP GRC Access Control!

Version

10.x - Access Risk Analysis
5.3 - Risk Analysis and Remediation
4.0 - Compliance Calibrator
1.0 - Virsa VRAT

Version

10.x - Emergency Access Management
5.3 - Super User Privilege Management
4.0 - FireFighter
1.0 - Virsa VFAT

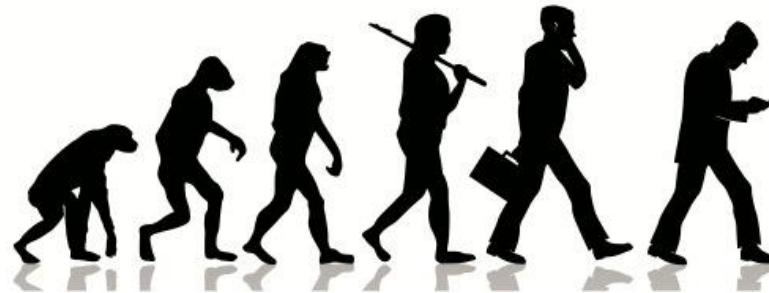
Version

10.x - Access Request Management
5.3 - Compliant User Provisioning
4.0 - Access Enforcer

Version

10.x - Business Role Management
5.3 - Enterprise Role Management
4.0 - Role Expert

**Much has changed over the years!
Including product functionality,
application names, and technology
platforms.**



4.0

ABAP

5.3

NetWeaver®

10

ABAP

10.1

ABAP
+ HANA

New and Improved!



Application	Component
Access Risk Analysis	GRAC-SAC-ARA
Emergency Access Management	GRAC-SAC-EAM
Access Request Management	GRAC-SAC-ARQ
Business Role Management	GRAC-SAC-BRM

GRC Access Control 12.0

ABAP + HANA + Fiori UI

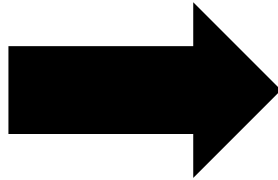
Service	Component
Access Analysis Service	GRC-IAG-AA
Privileged Access Management	GRC-IAG-PAM
Access Request Service	GRC-IAG-AR
Role Design Service	GRC-IAG-RD
Access Certification Service	GRC-IAG-CER

SAP Cloud Identity Access Governance

Cloud

#2. Evolution of a Customers GRC Requirements

What was once thought of as a “very thorough” and “progressive” GRC customer environment a few years back is now classified as a minimum requirement today!



SAP Products to Address GRC Challenges – Today Vs Tomorrow

SAP GRC and Security solutions

Solution mapping to key themes



Enterprise Risk & Compliance

- ✓ SAP Process Control
- ✓ SAP Risk Management
- ✓ SAP Audit Management
- ✓ SAP Business Integrity Screening



Identity & Access Governance

- ✓ SAP Access Control
- ✓ SAP Cloud Identity Access Governance
- ✓ SAP Access Violation Management by Pathlock
- ✓ SAP System Integration edition by Pathlock
- ✓ SAP Dynamic Authorization Management by NextLabs
- ✓ SAP Single Sign-On
- ✓ SAP Cloud Identity Services – Identity Authentication
- ✓ SAP Identity Management
- ✓ SAP Cloud Identity Services – Identity Provisioning



Cybersecurity, Data Protection & Privacy

- ✓ SAP Enterprise Threat Detection
- ✓ SAP Privacy Governance
- ✓ SAP Privacy Management by BigID
- ✓ SAP Customer Data Cloud
- ✓ SAP Data Custodian
- ✓ SAP Data Custodian, Key Management Service (KMS)
- ✓ UI masking for SAP
- ✓ UI logging for SAP
- ✓ SAP Code Vulnerability Analyzer
- ✓ SAP Fortify by Micro Focus



International Trade Management

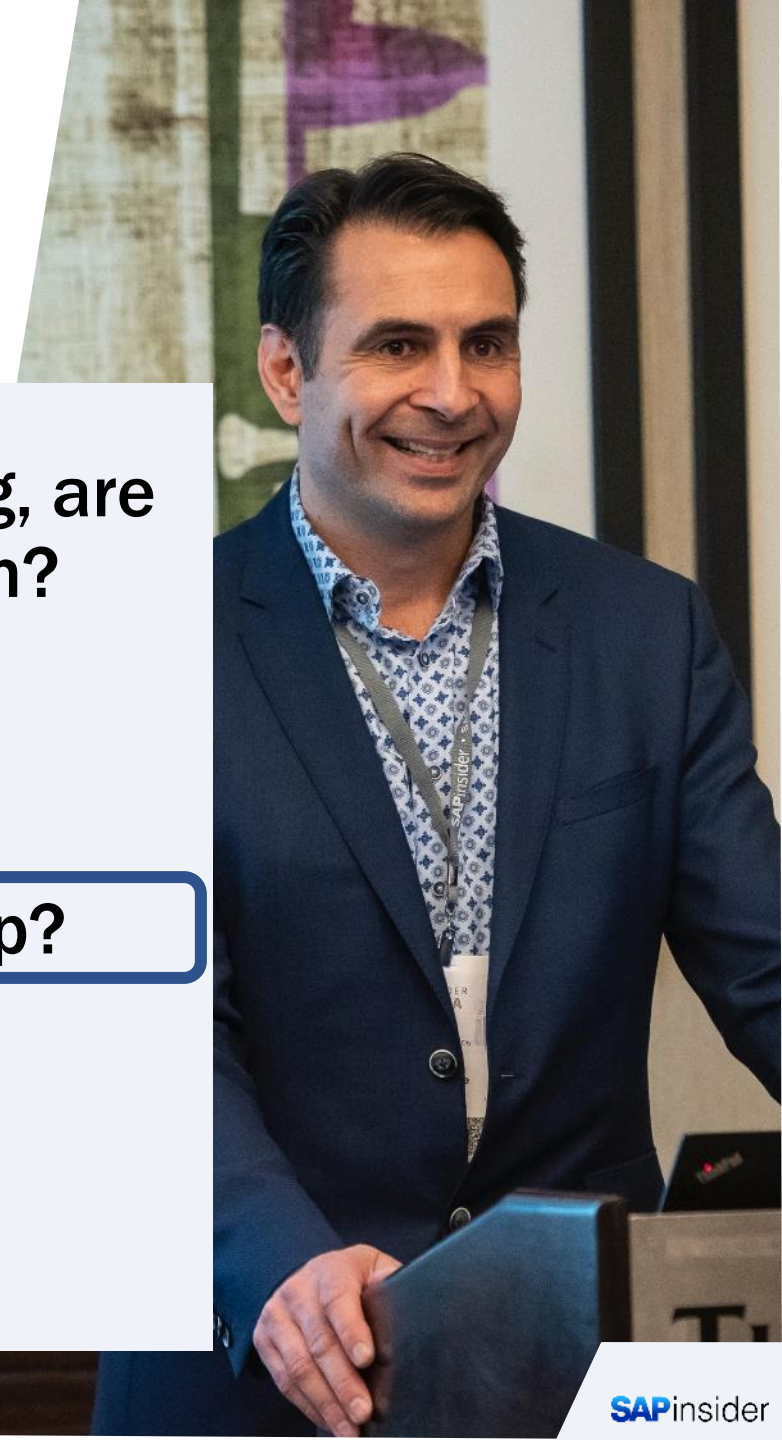
- ✓ SAP Global Trade Services
- ✓ SAP S/4HANA for international trade
- ✓ SAP Watch List Screening

Which Applications do you need today?
Which ones will you be needing 5 years from now?



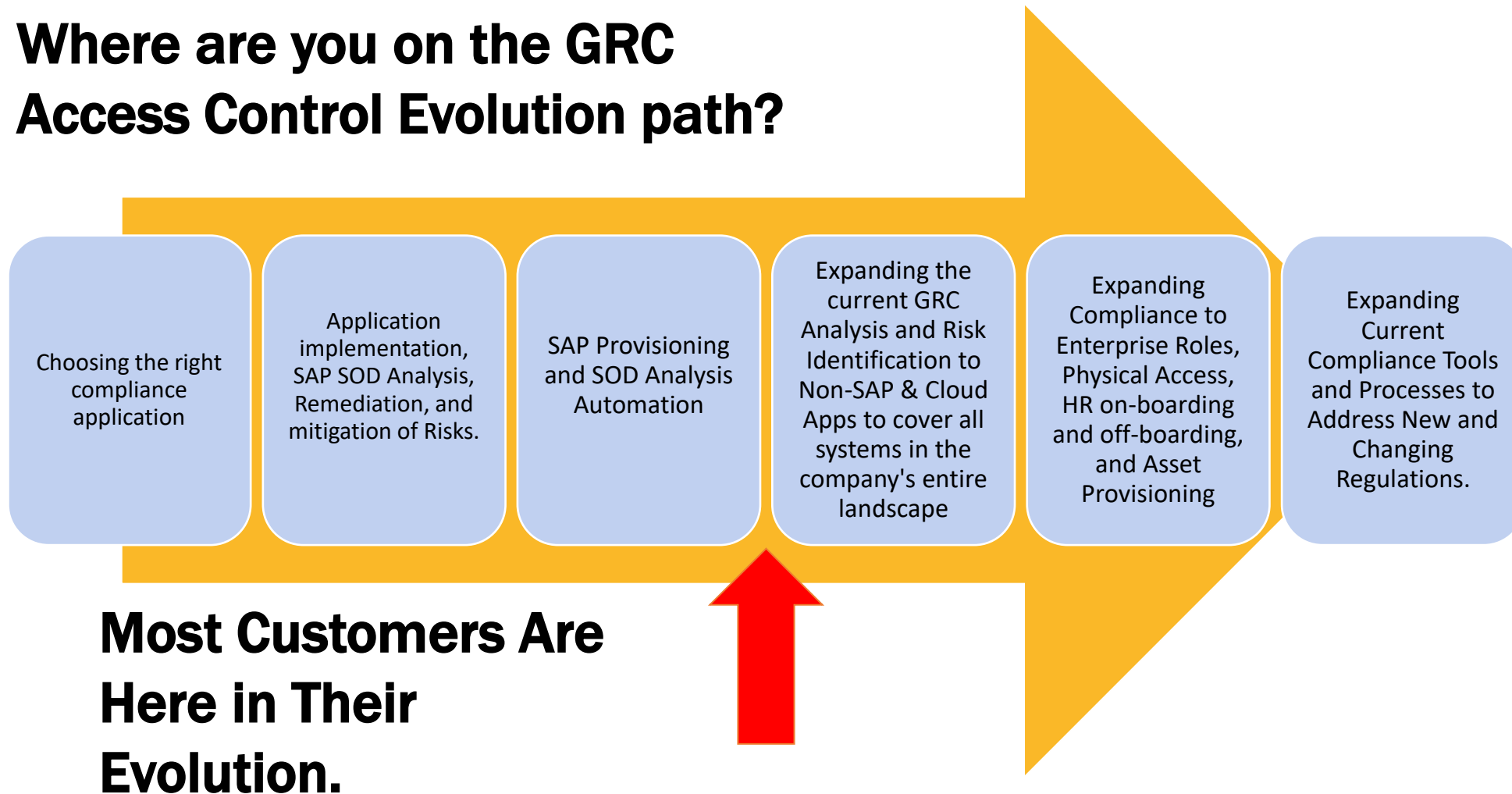
What We'll Cover

- GRC Evolution – Times are changing, are you keeping up? Do you have a plan?
- Two different types of Evolution:
 - #1. Evolution of SAP GRC Technology.
 - #2. Evolution of Customers GRC Requirements.
- Where are you on the GRC Roadmap?
- The GRC Journey – “Think Big, Start Small and Work Smart”
- Wrap Up



The Evolution of a Typical GRC Customer

**Where are you on the GRC
Access Control Evolution path?**



The Evolution of a Typical GRC Customer

Choosing the Right Compliance Application

Things to Consider Today and for Tomorrow:

Identifying the right application to address current requirements

Look for an application you can grow into based on future requirements and scalability for your company

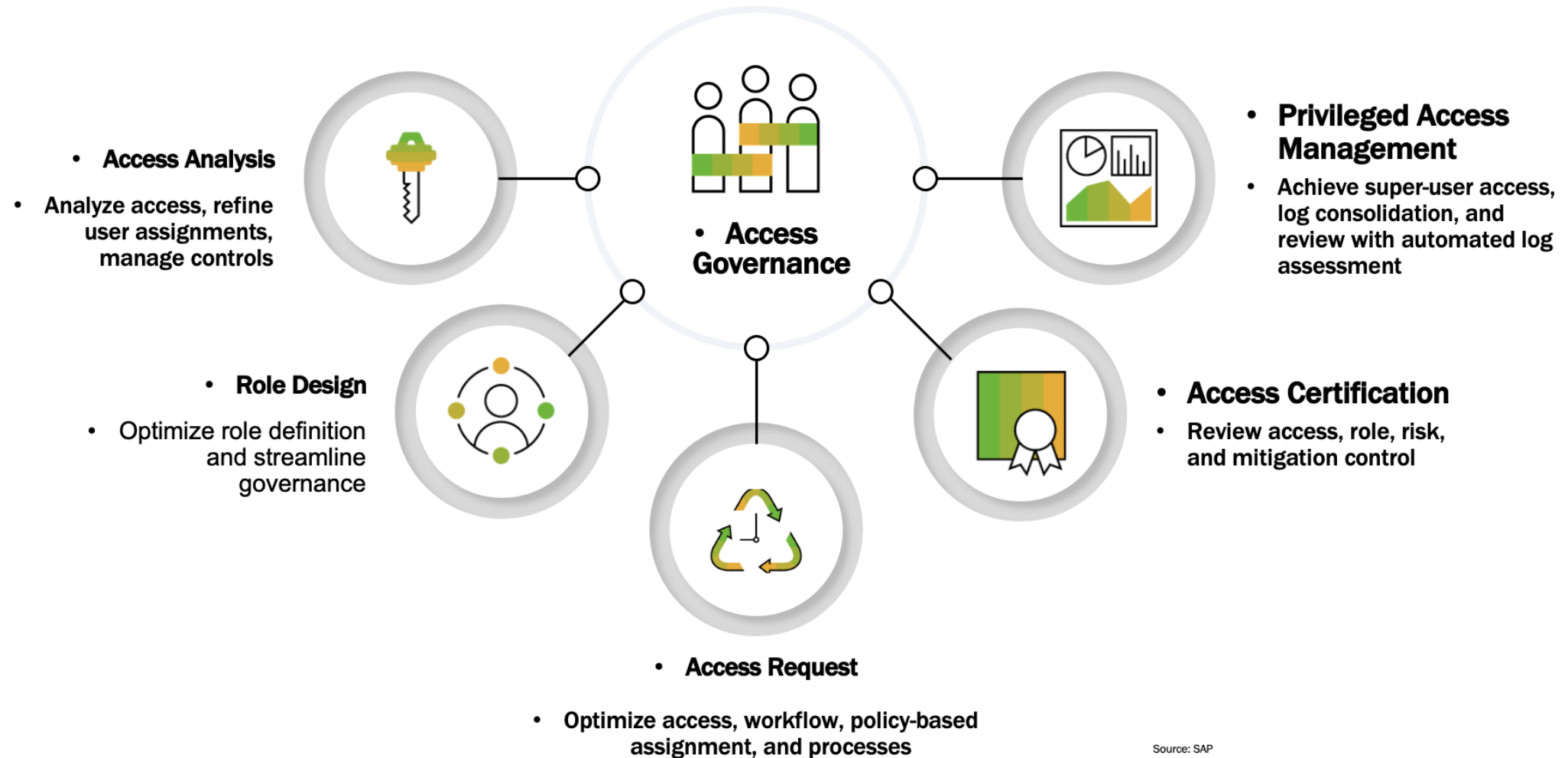
System integration and cross platform capabilities

Implementation effort, cost, and return on investment potential

Picking the right GRC software is critical. It needs to provide functionality to cover your current needs, but also be able to address your compliance requirements as you evolve



Picking the Right Software – Components of Access Governance



Source: SAP

SAP GRC AC 12.0 - Access Risk Analysis (ARA)

I call it the “SoD Engine” part of SAP Access Control.

- Access Risk Analysis is the primary SoD analysis and Reporting engine for the Access Control suite of applications.
- Is the central repository for SoD Rules, Critical Action Rules, and the Mitigating Control Library
- Facilitates the Identification of Segregation of Duty conflicts across all systems connected to GRC.
- Documents Mitigation Control Assignments to Users, Roles, Profiles,
- Provides ALERT functionality to identify when a set of conflicting or critical actions are executed.



SAP GRC AC 12.0 - Emergency Access Management (EAM)

Universally known as good ol' "FireFighter"

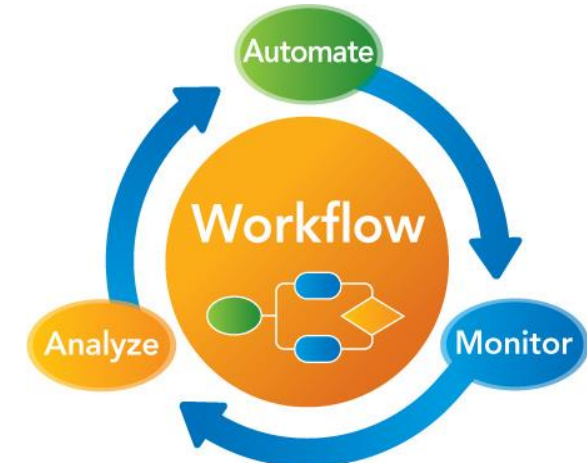
- Emergency Access Management is an application to allow users to gain additional SAP security access to perform sensitive or critical actions above and beyond their regular system duties.
- It also Logs all user activities performed under a FireFighter ID for review by a third party (Controller)
- FireFighter Log information can be distributed via Workflow for documented approval and audit purposes.



SAP GRC AC 12.0 - Access Request Management (ARM)

I call it the “Automation” part of SAP Access Control

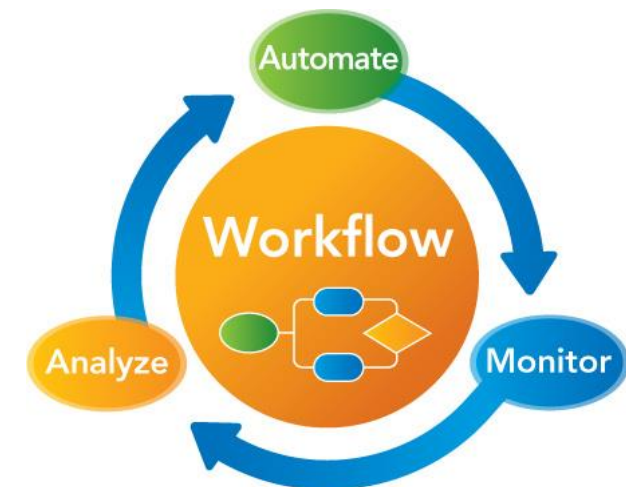
- Access Request Management is an automated user request, approval, and compliant provisioning solution which is workflow configurable with proactive SoD compliance checking.
- Is the main engine for User Access Reviews and SoD Review functionality
- Facilitates Password Self-Service
- Facilitates all Workflow enablement for the other Access Control applications including EAM log Reviews, ARA Mitigation and Rule set Change Control Approvals



SAP GRC AC 12.0 - Business Role Management (BRM)

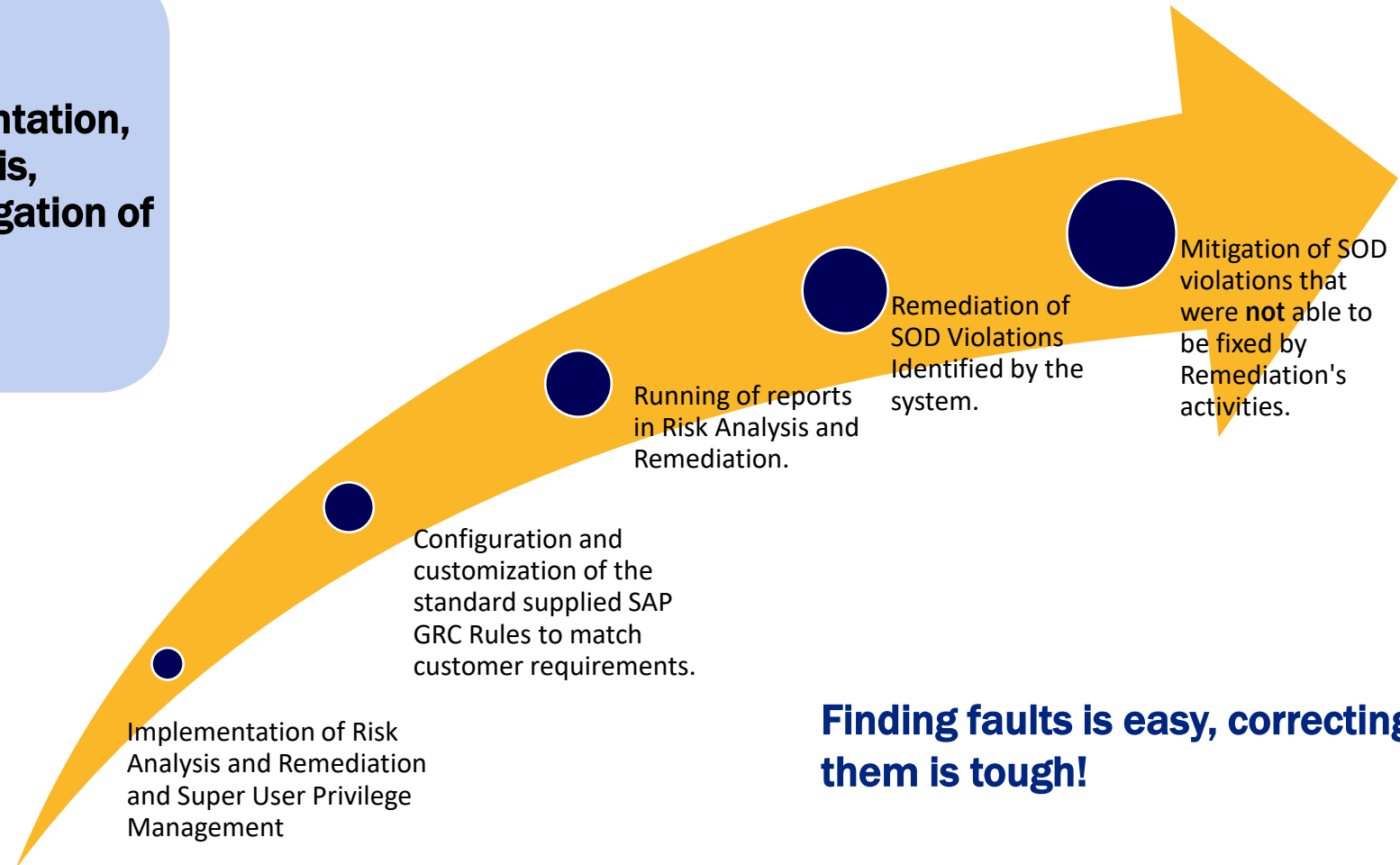
Workflow Enabled Role Maintenance

- Business Role Management allows customers to workflow enable the Role Creation and Maintenance process to enforce consistency and standards compliance.
- Is the central repository from all Role information for the entire Access Control application.
- Facilitates users to associate additional documentation and information to roles that cannot be stored in PFCG.
- Is NOT a replacement for PFCG, rather BRM incorporates the standard Role building t-code into the entire Role definition, approval, and maintenance process.



The Evolution of a Typical GRC Customer

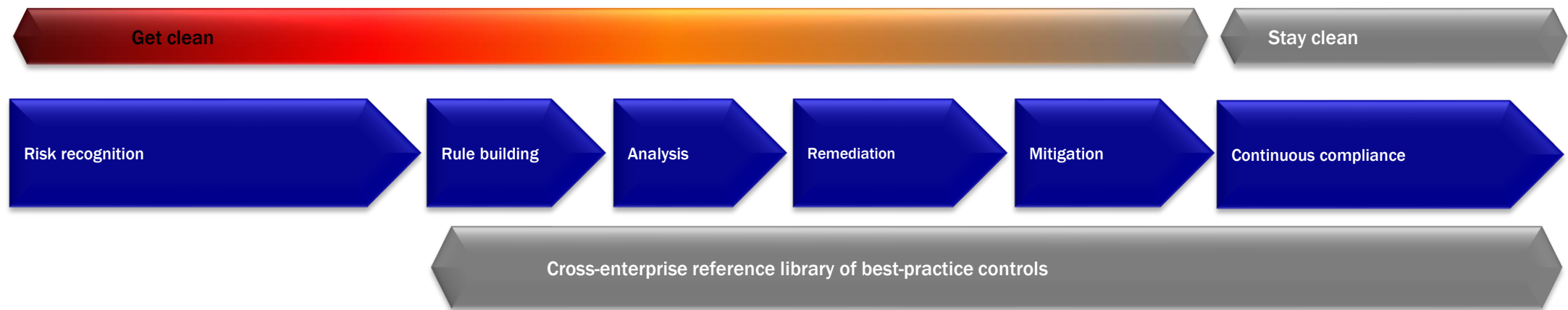
**Application Implementation,
SAP SOD Analysis,
Remediation, and Mitigation of
Risks.**



Finding faults is easy, correcting them is tough!

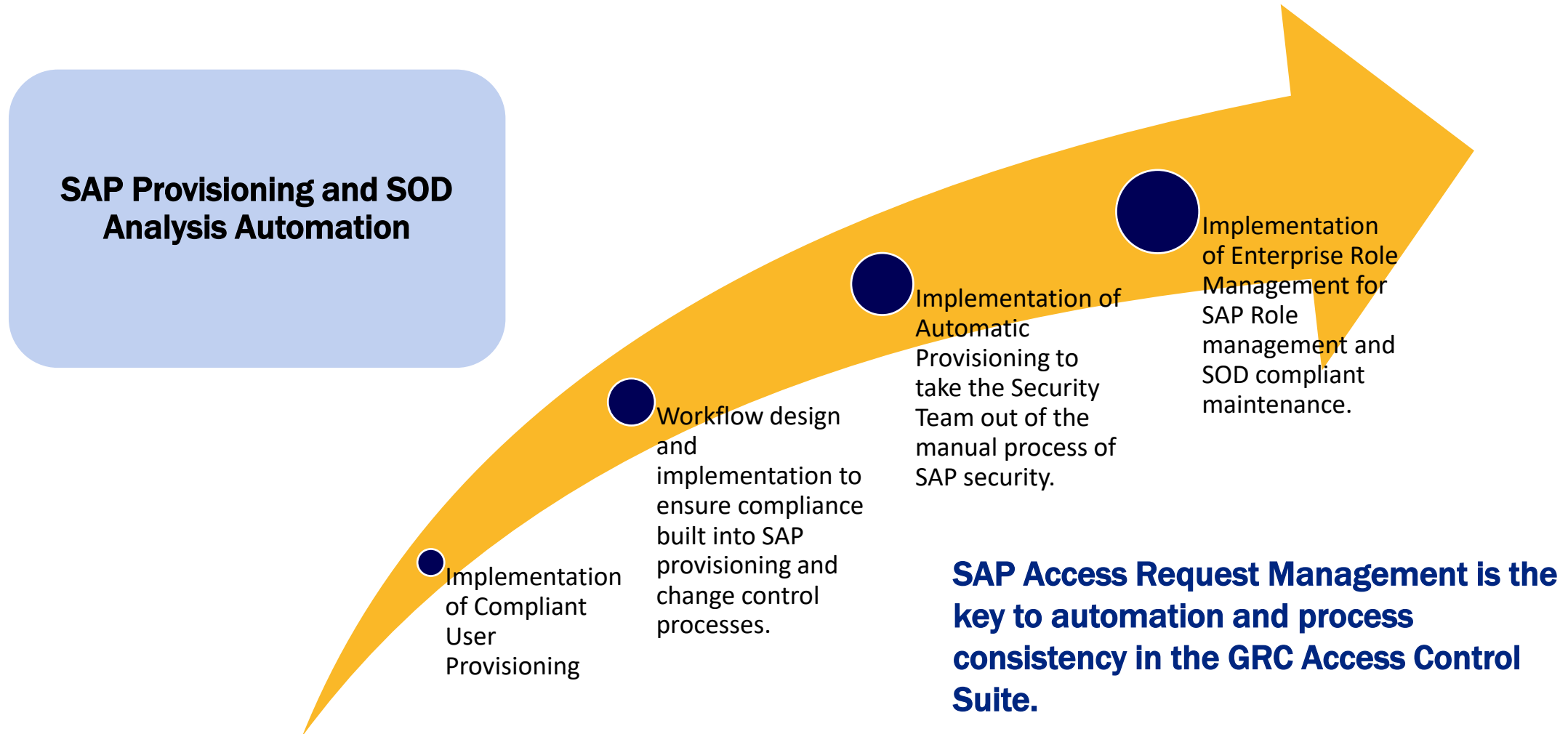


Remediation- The Road Map Shouldn't Stop There!



- The blocks do not represent the effort involved!
 - Remediation takes a lot of effort, first quick wins, but then....
 - Authorization role assignment structuring
 - Organizational change management
 - Mitigation is often 'manual' and 'stand-alone' at first
 - Can be integrated with existing control frameworks
- When reaching "Continuous compliance"
 - Integrate with automated user provisioning to have an efficient and effective process

The Evolution of a Typical GRC Customer



The Evolution of a Typical GRC Customer

Expanding the current GRC Analysis and Risk Identification to Non-SAP & Cloud Apps to cover all systems in your company's entire landscape

● Leverage Built in SAP functionality for Non-Real Time connections to Legacy systems

● Leverage the Non-SAP connectivity provided by SAP GRC, SAP Cloud IAG and Pathlock

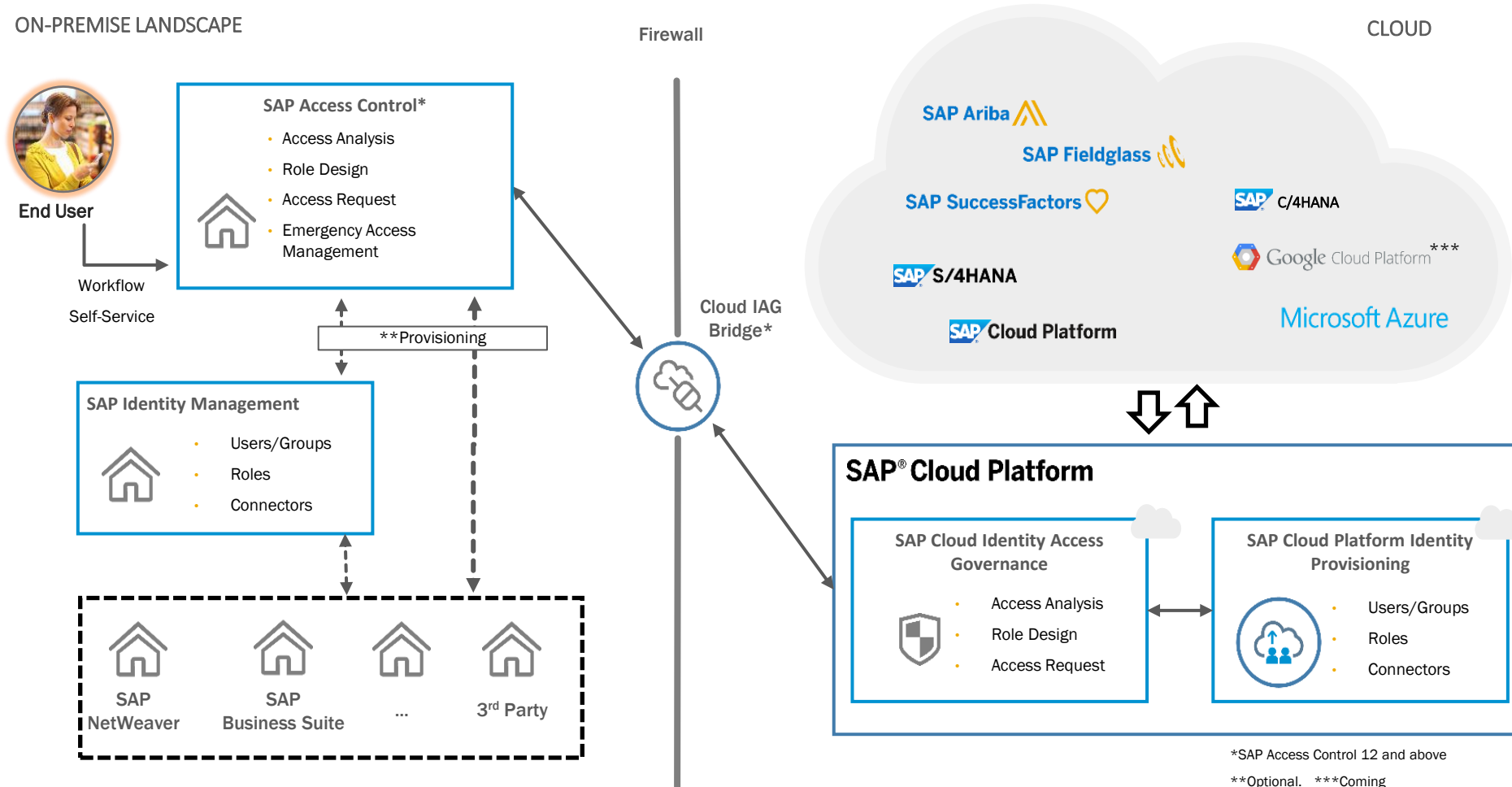
● Identification and Building of Cross System and Cross Platform Rules in Risk Analysis and Remediation

● Leverage additional provisioning functionality by implementing IDM for provisioning to all System platforms and integrating SAP GRC for SoD Analysis where supported

Compliance and SOD analysis is not only for SAP. True compliance means risk analysis for your entire customer landscape.

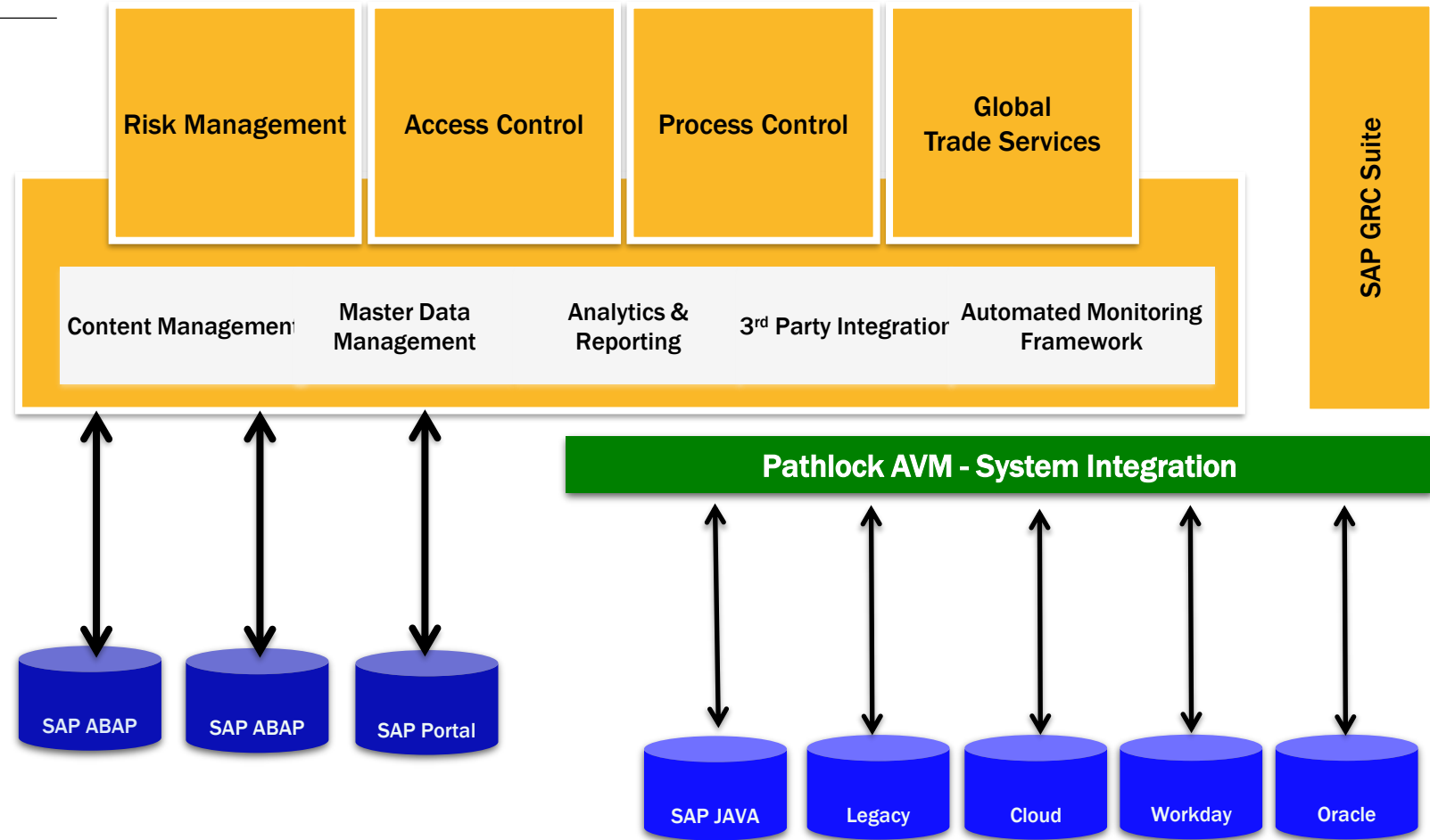


SAP Cloud Identity Access Governance Connectivity



SAP Access Violation Management by Pathlock – System Integration Edition

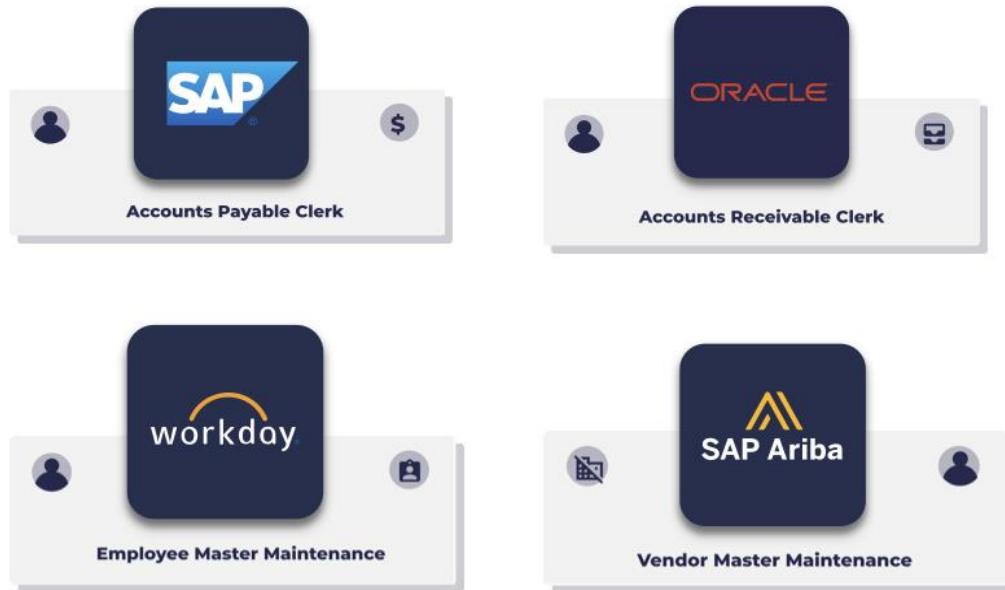
- Extend the capabilities of SAP Access Control across additional business applications and IT systems, eliminating administrative silos and enabling a more complete picture of user access across the organization.
- SAP Access Violation Management enables real-time risk analysis and provisioning, user access reviews, role management, and emergency access management to on-premise and cloud-based enterprise applications.



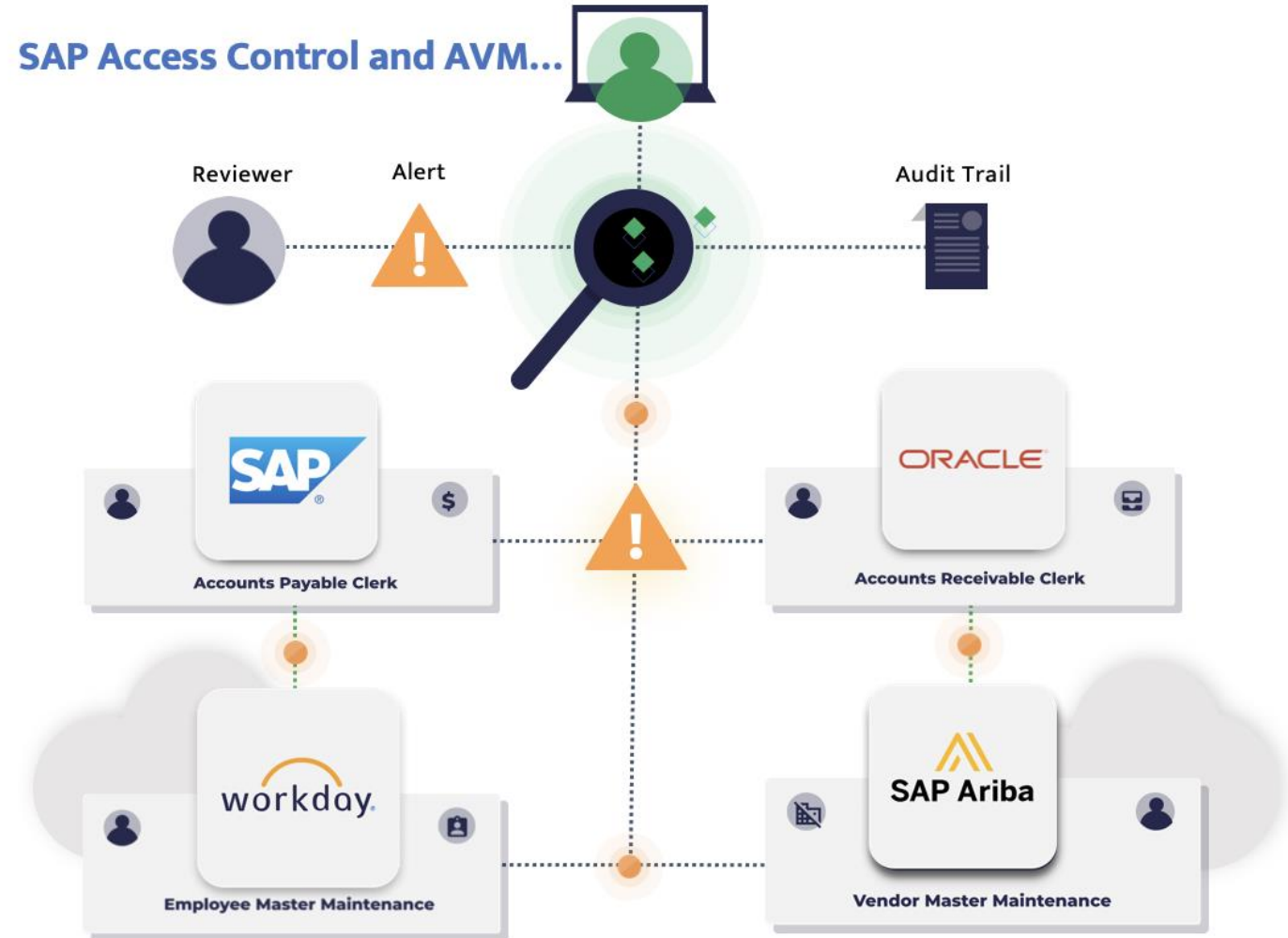
Cross System Risk Identification – Pathlock SAP GRC Integration

Current ...

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



Source: Pathlock



The Evolution of a Typical GRC Customer

Expanding Compliance to Enterprise Roles, Physical Access, HR on-boarding and off-boarding, and Asset Provisioning

Integration and automation with the HR on-boarding and off-boarding process for automated Provisioning and Deprovisioning

Identifying risks based on the combination of physical access levels and employee logical system access levels.

Centralizing provisioning functions for all logical systems, physical access, and asset provisioning.

Capability to run reporting, alert generation, and risk analysis for Asset Loss, combined Logical and physical access fraud.

Automation is the key! Integrating actions that occur in HR processes to correspond with access changes is the Holy Grail to reducing Security Efforts, reducing risk and staying Compliant



The Evolution of a Typical GRC Customer

Expanding Current Compliance Tools and Processes to Address New and Changing Regulations.

Compliance becomes inherent and relatively transparent to the end-user population

Changing regulations that are mainly focused on industry specific requirement for fraud protection, national security, economic protection, and environmental health and Safety standards

Rule set modifications, compliance system configuration changes will be made to stay in compliance with new regulations.

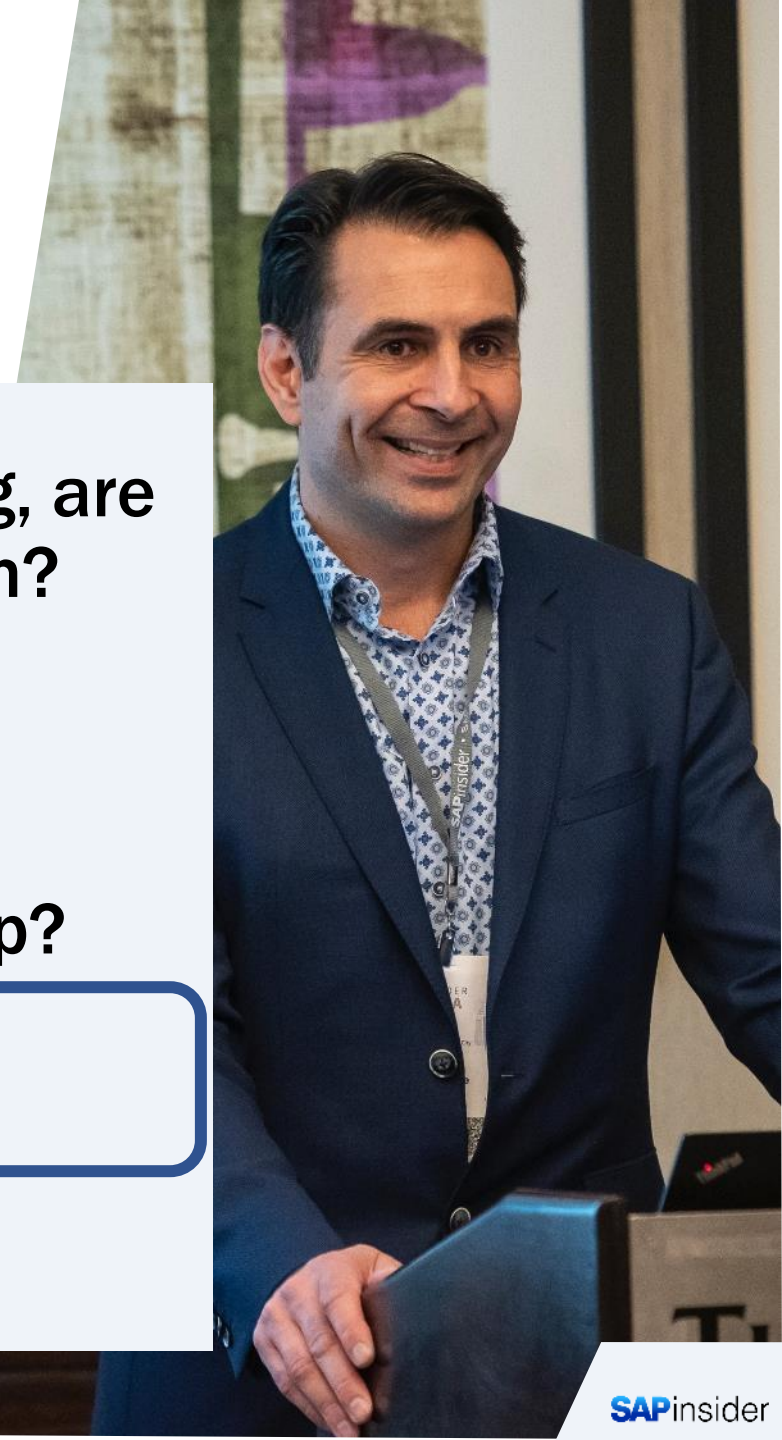
Continued efforts for compliance transparency and automation for all new corporate processes and corporate infrastructure.

Compliance standards are ever changing, you are never done with the evolution. But compliance application functionality and transparency will also improve.



What We'll Cover

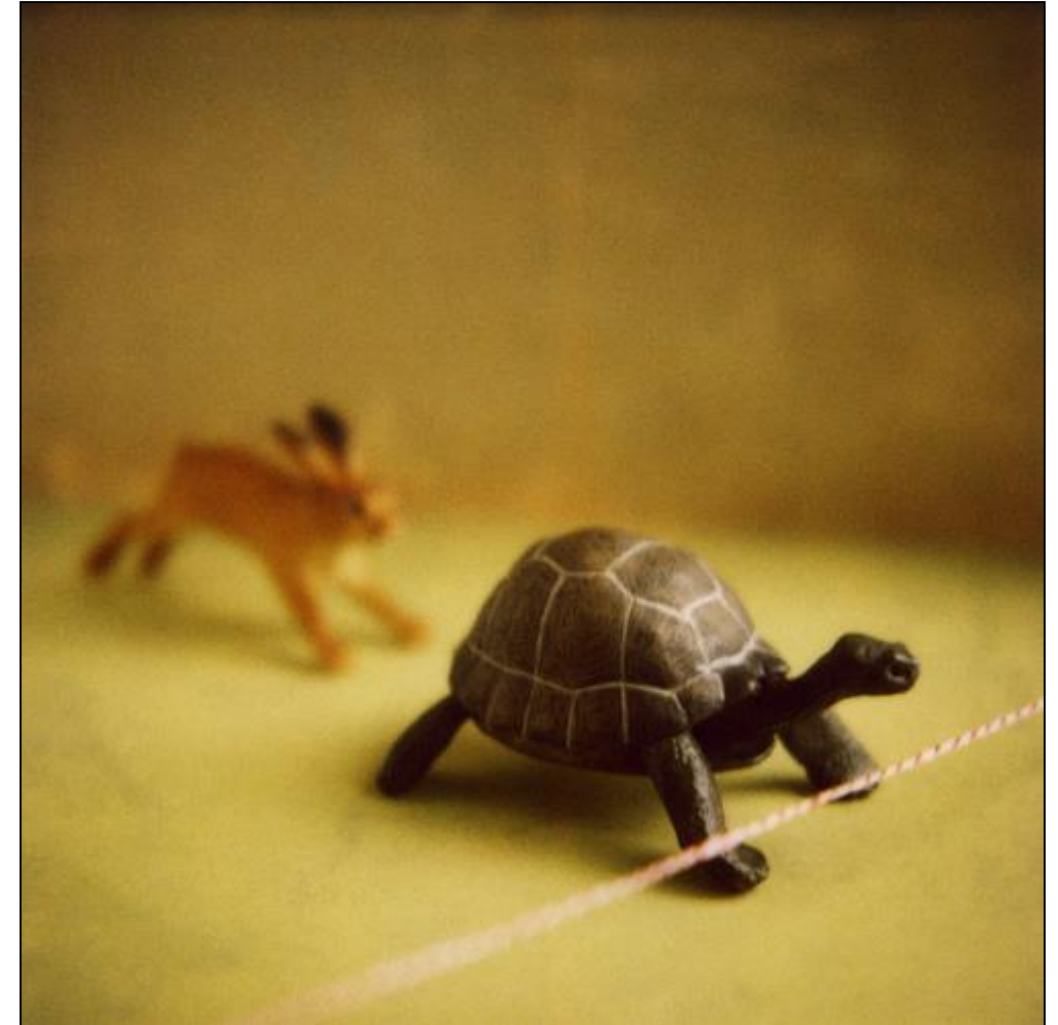
- **GRC Evolution – Times are changing, are you keeping up? Do you have a plan?**
- **Two different types of Evolution:**
 - #1. Evolution of SAP GRC Technology.
 - #2. Evolution of Customers GRC Requirements.
- **Where are you on the GRC Roadmap?**
- **The GRC Journey – “Think Big, Start Small and Work Smart”**
- **Wrap Up**



GRC Journey – Fast or Slow?

“I want to do it all at once, I bought the whole GRC Suite of Software!”

- Cutting edge does not always mean better compliance.
- Customers need to evolve at a rate that allows them to incorporate functionality and establish GRC processes that aligns with their ability to manage change.



Real Customer Quote:

“We Finished Remediation and have FireFighter running – That took a lot of work and time – I’m exhausted and need to do my “Real Job” again. We Need a Break From GRC!”



This is unfortunately where some customer GRC projects and compliance road maps stop. But they don’t understand that they can gain some real tangible ROI from the GRC software by continuing to evolve and to start using the Automation and Integration functionality of Access Control ARM and BRM.

Questions I Like to Ask Customers:

- Are you using:
 - Cross System Or Cross Platform SoD Analysis?
 - Access Request Management?
 - Business Role Management?
 - Access Alerts?
 - Password Self Service?
 - User Access Reviews?
 - Workflow enable change control for Mitigations and Rule Set changes?
 - The Business Role Concept Role Design?
 - IDM integration with GRC?
 - The IAG Cloud Bridge?
 - The Pathlock AVM Integration?

Why Not?




Role Management

Manage business and application roles

Quick Links

- [Role Maintenance](#)
- [Role Search](#)
- [Default Roles](#)
- [Role Reaffirm](#)




Compliance Certification Reviews

Perform user access, risk violation and role assignment reviews

Quick Links

- [Manage Coordinators](#)
- [Request Review](#)
- [Manage Rejections](#)



Access Alerts

Find, display, and clear conflicting and critical access alerts and alerts for mitigating controls

Quick Links

- [Conflicting and Critical Access Alerts](#)
- [Mitigating Controls](#)

Drive It Like You Own It!

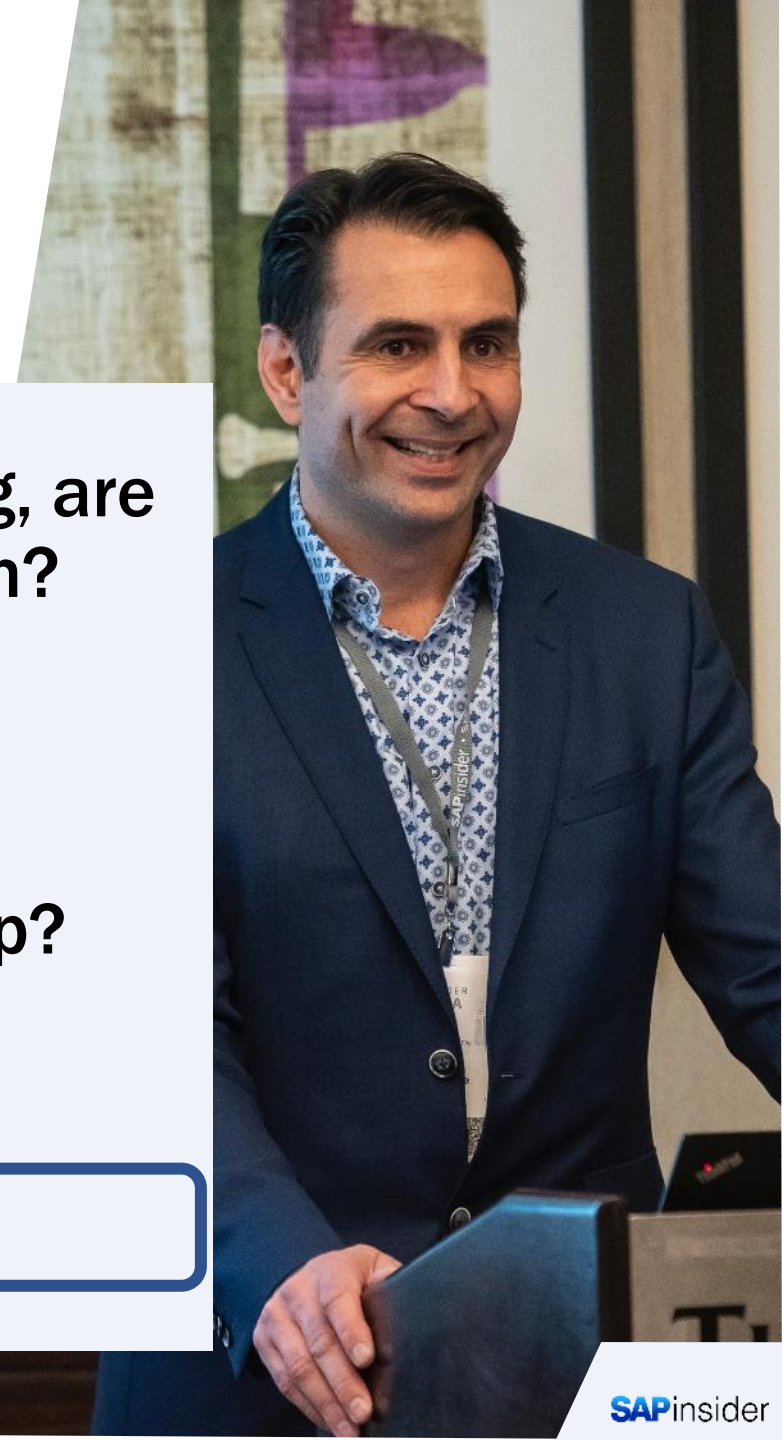
- SAP GRC contains a very robust and powerful set of applications that can address so many different compliance and security related issues ... but many customers are not getting the full ROI if they are only using a fraction of the functionality and not leveraging the full opportunities of integration within GRC

It's like owning a powerful sports car, but only being able to drive it 30 miles per hour and just on Sundays!



What We'll Cover

- **GRC Evolution – Times are changing, are you keeping up? Do you have a plan?**
- **Two different types of Evolution:**
 - #1. Evolution of SAP GRC Technology.
 - #2. Evolution of Customers GRC Requirements.
- **Where are you on the GRC Roadmap?**
- **The GRC Journey – “Think Big, Start Small and Work Smart”**
- **Wrap-up.**



Where to Find More Information

- SAP Access Control Product Availability Matrix
 - <https://support.sap.com/release-upgrade-maintenance/pam.html>
- Bridge: Access Control 12.0 with SAP Cloud Identity Access Governance Integration Guide
 - https://help.sap.com/doc/4835e84042834e6c96bfa35f5d7609aa/1902/en-US/AC12%20to%20IAG%20Bridge_Integration.pdf
- SAP GRC AC 12.0 Admin Guide:
 - <https://help.sap.com/doc/a877d9f274d3471c9ef107e7b9fa1eef/12.0.03/en-US/loio9e08a4211c104a9696cdffccdc9bb3c8.pdf>
- SAP Access Violation Management by Pathlock
 - <https://www.sap.com/products/access-violation-management.html>

Key Points to Take Home

- Defining your GRC Road map will be driven by two forms of Evolution: Evolution of SAP GRC Technology and Evolution of Customers GRC Requirements.
- Evolution does not need to be quick and drastic! Sometimes the smallest enhancement can make the largest impact in improving your current compliance environment! The key is to continue to move forward, as compliance requirements and audit standards will not stop and wait for you.
- Some stages in the GRC Roadmap will take longer to complete or turn out to be more challenging than others. The key is to have a clearly documented roadmap with tangible goals based on realistic success factors.
- Strive to prevent your GRC roadmap deviating off course by situations of inconsistent process ownership, internal staff turnover, and conflicting senior management compliance priorities.
- Don't become overwhelmed with the multi-dimensions of GRC. Focus on the smaller pieces and setting tangible goals to be accomplished at a rate that makes sense for your company.
- Leveraging a knowledgeable Consulting "Senior Advisor" with practical long-term experience to assist in defining your GRC Roadmap and to provide practical immediate ROI justified solutions will save time and prevent costly mistakes.



Please remember to complete
your session evaluation.

- **LinkedIn:** <http://www.linkedin.com/in/jamesroeske/>
 - **Twitter:** <http://twitter.com/Roeskinator>

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 750,000 global members.
