



Getting the most from your auditors

Natalie Freedline, Partner
EY

SAPinsider
Las Vegas

2023

SAPinsider

Disclaimer

- The views of third parties set out in this webcast are not necessarily the views of the EY organization or any of its member firms. Moreover, they should be seen in the context of the time they were made.
- This material has been prepared for general informational and educational purposes only and is not intended, and should not be relied upon, as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.
- Neither the EY organization nor any of its member firm thereof shall bear any responsibility whatsoever for the content, accuracy, or security of any third-party websites that are either linked (by way of hyperlink or otherwise) or referred to in this presentation.



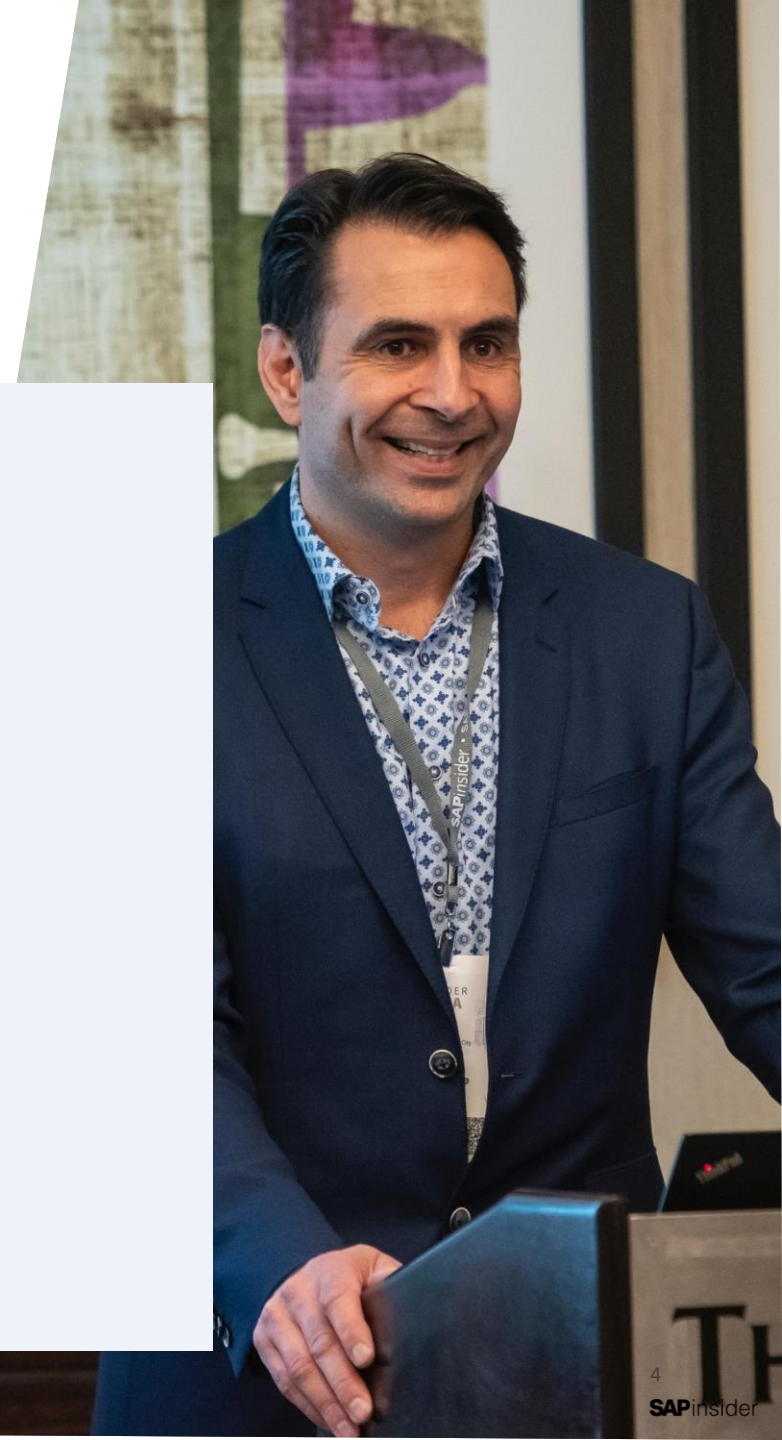
In this session

Is your organization implementing SAP GRC with the primary goal of streamlining your end-to-end Sarbanes-Oxley (SOX) Act function and increasing auditor reliance?

This session will provide guidance on which processes to enable within the tool, the optimal timeline and approach, and key tips and tricks to consider throughout your journey.

What we'll cover

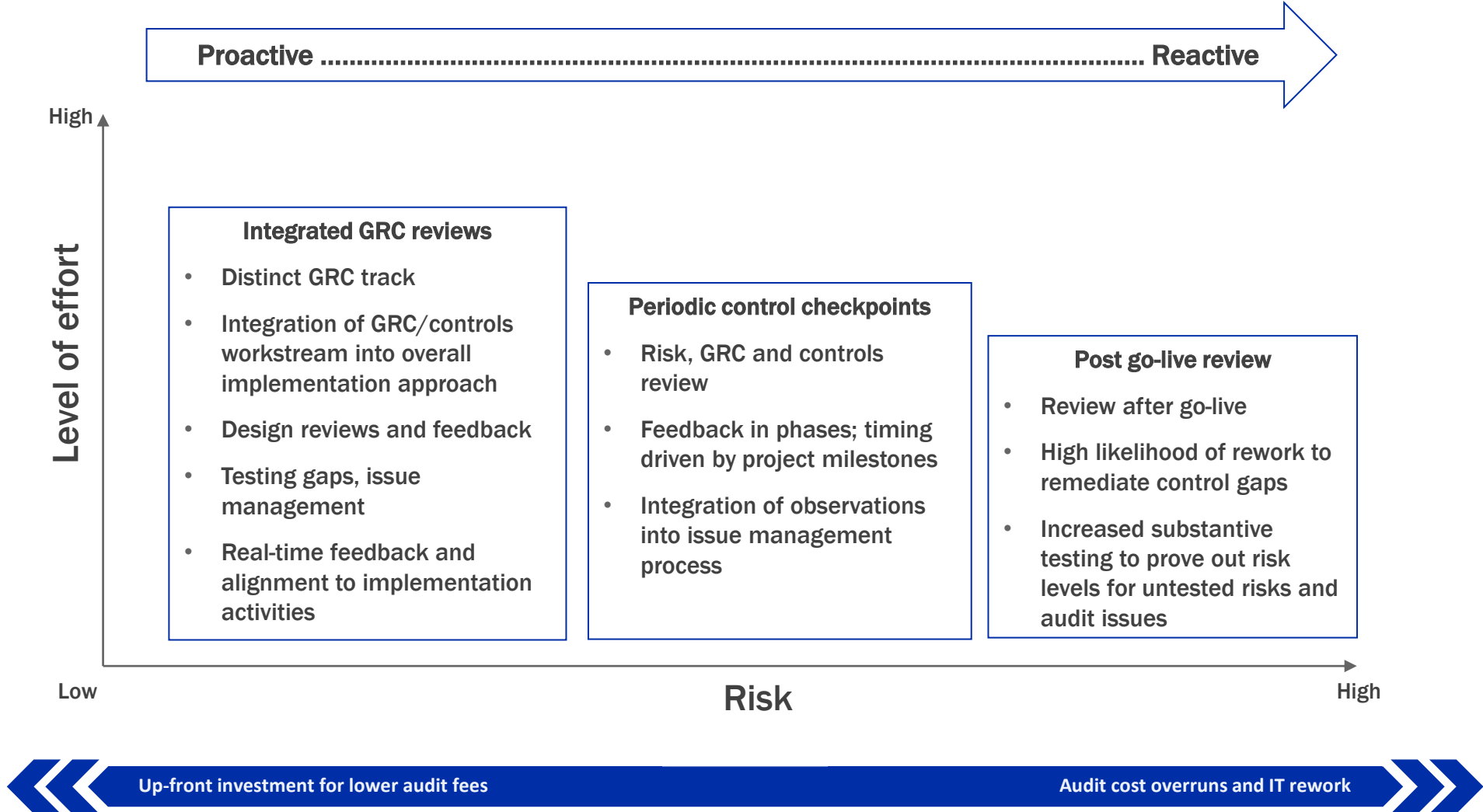
- How much risk are you willing to accept?
- What are the potential audit integration strategies?
- Which GRC processes support compliance?



How much risk are you willing to accept?



Audit integration approaches



Inherent implementation risks

- Audit risk:
 - Limited amount of time to remediate major gaps identified post go-live
 - Potential for significant deficiencies and/or material weaknesses in ICFR opinion
 - Criticality of a controlled hyper-care period as the application is stabilized post go-live
 - Audit effort to test new control environment as of go-live date under the application – including new control requirements and potential manual workarounds
- Operational risk:
 - Hyper-care support period during busiest time of year, where issues remaining at go-live could result in disruptions to supply chain, challenges with billing customers, etc.
 - Q4 employee holiday vacations
 - Prioritization challenges when everything is urgent



Pre-implementation assessments enable external audit integration into the project to proactively elevate and effectively mitigate risks prior to go-live.

Suggested audit touchpoints

In a typical SAP GRC implementation, each phase should have an audit touchpoint (with both internal and external audit), so the auditors are included continuously throughout the implementation.

When looking for reliance, make sure that you document each process enough so that it supports audit requirements.

Phase	Example touchpoint/review discussion points
Project Preparation	<ul style="list-style-type: none">• Project kick-off and general implementation strategy overview, project milestones• Review scoping considerations prior to developing your approach and timeline• Expectations from each group, including audit reliance• Confirm touchpoints and meeting points
Design	<ul style="list-style-type: none">• Review SAP GRC design documentation, including future state processes/workflows and GRC Security Model• Communication design gaps and priority levels• Confirm testing strategy and training strategy• Begin GRC governance discussions
Realization/Testing	<ul style="list-style-type: none">• Build and test results• High-risk issues• Traceability Matrix• Confirm cutover strategy
Cutover/Go-Live	<ul style="list-style-type: none">• Cutover sampling documentation and issue management for resolution of project issues• Final Audit Reliance Approach• Completeness and accuracy/data migration• Final pre-implementation ITGC/SDLC procedures• Final GRC Governance Plan

Watch out: You should not have to spend time training your auditors to view/navigate the SAP GRC system

Pre-implementation review activities

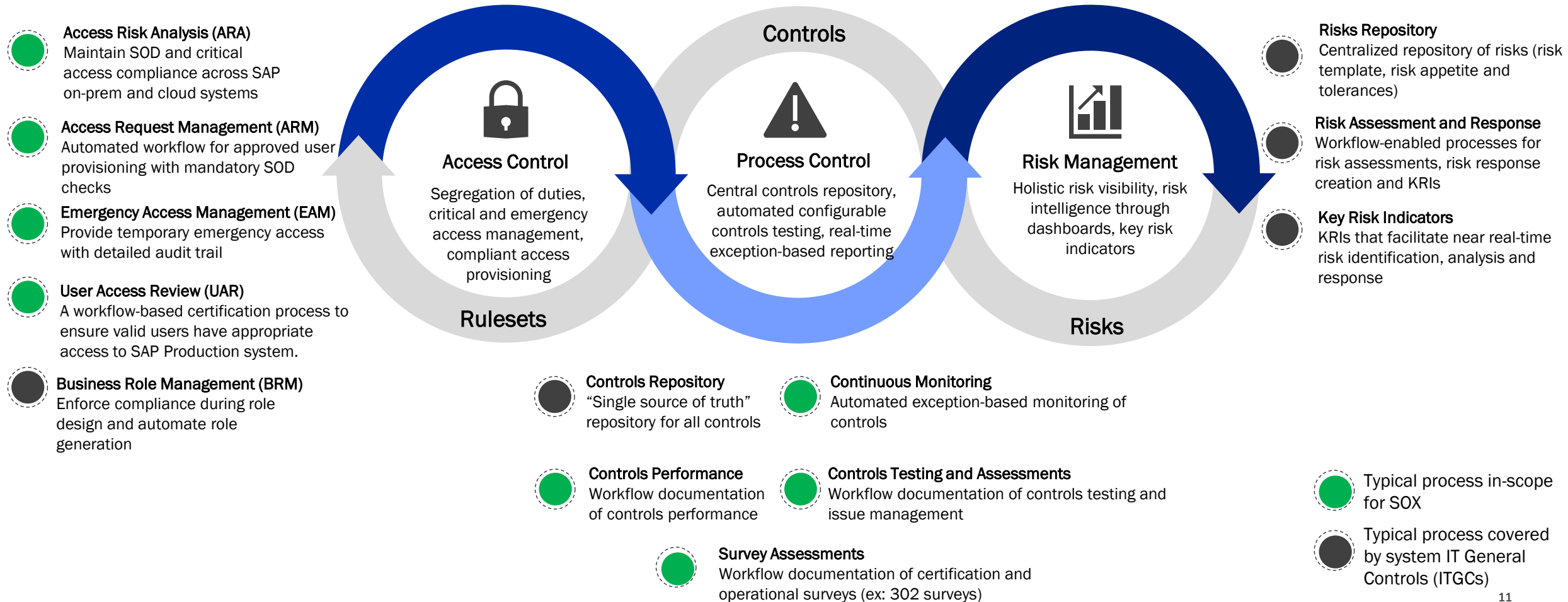
Audit Area	Key Review Activities	Leverage for Audit?	Considerations
SAP GRC Access Control/ Identity Access Governance (IAG)	Ruleset review/gaps at the tcode and permission level	Yes	<ul style="list-style-type: none"> Ruleset reviewed pre-imp can be baselined for post-imp High risk area will require independent testing; ability to assess privileged SAP access
	Review SOD mitigation strategy and mapping for control coverage	Yes	<ul style="list-style-type: none"> SOD mitigating control mapping can be leveraged for the post-imp audit SODs in production will require review, and any deviations
SAP GRC Process Control / Financial Compliance Management (FCM)	Business rule review	Yes	<ul style="list-style-type: none"> Business rule/CDS view design review to confirm control coverage pre-imp is a baseline for post imp High risk area will require independent testing; ability to assess privileged SAP access
Interfaces and Reports	Assessment/gaps on interface population, testing	Yes	<ul style="list-style-type: none"> Assess interface controls and manual reconciliations to understand controls over data feeds
	ITDM key control custom report validation for completeness and accuracy	Yes	<ul style="list-style-type: none"> Assess for completeness/accuracy pre-imp to allow for accurate initial reviews post-imp and address reliability concerns
System Development Lifecycle/ Implementation integrity	Review program documentation related to the protocols and sign-offs for all phases and evaluate the SDLC controls (i.e., requirements gathering, testing, cutover)	Yes	<ul style="list-style-type: none"> Independent perspective related to go-live readiness Assess project management approach and documentation
	Assess hypercare plan and review open issues to the extent that it will affect the future state RACM, interim controls	Yes	<ul style="list-style-type: none"> Detect open issues prior to go-live, allowing time for correction Evaluate interim controls (if necessary) for coverage on open issues

SAP Governance, Risk, and Compliance (GRC) overview



SAP GRC overview

SAP GRC is designed to seamlessly integrate with S/4 HANA and other SAP cloud platforms and provides automation capabilities and analytics to optimize access management and controls.



What's new in GRC?

Financial Compliance Management (FCM) SaaS subscription framework on BTP

- Global controls repository, control performance and testing
- Issue and remediation monitoring
- Uses CDS views for continuous monitoring
- Data Service is used to connect BTP to target backend system
- Embedded content and GRC content hub
- Integrates with Signavio

Identity Access Governance (IAG) An extension to existing SAP GRC solutions (extends capabilities to cloud systems)

- Options to connect to both on-premise and cloud applications
- Out of the box workflows for access risk analysis, access provisioning, certification, etc.

Architecting GRC technology solutions

SAP applications

SAP Solutions/Software		SOX Applicability	GRC Technology Enablement	FCM
S/4 HANA, CFIN	Core Finance and Accounting	Yes	SAP GRC	✓
S/4 HANA Public Cloud	Core Finance and Accounting	Yes	SAP GRC	✓
Ariba	Procurement	Yes	IAG/Bridge	
Logistics Business Network (LBN)/Extended Warehouse Management (EWM)/Transportation Management (TM)	Supply Chain	Yes	SAP GRC	✓
SuccessFactors	HR and Payroll	No	IAG/Bridge	
Integrated Business Planning (IBP)	Supply Chain	Maybe	IAG/Bridge	
SAP Billing and Revenue Innovation Management (BRIM)	Revenue	Yes	SAP GRC	
Global Trade Services (GTS)	International trade	Yes	SAP GRC	
SAP Concur	Expenses	No	IAG/Bridge	
SAP Fieldglass	Contracts	No	IAG/Bridge	

SAP GRC Process Control (PC) walkthrough



SAP GRC PC support for key compliance processes

Global controls library

- Single-source-of-truth repository for all controls (across multiple mandates)
- A centralized repository for business process controls and IT general controls (including mitigating controls – integration with SAP GRC Access Control)

Manual Control Performance and Testing

- Workflow-based documentation of controls performance/ testing by control owners/testers
- Drives greater insight, visibility, effectiveness and accountability, issues tracking and remediation

Assessments and surveys

- Workflow-based documentation of assessments
- Integration with Interactive Adobe offline forms
- Multiple types of surveys

Continuous monitoring

- Automated workflow to monitor for exceptions or trends within the SAP systems
- Enhance testing of SAP config controls or optimize delivery of key reports

Benefits and audit efficiencies – Global controls library

What are the benefits of a Global controls library?

- “Single source of truth” for all controls across multi-compliance frameworks (e.g., SOX, FDA, GxP)
- Enterprise-wide visibility and standardization of the risks and controls framework
- Streamlined governance approach over the assignment of valid mitigating controls to SOD risks
- Flexible and customizable organization and process hierarchies to drive ownership of compliance activities

How can this drive audit efficiencies?

Validation of Risk and Control Matrix (RACM) data

- RACM change requests can be managed with workflow and validated
- Audit log report to summarize control changes
- Mitigating controls report

Storing process documentation:

- Centralized repository for business process controls and IT general controls
- Documentation repository for process flows and control narratives

Benefits and audit efficiencies – Manual control performance and testing

What are the benefits of manual control performance?

- Allows controls owners to perform and document their controls in a central location based on predefined control execution plans
- Proactive notification to controls owners when a control is due to be performed, including reminders and escalation
- Reduces the burden on the business during testing cycles by minimizing the need for sample selection and document requests

What are the benefits of manual test of effectiveness?

- Real-time management visibility to status of manual control testing
- Processes efficiencies in the testing cycle through proactive notification and predefined test plans
- Workflow capability to enable control testers to test and document their control testing results in a central location based on predefined control testing procedures, including reminders and escalation

How can this drive audit efficiencies?

Manual Control Performance

- Improves controls effectiveness through prescriptive control execution plans and sign-offs, including date and time stamps
- Gives real-time management visibility to status of manual control performance

Manual test of effectiveness

- Provides a centralized location for storing and maintaining control test plans and test evidence
- Drives greater insight and accountability for testing, issues tracking and remediation

Manual control performance detailed example

1. Control performers execute controls and attach evidence in SAP PC on a predetermined basis.*
2. Control reviewers (if applicable) will review and approve documentation in SAP PC.
3. Control performance documentation requirements will vary on a case-by-case basis.

Control Type	Document Requirement	Testing Team Reliance
ITDM/Review	<ul style="list-style-type: none">• Evidence of report/supporting documentation reviewed as part of performance, including details of review (e.g., tickmarks, notes, signature and date)• Completeness and Accuracy of source file (if applicable)	<ul style="list-style-type: none">• SAP PC: Generate report to review overall status and sign-off of key SOX controls; download evidence based on sample selection• Outside system: Reach out to Control Owners on questions specific to attached evidence (if applicable)
Event-Driven/ Continuous	<ul style="list-style-type: none">• Evidence of the total population for the designated time frame (e.g., Excel file)• Completeness and Accuracy of population source file (if applicable)	<ul style="list-style-type: none">• SAP PC: Generate report to review overall status and sign-off of SOX controls; select testing sample from populations for the designated testing period• Outside system: Request additional evidence for sample selected from Control Owners

* Depends on the frequency of the control or the frequency of which evidence of the control needs to be captured

Manual test of effectiveness detailed example

1. Control testers will receive a notification from SAP Process Control when testing is due to be performed (e.g., Interim, Roll Forward).
2. Control testers will complete the associated test plan, attach evidence, and submit for review.
 - a) If a control is designated with a “Fail” rating, prior to submission, the control tester must log issues and designate the appropriate control owner as the issue owner.
3. Control test reviewers will review and approve testing documentation, including logged control exceptions, if appropriate.
 - a) If an issue is logged, a separate workflow will be initiated for documenting the issue and remediation process.



Tip

A detailed test plan can be housed directly within the tool and/or a testing template can be attached and automatically delivered with the testing notification.

Standard reports examples – manual test of effectiveness:

- Risk and Control Matrix – Used to determine the key in-scope controls per location and operating frequency
- Control Test History with Ratings – Used to monitor progress of manual control testing; provides a listing of rating by control, status, the user who tested the control and issues associated to the control
- Test step status – Used to review control test plan details for each organization and process, including comments
- Issue status – Provides visibility into issue statuses of each evaluation type

Tying it together

1

Manual Control Performance

Control Name: FSCP.UK.03

Control Description: The Monthly Financial Close Indivior UK Ltd and Indivior EU Limited Checklist is completed by the EMEA Finance Team and reviewed by the EMEA Finance Controller. Items included in the checklist include but are not limited to : Timely and proper submission of all regional

Steps

Control Info

Steps (3)

Step	Description	Evidence Requi...	Comments Req...	Sequence	Status	Last Updated
1	Run the Monthly Financial Close Indivior UK Ltd. Checklist	Yes	No	001	In Process	>
2	Perform a timely and proper submission of all regional entity results	Yes	Yes	002	Pending	>
3	Confirmation by local finance managers that all reconciliations have been performed	Yes	No	003	Pending	>

2

Control Effectiveness Manual Test: PP22_Vendor Payment Data Review

Test Period February 2015 Status Draft Organization North America Process Purchase to Pay (P2P) Subprocess Vendor Master Data Mainte

Submit Save Draft Assign to Next Tester

General Regulation Control Details Account Groups Risks Attachments and Links

Test Steps

Report Issue Download Form Upload Form

Step Description	Step/Test	Required	Fail End...	Sampling Meth...	Revised Sample	# Failed	Result	Comments	Initial Sa...
Inquire with appropriate personnel to understand the review and investigation process for discrepancies between payments recorded in SAP and recorded by the bank. Document your understanding.	Step	Yes	No	Random sample	0	0	▼ Add Comment	0	
Evidence timely reconciliation of SAP vs. bank payments by an appropriate individual.	Step	Yes	No		0	0	▼ Add Comment	0	
If discrepancies were identified, evidence that they were investigated and resolved timely.	Step	No	No		0	0	▼ Add Comment	0	
Validate that the reconciliation was appropriately and timely reviewed and approved.	Test	Yes	No		0	0	▼ Add Comment	0	

Test Details

Test Name: Log for Manual Test of Effectiveness PP22_Vend

Test Owner: ADMIN

Description: A review is performed to ensure that vendor payment data per the accounts payable system is completely and accurately transferred into the bank's payment system for locations utilizing banks to issue

Documents: 0 Attachments

Test Date:

Test Result:

Comments:

3

Control Effectiveness Manual Test: Control Performance Control

Test Period Year 2016 Status Draft Organization Control Performance Organization Process CP Process Subprocess CP Subprocess

Submit Save Draft Assign to Next Tester

General Regulation Control Performance Control Details Account Groups Requirement Risks Attachments and Links

Period	Year	Name	Regulation	Status	Start Date	End Date
Year	2016	Control Performance Test for CP Control	SOX	Done	01/01/2016	12/31/2016
Year	2016	Mtoe For Control Performance Test	SOX	New	01/01/2016	12/31/2016

Performance Steps

Step	Description	Evidence Required	Comments Required	Sequence	Status	Last Changed On	Last Changed By	Comments	Control Evidence
Inventory Check	Check the inventory weekly	Yes	Yes	001	Done	06/09/2016 13:26:29	ADMIN	Tested Successfully.	Link
Pick-Up Control	Record goods pickup	Yes	Yes	002	Done	06/09/2016 13:28:09	ADMIN	Successful.	Link
Delivery Tracking	Track Delivered goods	Yes	Yes	003	Done	06/09/2016 13:37:37	ADMIN	Completed.	Link

Benefits and audit efficiencies – Continuous monitoring

What are the benefits of continuous monitoring?

- Greater efficiencies in control execution, testing and documentation
- Enables greater business accountability for monitoring control exceptions
- Increased risk coverage (period vs. point-in-time) through real-time exception-based reporting

Reliable



Operate 365 days a year!

Consistent



Eliminating variations in processes

Scalable



Ramp up and down to match demand

Audit trail



Fully maintained logs for compliance

How can this drive audit efficiencies?

- Potential increased audit reliance versus manual testing

IT dependent manual control example

1. Eliminates need for controls owner to remember to run SAP reports
2. Electronic signoff – paper trail no longer required
3. Review covers full population of changes not just sampling
4. Focuses on exceptions only i.e., changes to key fields
5. Flexibility to be set up for near real-time (e.g., same day) if needed
6. Audit evidence readily available in the GRC tool for auditors

SAP configuration control example

1. On average, 60-80% efficiency over manual approach
2. Drives greater business accountability for the controls
3. Full coverage for period under review rather than a point-in-time check
4. Further reduces process owner and tester time if controls never change

Typical audit review areas



Tip: Don't forget about completeness and accuracy in your testing procedures

SAP GRC

- All SAP GRC transports will follow the transport path into the production system (SAP GRC DEV > SAP GRC QA > SAP GRC PROD)
- Changes made to the system will follow the IT system change control process
- Supporting documentation, references to associated testing evidence, and approvals will be housed in the agreed upon location as appropriate

SAP S/4 and SAP ECC

- Standard SAP plug-ins required for connection to SAP GRC
- Configuration table change log activations (as needed)
 - Table logging enabled at the server level – REC/CLIENT parameter
 - Table logging enabled via transport – Adding the REC/CLIENT parameter to the STMS transport overview setting
 - Table logging enabled for all tables leveraged in configurable business rules

Illustrative multi-year application controls testing approach

Procedure	FY24	FY25	FY26	FY27	FY28
SAP GRC PC ITGC Walkthroughs	Yes	Yes	Yes	Yes	Yes
SAP GRC PC ITGC Testing	Yes	Yes	Yes	Yes	Yes
SAP App Control Design/Operational Test	Yes	No*	No*	No*	Yes – re-establish benchmark**

* Assumes Change Management is “Effective” and there were no changes to application controls

** Could be 4 or 5 years depending on factors including, but not limited to consistent effectiveness of ITGCs, little to no changes within the configurations, and little to no changes to processes and controls

SAP GRC Access Control (AC) walkthrough



SAP GRC AC support for key compliance processes

Access Risk Analysis

- Ruleset enabled segregation of duties (SOD) and sensitive access (SA) reporting
- Monitoring processes to review and remediate

Access provisioning

- Workflow-based access provisioning with preventative SOD check
- Automated deprovisioning
- Integration with IAM enterprise tools and IT ticketing systems

Emergency access

- Pre-approved, workflow-based elevated access with logs enabled

User access reviews

- Workflow-based documentation of review of user access and privileges
- Integration with IAM enterprise tools

Benefits and audit efficiencies – SOD and SA monitoring

What are the benefits of SOD and SA monitoring?

- Maintain SOD and critical access compliance across SAP and non-SAP systems
- Remediation view for risk analysis reporting and efficient remediation of SOD conflicts
- Ability to mitigate by system and perform mass mitigation
- Technically tie mitigation controls to access risk violations
- Risk/function maintenance workflows
- User level and role level risk analysis available, including Fiori components

Typical audit review areas

- How risk framework has been determined, inputs from business
- How risk priority levels are being treated (i.e., Critical, High, Medium, Low)
- Processes/subprocesses supporting the SOD ruleset
- Custom tcode inclusion
- Completeness and accuracy of the ruleset
- Priority level remediation strategy for role and user level (i.e., Critical, High, Medium role level SODs will be remediated by Security design)
- Validate mitigating controls for risk coverage
- Annual process to review global ruleset



Do not forget to address cross-system Segregation of Duties risks – this could include monitoring cloud-based applications (i.e., IAG – Bridge)

Benefits and audit efficiencies – Access provisioning

What are the benefits of GRC access provisioning?

- Workflow that supports flexible, multi-tiered routing with enhanced audit trail
- Tailoring of routing requirements for simple to highly complex organizations
- Simplified request forms improve user adoption and usability
- Template-based and position-based access requests
- Integration with IT service ticket and IAM tools for enterprise provisioning

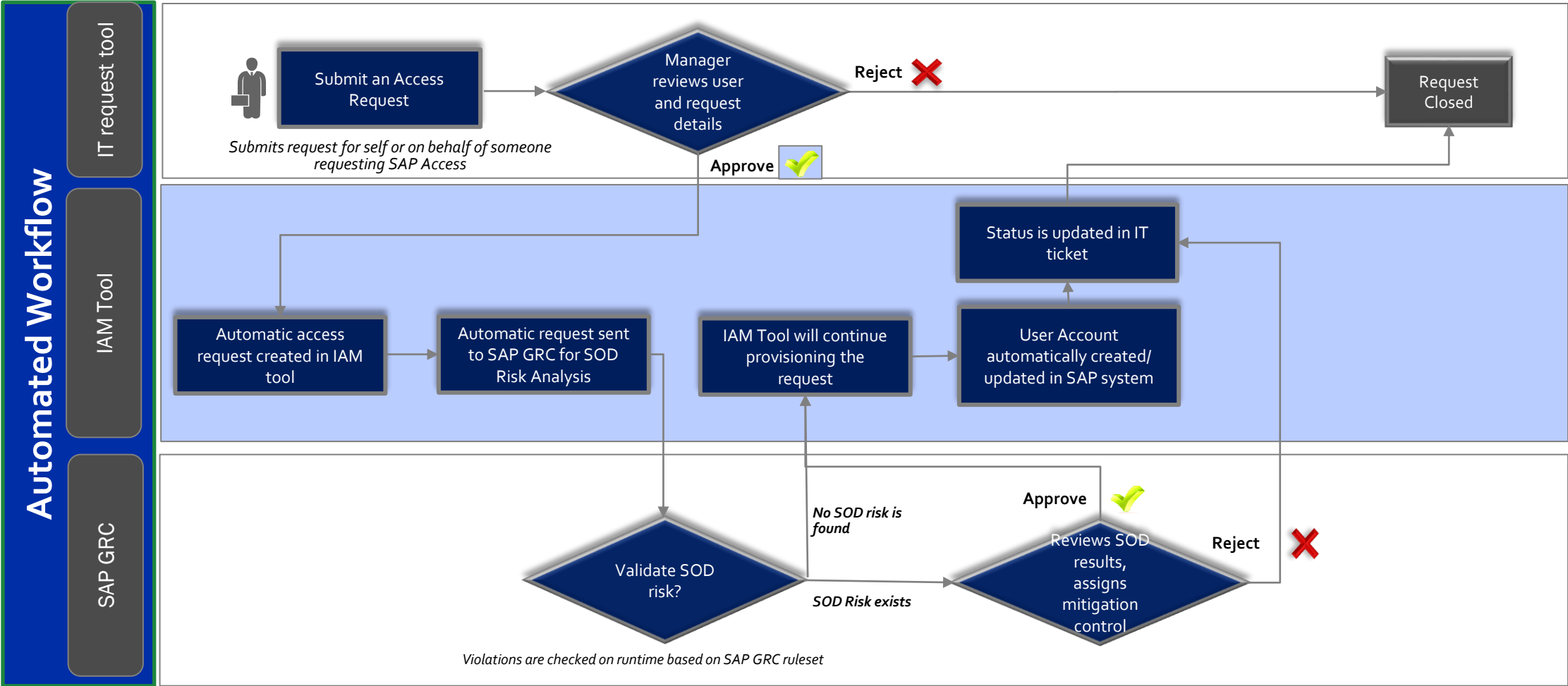
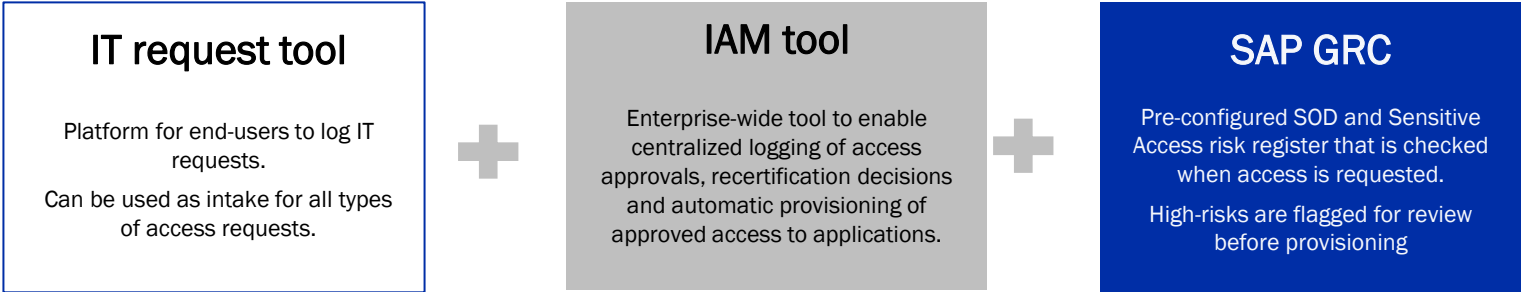
Typical audit review areas

- Process design and in-scope systems for user provisioning
- Governance over the process (i.e., who is reviewing, who is approving)
- Proactive, required SOD check during provisioning (and strategy – Critical, High, Medium SODs must be remediated or mitigated before access can be granted)
- Automatic end-date for certain types of user access
- Automated termination for SAP systems connected when user expires on AD



Within IAG you cannot proactively require an SOD check, also simulations cannot occur. The IAG bridge does allow for both (as it is just a provisioning engine).

Illustrative example – Integration



Benefits and audit efficiencies – Emergency access

What are the benefits of Firefighter?

- Centralizes firefighting and administration across all systems
- Auditable workflow process for tracking log report approval
- Reduces effort required to grant and provision emergency access to multiple systems
- Provides a structured and documented process around emergency access
- Consolidated Log Report available

Typical audit review areas

- Critical and non-critical classification of FF IDs
- Critical and non-critical FF logs review requirements (i.e., 3 days vs. 5 days), governance and process
- Granularity of FF log review
- Use of permanent FF IDs
- Automated email reminders and auto-escalation procedures
- Process to validate FF IDs and owners periodically
- Level of access within the maximum FF role

Benefits and audit efficiencies – User Access Review

What are the benefits of automated UAR?

- Automate the periodic process of reviewing and reaffirming end user role assignments
- Business managers or role owners either approve or remove the roles that are assigned to each user
- Removals can be automatically de-provisioned from back-end systems
- Potential to lower change management activities by utilizing offline approval (Adobe forms)
- Integration with IAM tools for enterprise UAR process

Typical audit review areas

- Process to validate user access periodically
- Types of access being reviewed (i.e., all users, role-based review, sensitive access risks)
- Timeliness of user review response
- Completeness and accuracy of user access population
- Access removal process and lookback analysis for inappropriate users identified
- Watch out – only employees (not contractors) can opine on the appropriateness of users



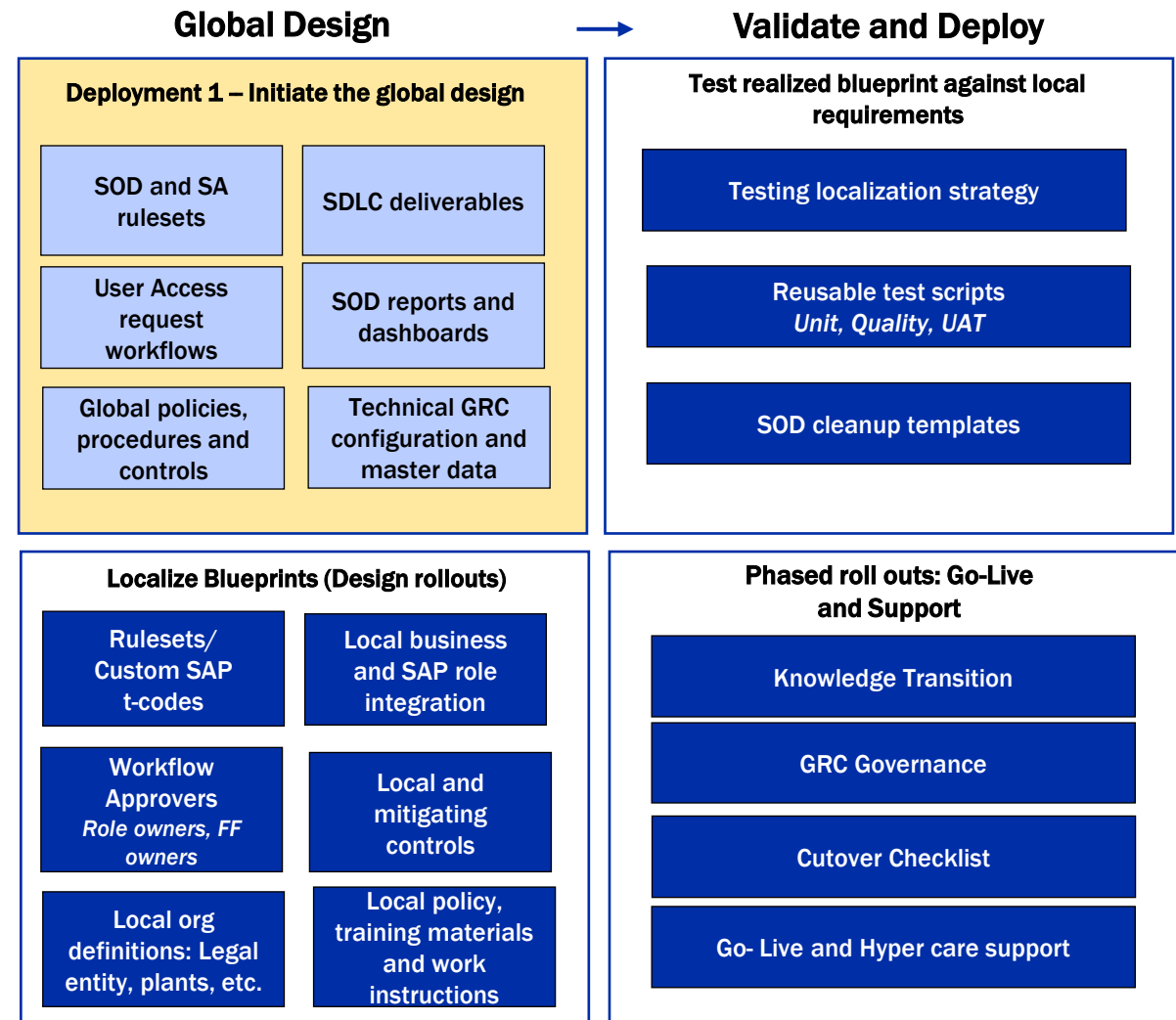
Identification of reviewers can be cumbersome, especially in a global organization, look for patterns in the data to generate logic for appropriate reviewers when integrating with IAM tools.

Audit review watch-outs

Area	Considerations
General/SDLC	<ul style="list-style-type: none">• Validate program test scripts to confirm all the scenarios are covered in testing (can be leveraged for audit)• Make sure policies/SOPs, governance, processes are up to date/approved• GRC baseline assessment over configuration settings
SOD and SA Monitoring	<ul style="list-style-type: none">• Ruleset gaps are at the tcode and authorization/permission level• GRC Ruleset Baseline and SOD mitigating control mappings can be leveraged for 3-5 years based on findings• High-risk areas will require independent testing; ability to assess privileged SAP access
Access Provisioning	<ul style="list-style-type: none">• Validation of the user termination process including SSO configurations• Validate self-service processes (password reset and lock/unlock) to make sure processes are appropriately integrated with the incident management system (ITGC – IT Ops)
Emergency Access	<ul style="list-style-type: none">• Testing includes a test of management’s control of reviewing and approving log activity, but does not include detailed review of each activity
User Access Review	<ul style="list-style-type: none">• Completeness and accuracy• Review granularity and integrity• LOOKBACKS!!

Phased, multi-release global SAP GRC rollouts

- The goal is to help enable SAP GRC phased rollouts in a self-service mode.
- The initial deployment will establish the foundation for building a sustainable SAP S/4HANA and GRC program.
- Audit reliance strategy should consider the delta and be aligned with your rollout strategy.



Wrap up



Where to find more information

[EY and SAP Alliance - Agile Risk | EY – Global](#)

- How can you prepare for what you can't control?

[5 common compliance myths when moving to S/4HANA](#)

- Natalie Freedline (LinkedIn Blog post, June 2022)

[Twenty questions to enhance your internal controls | EY - Global](#)

- Implementing the right integrated risk and control model and processes to address governance

Key points to take home

- **Implement SAP GRC/IAG to streamline your end-to-end SOX compliance function and increase auditor reliance.**
- **Help deliver innovative value by looking at enterprise-wide strategy to streamline, create efficiencies and avoid redundancy.**
- **Utilize the full GRC suite to get the most out of your investment.**
- **When creating your GRC business case include audit reliance for additional ROI.**
- **Work with your auditors to define a proactive audit approach.**

Thank you! Any questions?

Natalie Freedline

natalie.freedline@ey.com

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

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.
