Real-Time SoD Detection & Prevention

December 2021

APPSIAN

Intro

Improving SAP Segregation of Duties with Real-Time Detection & Prevention

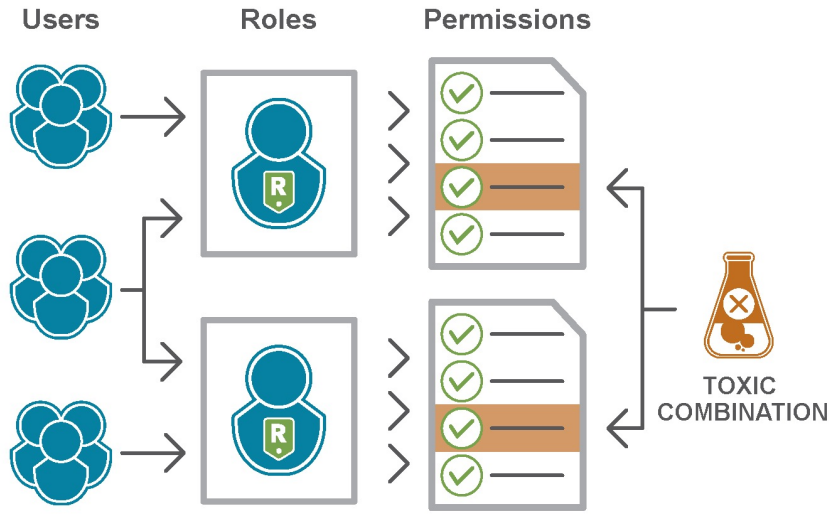
- Explore the challenges of today's static Segregation of Duties model in SAP
- Enable dynamic SoD scenarios in a secure and compliant fashion
- Eliminate the need for mitigating controls, and automate those controls when necessary
- Streamline SoD audits with an accurate view of actual SoD violations and accompanying details (false-positive free)

So What's Wrong with the Current Approach?

Static Role-Based Access Controls *Constrain* Segregations of Duties

A person can hold no more than one role within a set of permissions at a time.

Any exceptions to this static SoD model requires Compensating Controls



And Preventive Controls are Always Desired! (*When Available*)

Compensating Controls

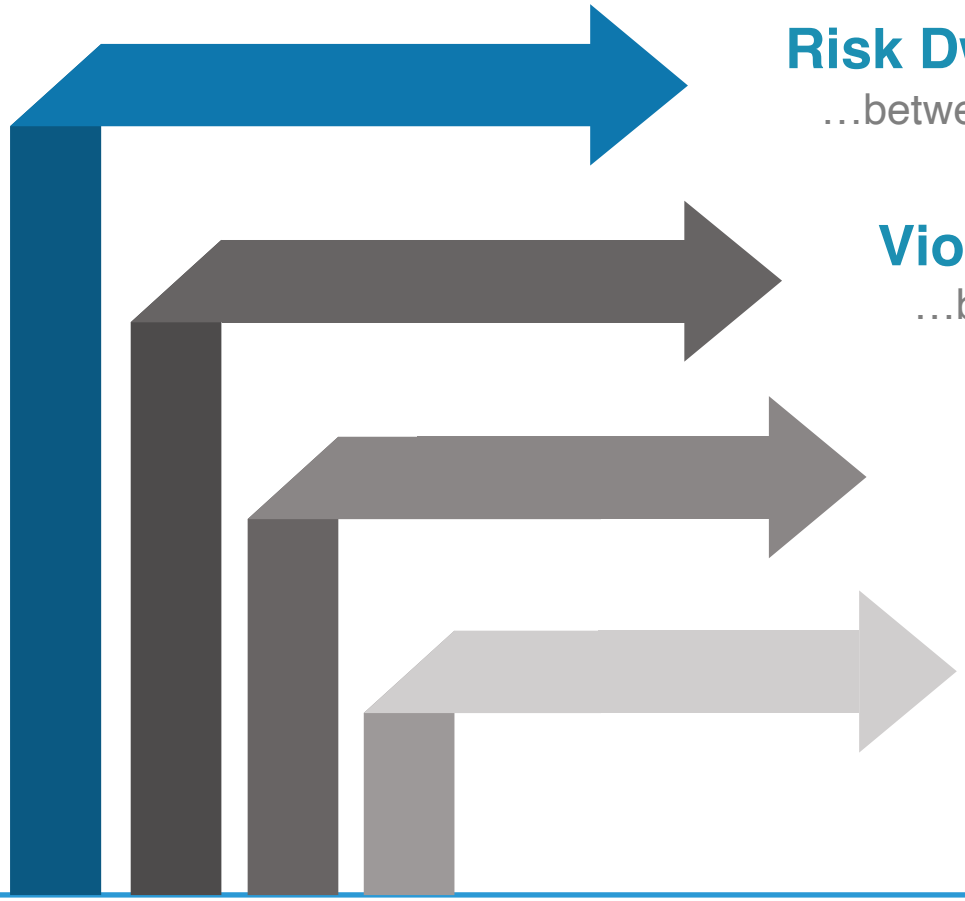
- Reactive
- Requires manual human review
- Flexible, but prone to error
- Unscalable, adds overhead

Preventive Controls

- Proactive
- Enforced automatically
- Rigid, but effective
- Scalable

IDEAL

The Business Impact of Exceptions



Risk Dwells Undetected
…between review periods

Violations Are Missed
…because of human error

Resources Are Diverted
…to review & approve audit logs

Audit Scope Is Limited
…due to overhead

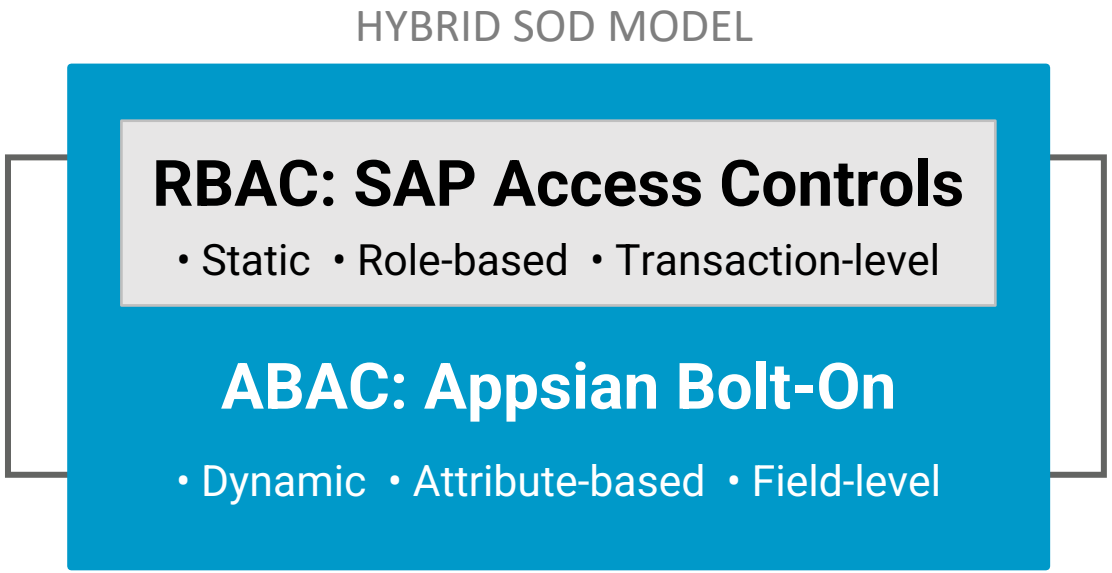
The Solution?

Attribute-Based Access Controls

Using a Hybrid RBAC + ABAC Model for Segregation of Duties

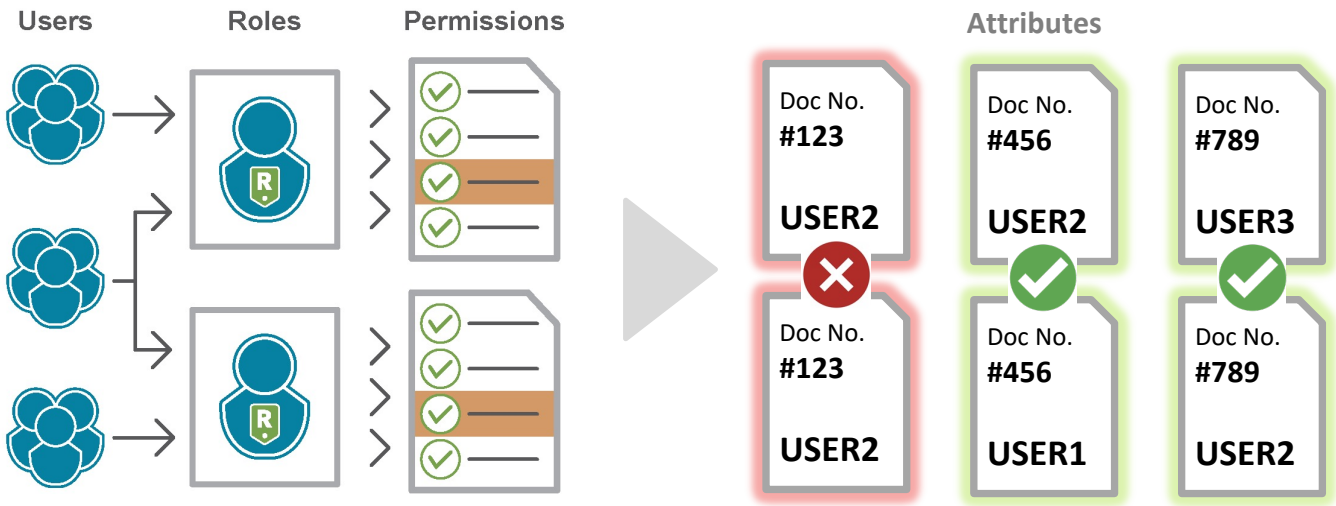
The authorization logic of **RBAC** is **limited** to static roles and permissions.

Adding **ABAC** extends authorization logic down to the **field-level**



Using a Hybrid RBAC + ABAC Model for Segregation of Duties

This granularity enables a **technical control** that can decipher ***actual violations*** from *false-positives* **at the authorization decision point.**



Strengthening SoD with Attribute-Based Controls and Real-Time Visibility

Add Preventive Controls to Exception Scenarios

Stop actual SoD violations while still allowing non-violating activity.

Reinforce Role-Based SoD Policy

Add a second layer of defense against unintentional over-provisioning

Detect & Report Violations in Real-Time

Enable continuous controls monitoring and alerting for control owners.

Dynamic Segregation of Duties – Conflicting Permissions

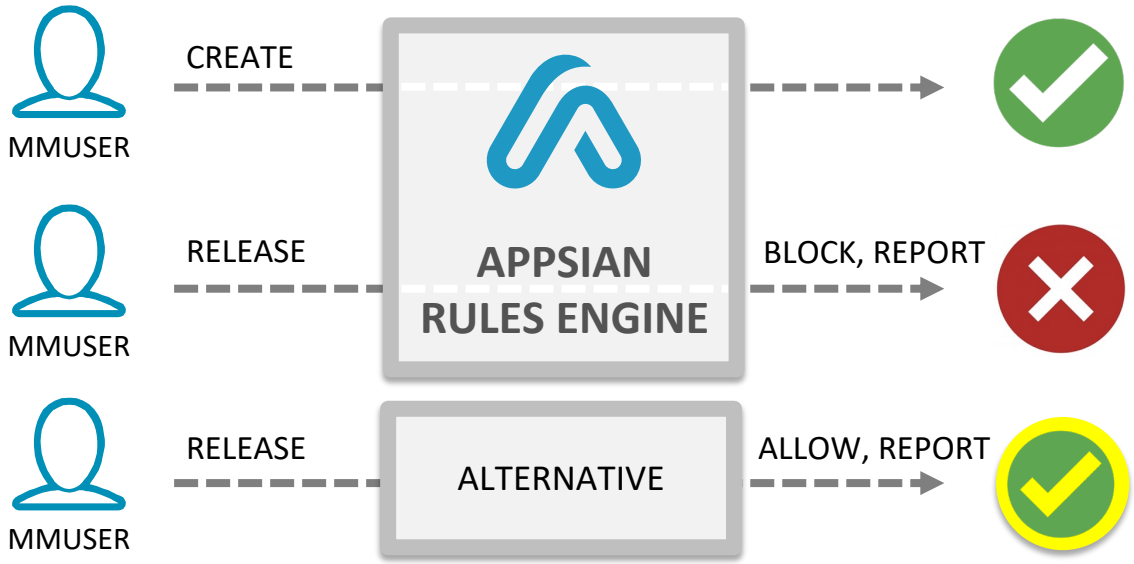
Enforcing SoD Policy based on User, Data and Transaction Attributes

MMUSER runs transaction, ME21N, to Create Purchase Order

MMUSER runs transaction, MIGO for GR Goods Movement (to same PO)

Option A.) Block & Report (with real time alert)

Option B.) Allow & Report (with real time alert)



Monitoring Segregation of Duties

Real-time reporting and alerting for SoD violations

Segregation of Duties

SOD Violations

User	Name	Department	Group	TCODE PO	TCODE PO Decription	PO Document	TCODE GR	TCODE GR Decription	GR Document
MMUSER	Mr. Mark Madison		MMGROUP	ME21N	Create Purchase Order	4500000013	MIGO	Goods Movement	5000000011
SAPDEV	Mr. George Washington		ADMIN	ME21N	Create Purchase Order	4500000006	MIGO	Goods Movement	5000000010
SDUSER	Mr. SD Consultant		SDGROUP	ME21N	Create Purchase Order	4500000001	MIGO	Goods Movement	5000000007
SDUSER	Mr. SD Consultant		SDGROUP	ME21N	Create Purchase Order	4500000001	MIGO	Goods Movement	5000000006
SDUSER	Mr. SD Consultant		SDGROUP	ME21N	Create Purchase Order	4500000001	MIGO	Goods Movement	5000000005
SDUSER	Mr. SD Consultant		SDGROUP	ME21N	Create Purchase Order	4500000001	MIGO	Goods Movement	5000000004
SDUSER	Mr. SD Consultant		SDGROUP	ME21N	Create Purchase Order	4500000001	MIGO	Goods Movement	5000000003
SDUSER	Mr. SD Consultant		SDGROUP	ME21N	Create Purchase Order	4500000001	MIGO	Goods Movement	5000000002
SDUSER	Mr. SD Consultant		SDGROUP	ME21N	Create Purchase Order	4500000001	MIGO	Goods Movement	5000000001
FIUSER	Mr. Fred Iceman		FIGROUP	ME21N	Create Purchase Order	4500000000	MIGO	Goods Movement	5000000000

Wrap Up

- Exceptions don’t have to be a pain!
- Fine-grained Preventive Controls are possible
- Using a Hybrid RBAC & ABAC model can strengthen SoD
- Real-time violations monitoring will catch red flag events faster and help streamline auditing

Thank You