



Managing risk after upgrading to S/4HANA

Greg Capps
SAP Business Consultant
Georgia-Pacific

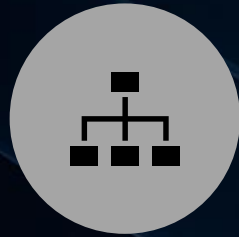
Anyone can deliver security; it is only a transaction and role assignment. This mindset existed several years ago but technology has changed. Understand how Fiori apps work with standard SAP controls. How to trace security authorizations for Fiori and best practices for updating authorization defaults. Understand the case for building business roles in GRC instead of assigning a single role to a connector. Integration across systems, on premise and in cloud architecture are important reasons to embrace GRC and maybe even IAG.

S4/HANA is not just an upgraded ERP system. Many companies have approached SAP upgrades as technical activities and not embraced enhanced business functionality. With those changes your infrastructure, database and even security are impacted. What are risks that you should be aware of with S4/HANA? Do you use GRC Access Control? Are you embracing new functionality or recreating old business processes? Are you on-prem or did you Rise to SAP in the cloud? Join us as we discuss how to reduce risk, simplify your project tasks and manage your digital transformation.

AGENDA



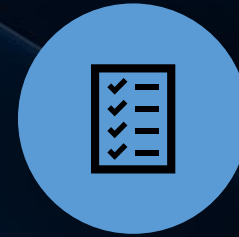
S/4HANA
BROWNFIELD OR PRE-
1909



MANAGING RISK &
PROVISIONING



SECURITY BY DESIGN



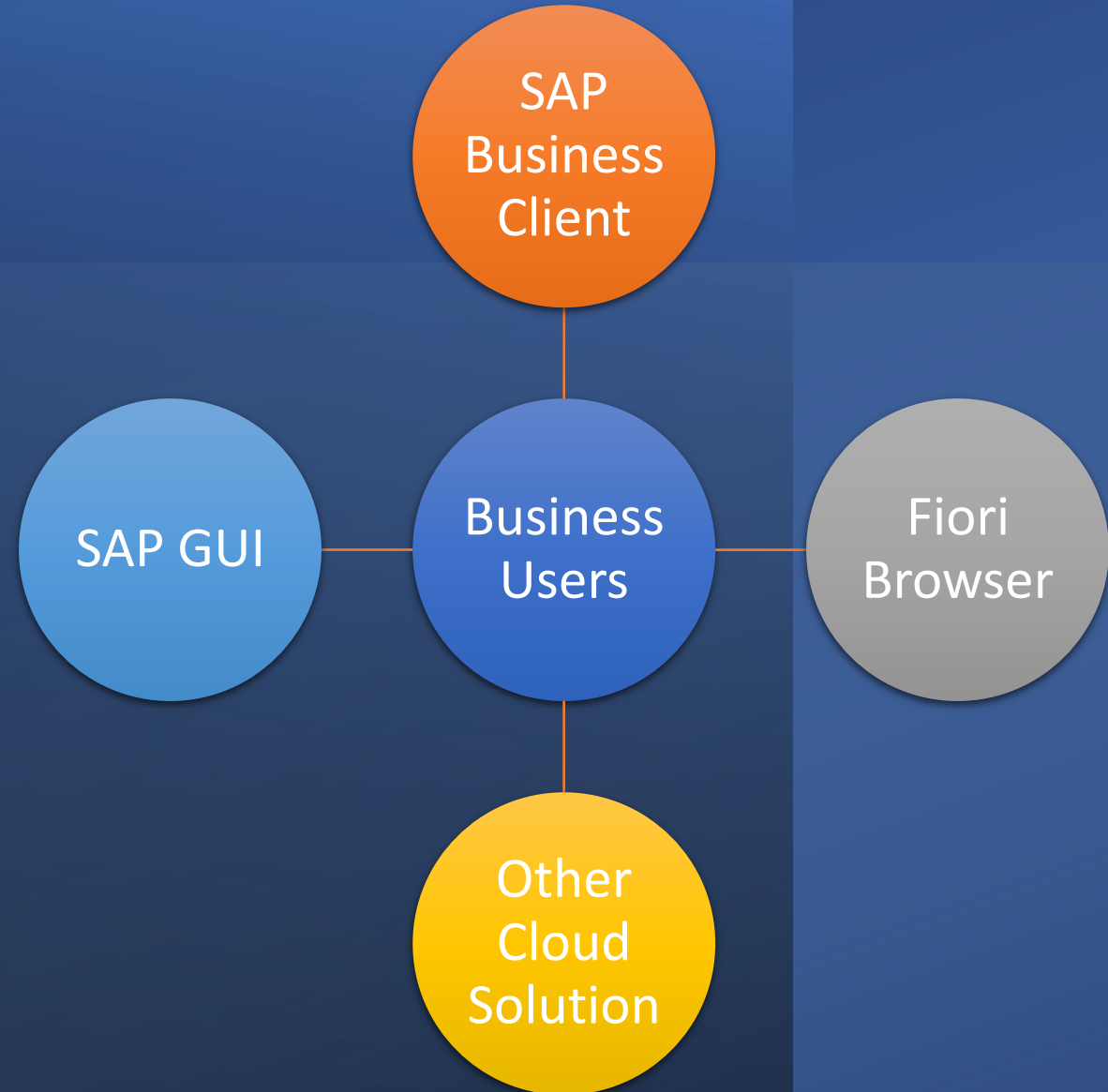
UPDATED AUDIT
INFORMATION SYSTEM



LESSONS LEARNED

S/4Hana Brownfield
or Pre-1909

How will Business Users Interface with S/4HANA Systems?



SAP Simplification Continues : Transactions & Programs are Becoming Obsolete

- First Release of S/4HANA obsolete (1511)
- S/4HANA 1511, 1610, 1709 and 1809 implementations becoming obsolete
- Standard Maintenance for new releases is 5 Years (after 2023 proposal for 7 years w/feature packs)
- ECC was setup and support forever
- S/4HANA is an ongoing continuous improvement project
- You must embrace change to enable easier upgrades



SAP Simplification Continues : Transactions & Programs are Becoming Obsolete

- Master list of impacted transactions/programs - DNE
- Program PROFGEN_CORR_REPORT_2 provides list of obsolete transactions in role menus
- Many Central Transactions replaced derivations
- Some transactions enhanced instead of becoming web-based Fiori Apps

[Simplification Item Catalog](#)

SAP S/4HANA 2022

734

734 Items

SAP S/4HANA 2021

695 Items

SAP S/4HANA 2020

677 Items

SAP BW/4HANA 2.0

85 Items

SAP Simplification Continues : Transactions & Programs are Becoming Obsolete

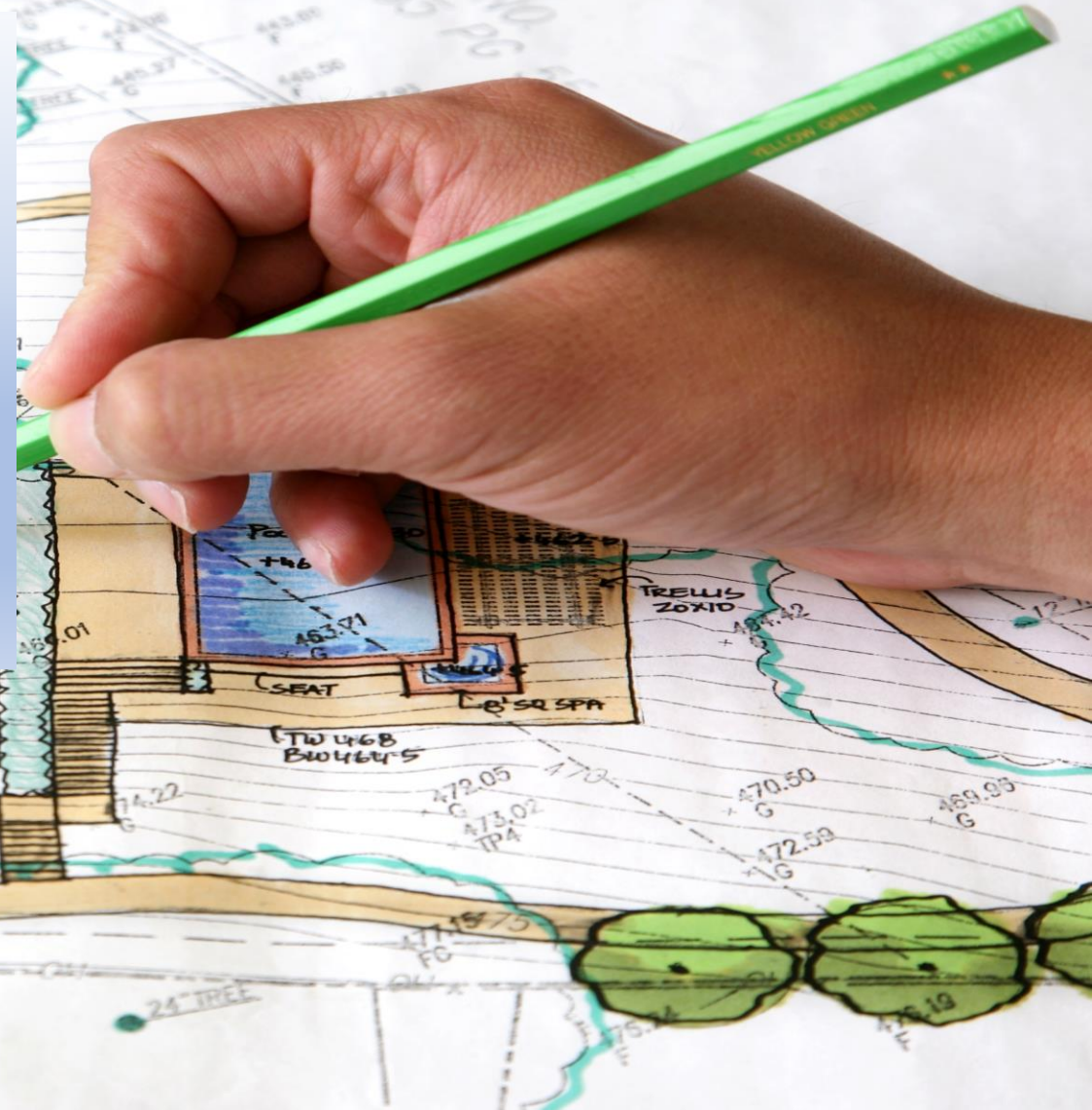
- Table SBLM_BLACKLIST – Obsolete Transactions, Programs, etc.
- SAP Error - [2476734 - Runtime error SYSTEM ABAP ACCESS DENIED](#)
- SAP Error - [2295840 - Outbound / Inbound calls from external to RFC FM are blocked when the FM is blacklisted and the UCON-Check is active](#)
- S/4HANA 2109 UCON is active by default

Table SBLM_BLACKLIST Select Entries 5,007

●○○	PS4S:ITR:HM:XXX:MAS...	ITR - HM - Mass Mainten...	56	Transaction	IW37	Entry will be replaced	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IW37N	Change Orders and Operat...	
○▲○	PS4S:ITR:PN:XXX:COM...	ITR - PN - ITR Common ...	107	Transaction	IW49	Old entry will be deleted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IW49N	Display Orders and Operati...	Transactio
○▲○	PS4S:ITR:PN:XXX:COM...	ITR - PN - ITR Common ...	111	Transaction		Old entry will be deleted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			Transactio

SAP Simplification Continues : What do you do?

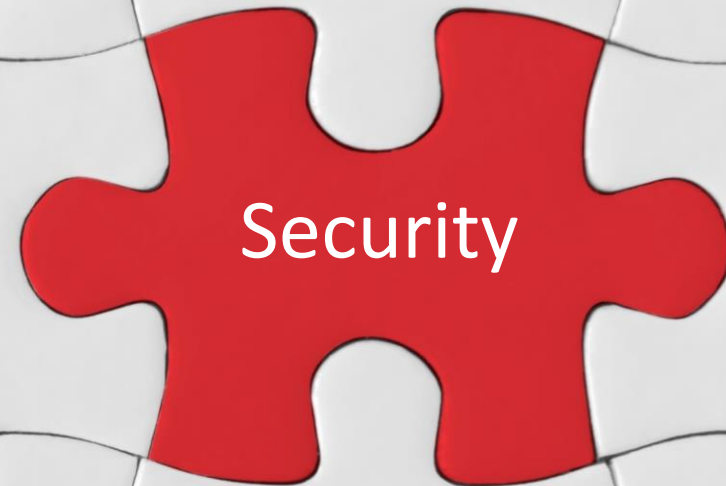
- SU25 Upgrade Procedures
- Use the SAP Upgrade Tools
- Customer Specific Digital Transformation - SAP Readiness Check
- Based on your activity and configuration a plan
- Process Improvements
- TEST, TEST, TEST





Overhaul what you own or Charge Ahead
Brownfield, Bluefield, Greenfield
Every choice has a cost/benefit but what do you have
when you are live?

Security transactions, Fiori Apps authorizations, object values and roles are only a small piece of the S/4HANA journey.





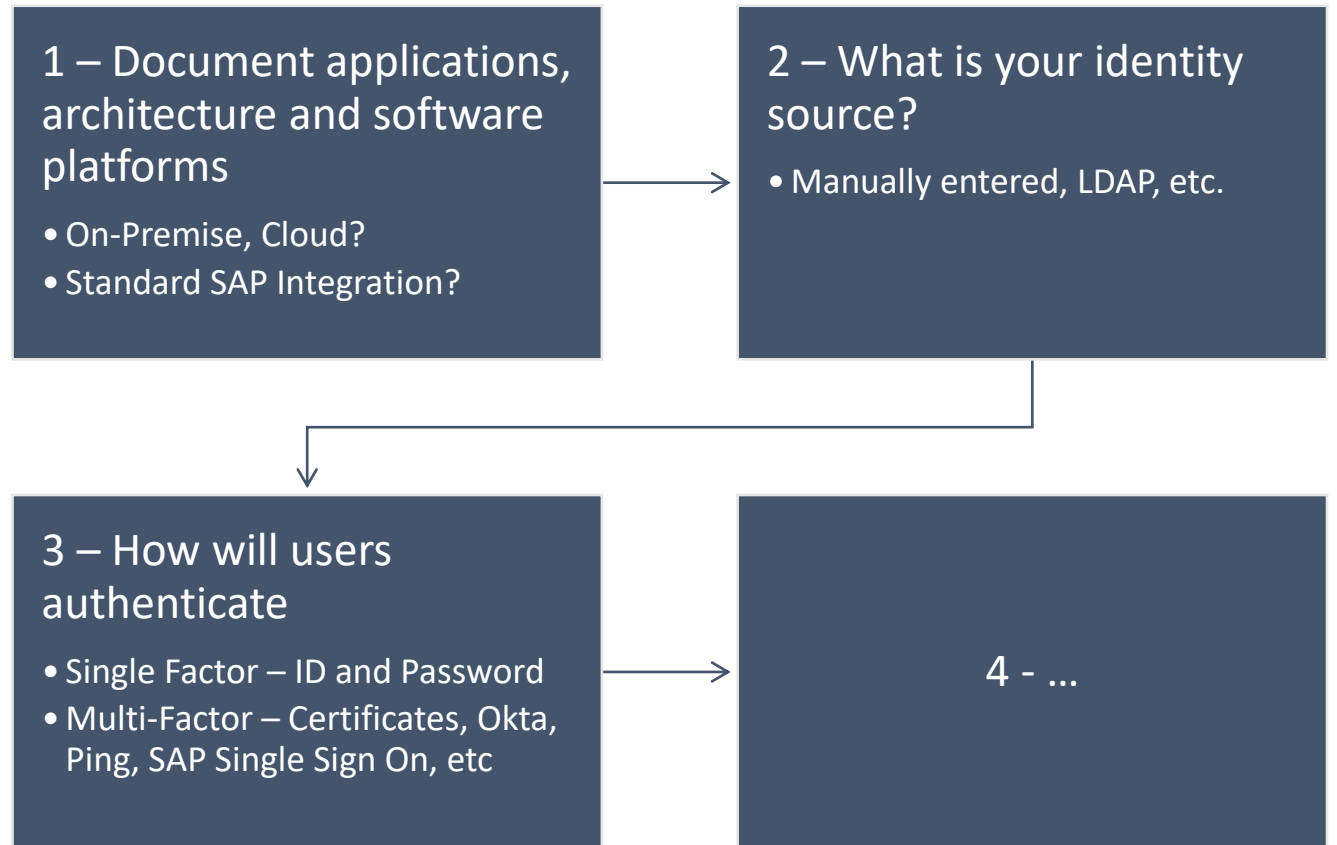
Security – ~~Set of business transactions assigned to a role.~~ MUCH MORE

- Security Parameters for your new infrastructure
- Authentication methods
- Internal or Alternative Identity Source?
- On-Prem Datacenter
- On-Prem Private Cloud
- Private Cloud
- Public Cloud
- VPN Only or Internet Accessible?
- Mobility (RF, Tablet, Phone, Camera...)

Managing Risk & Provisioning:
GRC Access Control, IAG,
Manually, ??



Understand the user lifecycle and daily processes



	Systems in Scope	Authorization Sync	Prefix/Abbreviation	Risk Analysis	Standard Ruleset Available
Traditional Tcodes/Action & Authorization	SAP/ERP, ECC, Portal	Yes	Traditional Actions	Yes	Yes
Webdynpro Application	SRM	Yes	[WDY]	Yes	Yes
Odata Services	S/4, Basis Release 731 & above having Odata Services	Yes	[SVC]	Yes	Yes
Fiori Application	Fiori system	Yes	[FAPP]	Yes	Yes
Fiori Catalog	Fiori system	Yes	[FCAT]	Yes	No

[2655122 - Maintaining GRC Risks Beyond Transactions](#)

GRC Risks and Rules

Note 2655122 is a great overview

Running SOD Risk analysis in GRC application requires risks / rules with the combination of ...

- **Proper Action / Transaction Code** - Both the SOD Functions have proper action added in Action tab along with required permissions in Permission tab. Such combination creates rules with proper actions. These actions are normal Transaction codes available in source system. For example. SU01 v/s PFCG. Both the SU01 & PFCG are executable transaction codes which are used as Actions in Functions. Note :- Best Practices Risks information is available in KBA # [986996](#).
- **Webdynpro Application** - Function can have webdynpro application as an action in action tab. To create risk with Webdynpro Application, Action should have [WDY] as prefix. In other words, All the webdynpro application actions start from [WDY] to differentiate it from the traditional transaction codes of R3/NW system. For example, [WDY]/SAPSRM/WDA_L_FPM_OIF v/s BBPBWSP_SIMPLE. BBPBWSP_SIMPLE is a traditional SRM tcode and [WDY]/SAPSRM/WDA_L_FPM_OIF is a webdynpro application. Combination of both creates risks.

Note :- SAP introduced SRM Webdynpro Application rules in 2015. Refer to KBA # [2171822](#) for more details. If you are creating your Custom rules for Webdynpro Application, you need to prefix [WDY] with action

- **ODATA Services** - Function can have ODATA services as an action in action tab. To create risk with ODATA Services, Action should have [SVC] as prefix. In other words, all the ODATA services starts from [SVC] to differentiate it from traditional transaction codes of R3 / NW system. For example, [SVC]FAP_PAYMENT_POST_SRV 0001 v/s FD01. FD01 is traditional transaction code and [SVC]FAP_PAYMENT_POST_SRV 0001 is a webdynpro service. Combination of both creates risks.

Note:- 1. SAP introduced standard Fiori & S4 HANA rules including Services in 2018. Refer to KBA# [2539742](#) for more details. S4 Hana standard rules are having services enabled. If you create your own custom risks, you need to prefix [SVC] with Service name.

Note:- 2. If S_SERVICE authorization object is used with Field SRV_NAME in custom rules, then service name should have prefix [SVC] with service name, in order to get the correct risk analysis result of services. (Example below from GRC delivered Function.)

The screenshot shows the SAP GRC configuration for Function AR01. The 'Details' tab is active, showing the following fields:

- Function ID: AR01
- Description: AR01 - AR Payments
- Business Process: Order to Cash
- Analysis Scope: Single System

The 'Action' tab is also visible, showing a table of permissions:

System	Permission Group	Permission	Field	Value From	Value To	Condition	Status
SAP_S4A_LG	[FAPP]AccountingDocumei	S_SERVICE	SRV_NAME	[SVC]ABC5A2651FDD0A3E4C90CF317938F0		AND	Active

Note:- 3. Certain fixes are available for S_SERVICE Auth Objects. Refer to KBA # [2639161](#).

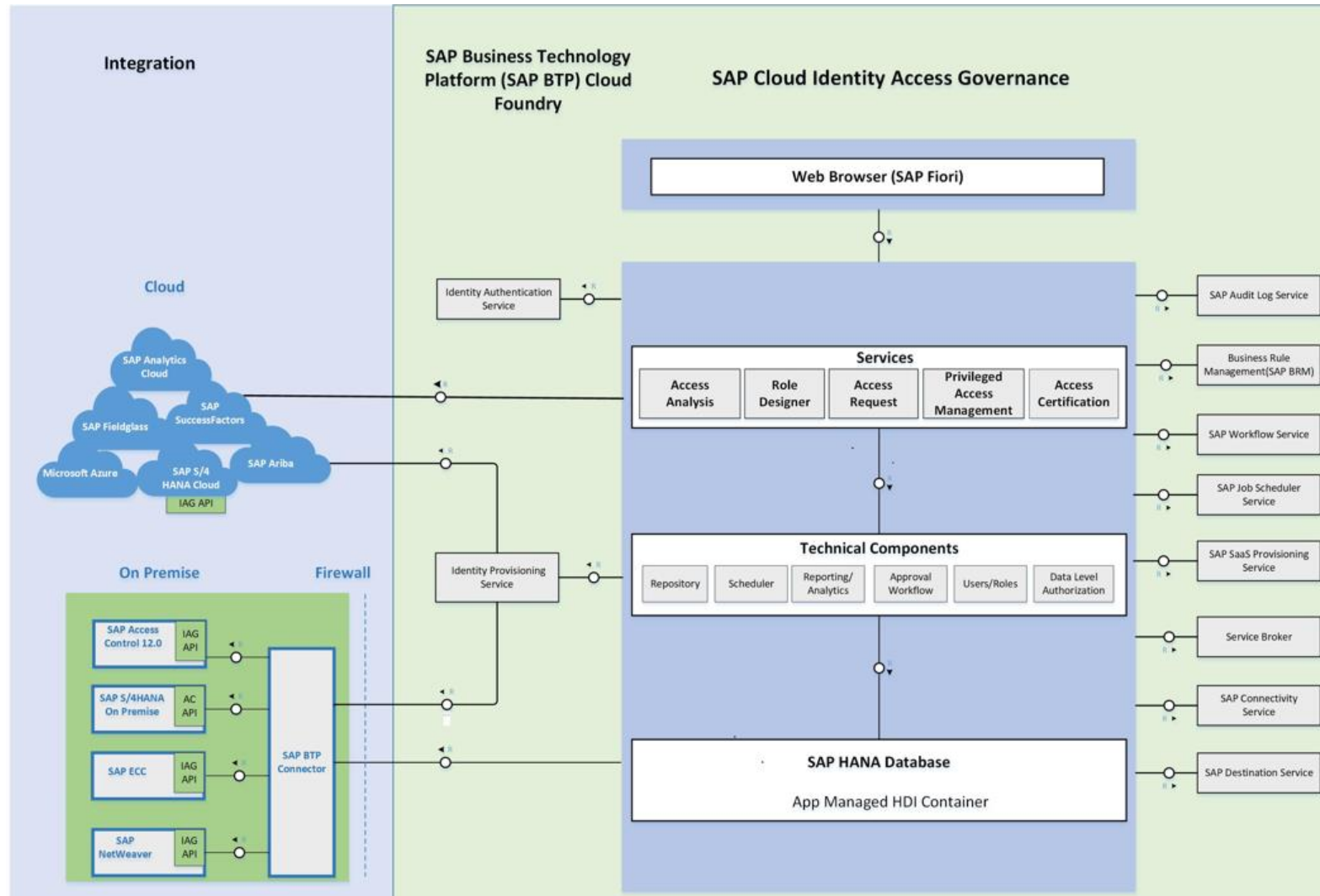
- **Fiori Application** - Function can have Fiori Application as an action in action tab. To create a risk with Fiori Application, Action should have [FAPP] as prefix. In other words, all the Fiori Application actions should have [FAPP] as prefix to differentiate it from traditional transaction code of R3 / NW system. For example, [FAPP]Supplier-postPayment v/s FD01. FD01 is a traditional R3 transaction code and [FAPP]Supplier-postPayment is a Fiori Application. Combination of both creates a risk.
- **Fiori Catalogs** - Function can have Fiori Catalogs as an action in action tab. To create a risk with Fiori Catalogs, Action should have [FCAT] as prefix. In other words, all the Fiori Catalogs actions should have [FCAT] as prefix to differentiate it from traditional transaction code of R3 / NW system. For example, [FCAT]SupplierPayment v/s FD01. FD01 is a traditional R3 transaction code and [FCAT]SupplierPayment is a Fiori Catalogs. Combination of both creates a risk.

GRC Risks Combinations

- Traditional Transaction within both sides of a risk
 - Traditional Transaction versus an ODATA service
 - ...
 - If you upgraded without maintaining your ruleset
 - If your scope for your new project was only security roles
 - If you want to manage risk
-
- GRC Risk Analysis Requirements are a large set of tasks!

[New Approach for Risk Analysis | S/4HANA On-Premise](#)

GRC and Identity Access Governance (IAG)



Overview of IAG Components

Component	Description
Target Applications (on-Premise, cloud)	This is the target system containing user data.
IAG API	The API for SAP Cloud Identity Access Governance services extracts data from the target application. The API is part of SAP NetWeaver; make sure your system has the required NetWeaver Basis Support Packs. The API is available for on-premise and the SAP HANA Cloud.
SAP BTP connector	The cloud connector sits behind the firewall and establishes connectivity between SAP BTP and the target system.
IAG Services	SAP Cloud Identity Access Governance services include: Access Analysis service; Access Request service; Role Design service; Access Certification; Privileged Access Management.
Technical Components for IAG services	SAP Cloud Identity Access Governance services components include: Repository, Scheduler, Reporting and Analytics, Approval Workflow, and Users and Roles
Identity Authentication service	Identity Authentication service is used to authenticate users before allowing access to the SAP Cloud Identity Access Governance solution and services.
SAP Workflow Management service	SAP Workflow Management is used for automation of access requests through the various stages of creation and approval.
SAP Business Rules Service	Business Rules Service enables embedding business decisions into the workflow.
Identity Provisioning service	Identity Provisioning service allows provisioning of centrally managed identities and their access across the enterprise (on-premise and cloud).

GRC Emergency Access

EAM or Firefighter Requirements

- On-Premise ABAP
- SAP Cloud
- Database Firefighter
- ?



Security By Design



SAP Design or Your Design

When you hear SAP state Security by Design, what do you think they are communicating?



Authorization Errors

- SU53 : Evaluate Authorization Check
- STAUTHTRACE : System Trace for Authorization Checks
- Parameter auth/tcodes_not_checked : Value "SU53 SU56"
- Failures are not necessarily required values
- Cross System Analysis required?
- SM20 : Security Audit Log Analysis

Authorization error analysis

You can use transaction `SU53` to analyze an access-denied error in your system that just occurred. It displays the **last failed authorization check**, the user's authorizations, and the failed HR authorization check.

You can use transaction SU53 from **any of your sessions**, not just the one in which the error occurred.


Set it and forget it

- **One Time**
- **Annual Audit Review**
- **Environment Changed**
- **Migrate Old Values**
- **Incident Occurs**
- **What triggers your review of SAP Security Settings?**


Prior to
S/4HANA

- Password Complexity & Period Updates
 - login/min_password_diff
 - login/min_password_digits
 - login/min_password_letters
 - login/min_password_lng
 - login/min_password_lowercase
 - login/min_password_specials
 - login/min_password_uppercase
 - login/password_expiration_time
- Met many audit requirements but falls short with a single factor for entry
- Some believed just extended Minimum Password to 10 or 12 solves risk

Current Best Practices SAP Security Parameters

- Basic Password Complexity – Minimum even with SSO
 - login/min_password_lng value of 8 or greater
 - Login complexity should force at least 3 types (upper, lower, number, special, etc)
 - login/password_max_idle_initial value of 14 or less
 - login/password_max_idle_productive consider 90 days to deactivate SSO only users or inactive accounts
 - [863362 - Security Best Practice Checks](#)
 - [SAP Security Configuration Guide](#)
- 

Report RSPFRECOMMENDED

<  Show all recommended values

🔍 ☰ ☰ 🔍 📄 📄 📄 📄 📄 📄 📄 📄 📄 📄 More ▾

Parameter Name	Actual Value	Recommended Value
auth/check/calltransaction	2	3
auth/object_disabling_active	Y	N
auth/rfc_authority_check	1	6
login/password_downwards_compatibility	0	0
login/show_detailed_errors	1	0
rdisp/gui_auto_logout	3600	3600
rdisp/vbdelete	400	0
rfc/callback_security_method	1	3
rfc/reject_expired_passwd	1	1
login/password_hash_algorithm	encoding=RFC2307, algorithm=iSSHA-1, iterations=1024, saltsize=96	encoding=RFC2307, algorithm=iSSHA-512, ite
login/disable_cplic	0	1
icf/set_HTTPOnly_flag_on_cookies	3	0
gw/rem_start	REMOTE_SHELL	DISABLED
gw/reg_no_conn_info	1	255
ms/http_logging	0	1
ms/HTTP/logging_0		PREFIX=/,LOGFILE=\$(DIR_LOGGING)/ms-htt
icm/security_log	LOGFILE=dev_icm_sec,MAXSIZEKB=10000	LOGFILE=\$(DIR_LOGGING)/dev_icm_sec-%y

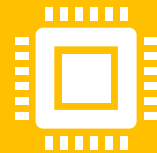
Security by Design by Default



Brownfield implementations or go lives prior to 1909 must manually implement Security by Design Parameters



Enhanced with 2020 and 2021



[2926224 – Security by Design for SAP S/4HANA and SAP BW/4HANA](#)

Security by Design Profile Parameter Supporting Documentation

	A	B	C	D	E	F	G	H	I
1	Area	Type of setting	Name	Storage	Description	Relevant SAP Note	SAP Note URL	New recommended value	Impact to operation
2	Authorizations	Profile parameter	auth/check/calltransaction	DEFAULT.PFL	Behavior of authority check during call transaction: Controls how CALL TRANSACTION statements in all programs react regarding missing entries in SE97 / table TDCOUPLES. If not set to 3, authorization checks are not properly enforced.	515130	515130	3	In special cases, "jumps" from with another may fail due to missing a
3	Authorizations	Profile parameter	auth/object_disabling_active	DEFAULT.PFL	Enables to globally switch off authorization checks for selected authorization objects (prerequisite for transaction AUTH_SWITCH_OBJECTS). If not set to "N", a global deactivation would be possible.	2926224	2926224	N	The disabling of authorization obj This feature can no longer be used
4	Authorizations	Profile parameter	auth/rfc_authority_check	DEFAULT.PFL	Execution option for the RFC authority check: Controls the behavior of enforced authentication and authorization checks when RFC function modules are called from remote. If not set to 6, an information disclosure vulnerability exists for unauthenticated users.	2216306	2216306	6	In certain cases, dumps may occur interfaces try to retrieve informati authentication. In transaction SM functions like "Unicode test" for a user, a logon will be prompted.
5	Server infrastructure	Profile parameter	gw/reg_no_conn_info	DEFAULT.PFL	Specific security-related additional functions for the RFC gateway are activated depending on which bits are set in this bitmask. If not set to 255, not all security checks may be properly enforced in the RFC gateway.	2776748 1444282	2776748	255	In very rare situations, connects fr the RFC gateway may fail. This wil requiring the 3rd party service.
6	Server infrastructure	Profile parameter	gw/rem_start	DEFAULT.PFL	This setting specifies with which method an RFC server might be started on OS level from an external endpoint. If not set to "DISABLED", attempts to utilize an improper or even insecure OS logon method (like RSH) might be possible.	2776748 1520096	2776748	DISABLED	In very rare situations, connects fr the RFC gateway may fail. This wil requiring the 3rd party service.

Security by Design by Default



**SECURITY
DEFAULTS**



**BEST
PRACTICES**



REDUCES RISK



**CUSTOMERS
FAILING**

Solution Manager Configuration Validation

- No Longer Set & Forget
- Periodically Validate all SAP Systems within production landscape
- One system as a reference system or a profile
- Report card of all systems not in compliance
- Built into Solution Manager Root Cause Analysis

SAP Configuration Validation Help

- [SAP Solution Manager Setup - Support Wiki](#)
- Videos available on YouTube
- Guided Procedures within Solution Manager
- Must download Configuration Validation defaults for import

https://support.sap.com/sos

SAP Support Portal Home / Offerings & Programs / Support Services

SAP Security Optimization Services Portfolio

Best Practices Overview Topics Services & Tools **Media Library**

Media Library

Search:

Title	Type	Changed
_SAP Security Notes Advisory	ZIP	2022-06
_Security Notes Webinar	PDF	2022-06
Security Optimization Services - Sample Report for SAP BTP	PDF	2022-05
SAP CoE Security Services - Security Baseline Template Version 2.3 (including ConfigVal and Dashboard Builder Package 2.3_CV-1)	ZIP	2021-12

SAP Unified Connectivity (UCON)

Problem: SAP Customers have not followed best practices and excessive remote access is available for exploitation.

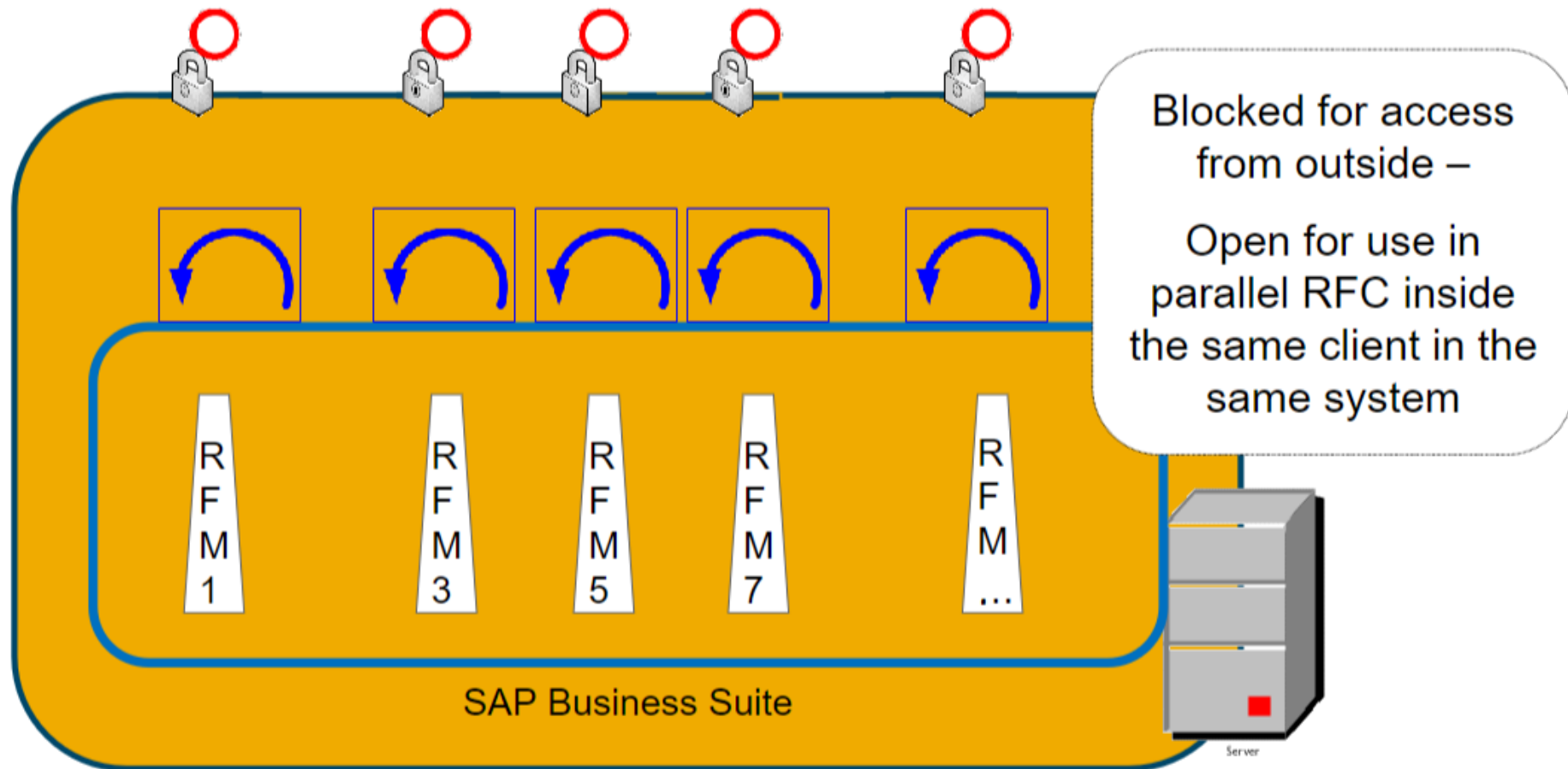
Facts: Most customers require a limited number of exposed function modules but continue to expose over 40,000

Solution: SAP Unified Connectivity (UCON)

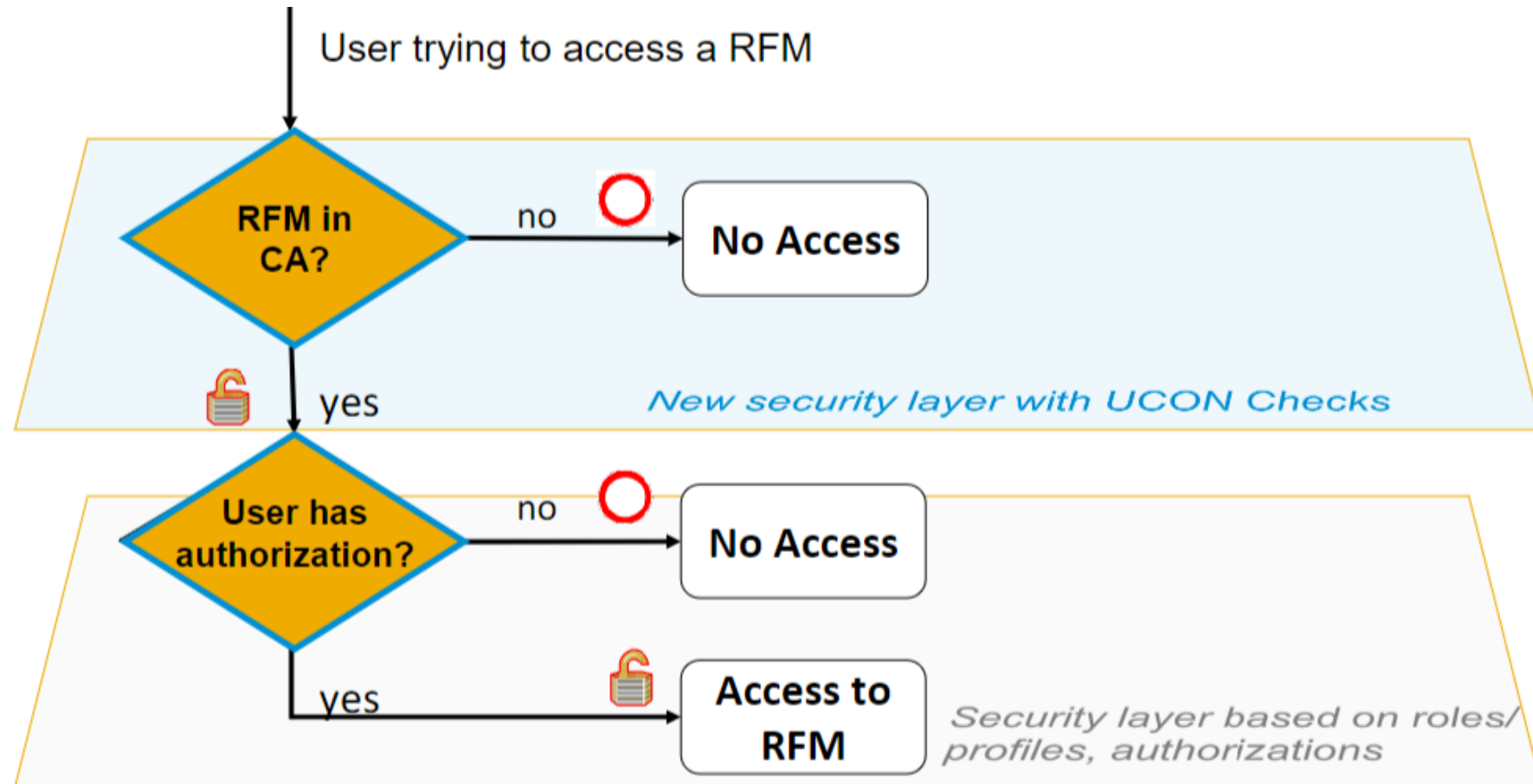
- Identify Function Modules Required
- Block all remaining Function Modules



UCON Does not impact local system/client



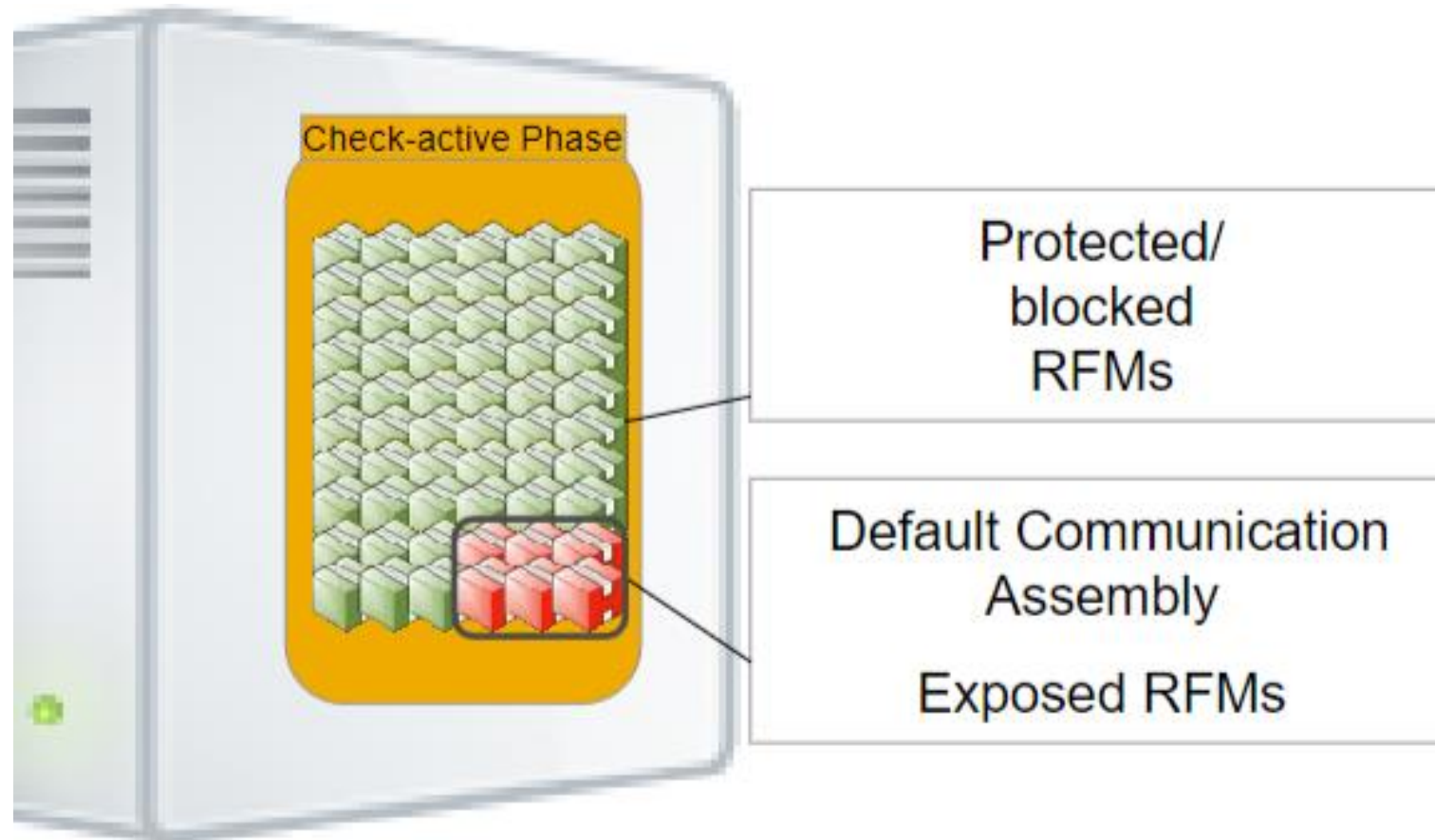
UCON – A new independent layer of checks



UCON Setup & Configuration

- Activate UCON profile parameter - UCON/RFC/ACTIVE = 1
(enable UCON runtime checks for RFM on all servers)
- Activate UCON service in DEV for transport- UCONCONF

RFC Risk after UCON CA is active





Questions

A photograph of a textile mill. In the foreground, a large roll of fabric with a pattern of blue and green circular motifs is being processed. The background shows yellow metal scaffolding and industrial machinery. The image is dimly lit, with a semi-transparent dark overlay.

Contact Details:

E: greg.capps@gapac.com

Li: [linkedin.com/in/cappsgreg/](https://www.linkedin.com/in/cappsgreg/)
