IBM Security

SAP Security

Holistic focus to cover the 13 layers of SAP Security

Victor Garcia Rodriguez

IBM Security – Associate Partner – CoC Lead for SAP Security & GRC

Milano, June 18th 2019

IBM

Table of Contents

The 13 layers of SAP Security by IBM

1. SAP Security

The other side of the Compliance “coin”

1. SAP Security – The other side of the Compliance "coin"

The SAP Security market is split into two big areas: Compliance and IT Security

Regulatory Compliance

- **Audit** centric
- **Risks** driven (COSO)
- Driven largely by **regulatory requirements**
- **Sample** based
- Scope limited by **audit domain**
- Evaluated on a **quarterly or annual basis**

IT Security

- **Business** centric
- **Policies and Controls** based (COBIT)
- Driven by **business requirements**
- **Scope is Holistic**
  - Enterprise and extended community (E.g. 3rd parties, suppliers, partners, etc.)
- Evaluated on a **near-real time basis**

Mainly is a **Big4 / Audit firms** world…

Mainly is an **IT / Technical companies** world…

1. **SAP Security** – The other side of the Compliance “coin”

What does it mean? What does people usually think SAP Security is?

SAP Authorizations

Segregation of Duties

SAP Roles

SAP Identity Management

SAP GRC Access Control

Single Sign-On

SAP Security Parameters

1. SAP Security – The other side of the Compliance “coin”

Scope of this session: Technical SAP Security

1. Governance		**Internal Control**, **Internal Audit**, **Enterprise Risk** and **Regulation Affairs**: Integration and Automation of the Three Lines of Defense
2. Access Management		**Segregation of Duties, Identity and Role Management**: User Access complying with Regulatory Requirements (E.g. SOX)
3. Data Privacy		**GDPR** (and others): Data Retention and Data Deletion, Data Portability, Data Field Masking, Access Logging to Personal Data
4. Business-IT Monitoring		**Continuous Control Monitoring (CCM)**: Configurable and Transactional controls // Fraud Scenarios // RPA // Predictive Risk Analytics
5. Authentication		**Unified Access to SAP systems**: Single Sign-On // **Double Factor Authentication** (Two-Factor) // **Secured Communication**
6. Application Security		**Custom Source Code**: Automated analysis to Identify potential Security Breaches // Optimize Performance using SAP best-practices
7. Application Server		**SAP Server configuration**: Security Parameters of all Clients // Secured Services // Patching Level // OSS Notes
8. Database Security		**SAP HANA**: Secured access to SAP HANA Views and Schemas // Integration with data lakes // Ensure no open paths to access data
9. Data Encryption		**Data Volume Encryption** (HANA) // Usage of SAP **Cryptographic Libraries** // Secured Socket Layer // Public Key Infrastructure (**PKI**)
10. Network and Communications	**Pen Testing**	**Securization of RFCs** (Remote Function Calls) // **Support from SAP** // Management of **Web connections**
11. Vulnerability Assessment		**OS users** (broad privileges) // **SAP log analysis** and integration with SIEM solution // Integration of **antivirus** into SAP
12. Infrastructure Security		**Configuration of physical / logical devices**: Firewall and Gateways // OS and Applications Logs
13. Physical Security and Hosting		**Standard Controls Coverage** (SOC reports) // **Compliance Level** of each Cloud platform // Ad-hoc Security audits // Physical hacking

2. The 13 layers of SAP Security by IBM

SAP Security requires an holistic focus, analyzing it "as a whole"

2. The 13 layers of SAP Security by IBM

Impact of SAP Security on Business: **Ponemon Research Report** – Key Findings

92%

92% indicated an **SAP breach would be serious, very serious or catastrophic**

65%

65% said their **SAP System** was **breached at least once in the past 24 months**

$4.5M

Average cost to take SAP offline was $4.5M **per incident**

47%

47% indicated they were **“not confident” or had “no confidence”** that they could **detect an SAP breach** within a year

59%

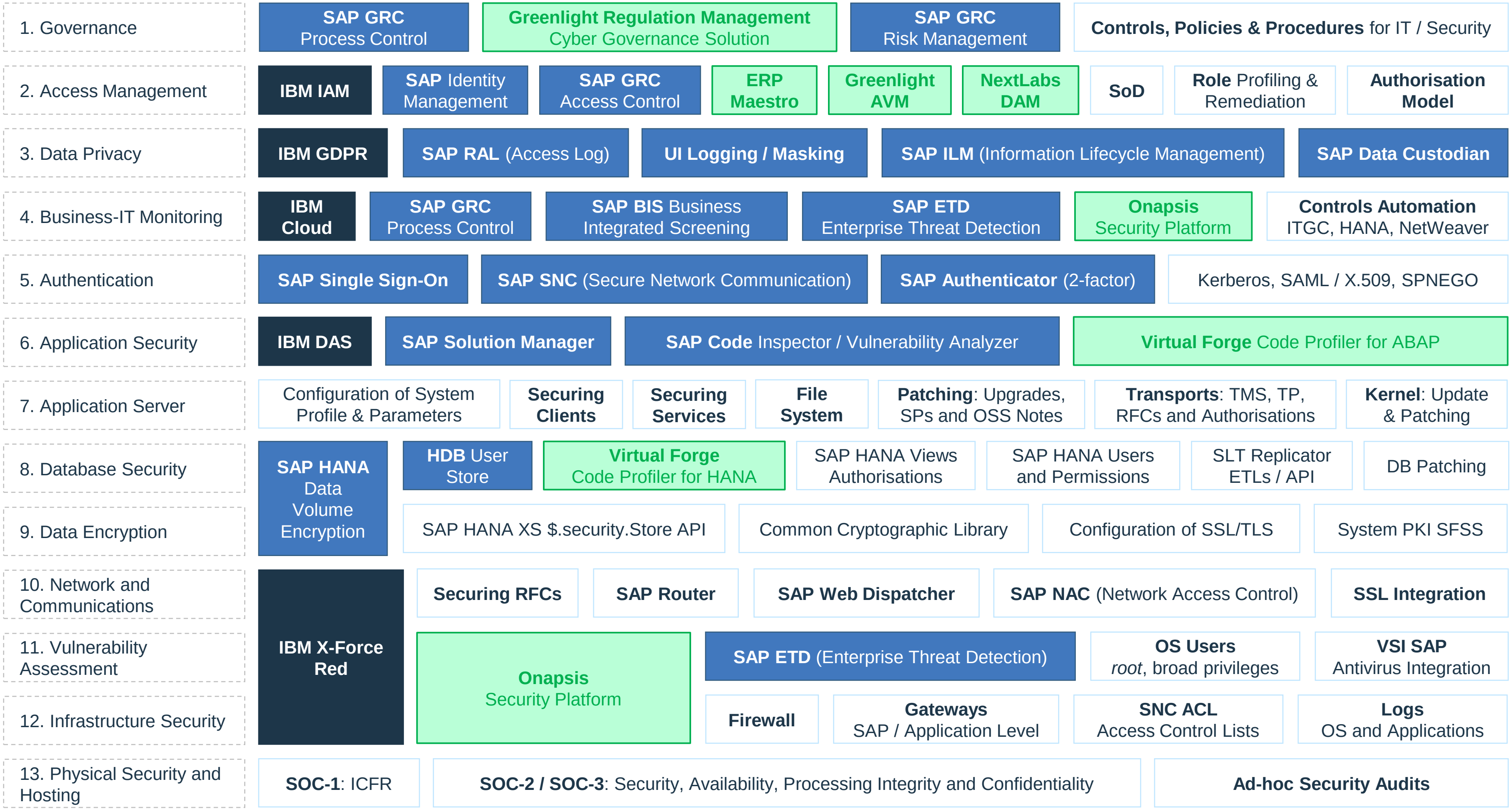
59% believe **Cloud, SAP HANA, SAP Fiori, IoT** all **increase likelihood** of an attack

Ponemon INSTITUTE

2. The 13 layers of SAP Security by IBM

IBM point of view of SAP Security

Security Layers	SAP product
Sub-competency	3rd Party product

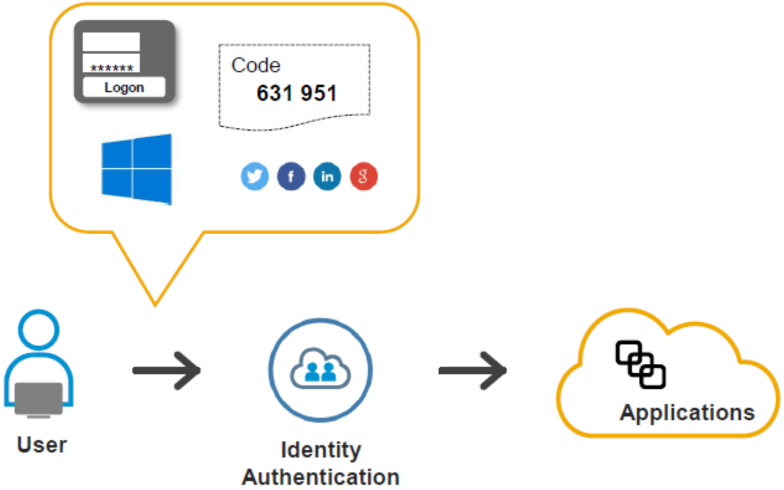


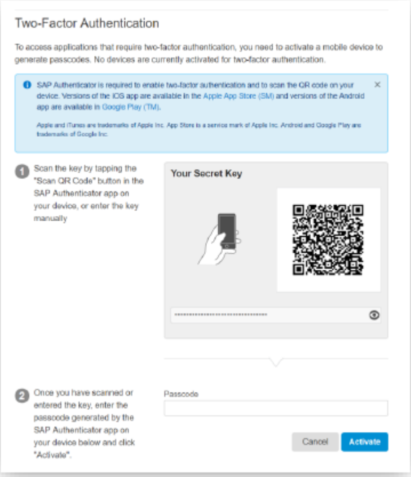
Layer	Components
1. Governance	**SAP GRC** Process Control **Greenlight Regulation Management** Cyber Governance Solution **SAP GRC** Risk Management **Controls, Policies & Procedures** for IT / Security
2. Access Management	**IBM IAM** **SAP** Identity Management **SAP GRC** Access Control **ERP Maestro** **Greenlight AVM** **NextLabs DAM** **SoD** **Role** Profiling & Remediation **Authorisation Model**
3. Data Privacy	**IBM GDPR** **SAP RAL** (Access Log) **UI Logging / Masking** **SAP ILM** (Information Lifecycle Management) **SAP Data Custodian**
4. Business-IT Monitoring	**IBM Cloud** **SAP GRC** Process Control **SAP BIS** Business Integrated Screening **SAP ETD** Enterprise Threat Detection **Onapsis** Security Platform **Controls Automation** ITGC, HANA, NetWeaver
5. Authentication	**SAP Single Sign-On** **SAP SNC** (Secure Network Communication) **SAP Authenticator** (2-factor) Kerberos, SAML / X.509, SPNEGO
6. Application Security	**IBM DAS** **SAP Solution Manager** **SAP Code** Inspector / Vulnerability Analyzer **Virtual Forge** Code Profiler for ABAP
7. Application Server	Configuration of System Profile & Parameters **Securing Clients** **Securing Services** **File System** **Patching**: Upgrades, SPs and OSS Notes **Transports**: TMS, TP, RFCs and Authorisations **Kernel**: Update & Patching
8. Database Security	**SAP HANA** Data Volume Encryption **HDB** User Store **Virtual Forge** Code Profiler for HANA SAP HANA Views Authorisations SAP HANA Users and Permissions SLT Replicator ETLs / API DB Patching
9. Data Encryption	SAP HANA XS $.security.Store API Common Cryptographic Library Configuration of SSL/TLS System PKI SFSS
10. Network and Communications	**IBM X-Force Red** **Securing RFCs** **SAP Router** **SAP Web Dispatcher** **SAP NAC** (Network Access Control) **SSL Integration**
11. Vulnerability Assessment	**Onapsis** Security Platform **SAP ETD** (Enterprise Threat Detection) **OS Users** *root*, broad privileges **VSI SAP** Antivirus Integration
12. Infrastructure Security	**Firewall** **Gateways** SAP / Application Level **SNC ACL** Access Control Lists **Logs** OS and Applications
13. Physical Security and Hosting	**SOC-1**: ICFR **SOC-2 / SOC-3**: Security, Availability, Processing Integrity and Confidentiality **Ad-hoc Security Audits**

2. The 13 layers of SAP Security by IBM

Layer 5 – Authentication: **Single Sign-On** (On-Premise and Cloud) and **Two Factor Authentication**

- Implementation of SAP Single Sign-On solutions
- Based on **On-Premise and Cloud** solutions (using **SAP Cloud Platform Identity Authentication Service**, IAS)
- Out-of-the-box integration with all applications supporting **SAML 2.0**
- Different authentication options:
  - **Basic authentication**: User ID / e-mail, and password
  - **Reuse of Windows Domain logon**: Use of Kerberos token for Single Sign-On
  - **Two Factor Authentication**: Second factor on mobile device
  - **Delegated Logon**: Social IdPs (Google, Facebook) or Corporate IdPs (IBM w3 Id)





Two-Factor Authentication

To access applications that require two-factor authentication, you need to activate a mobile device to generate passcodes. No devices are currently activated for two-factor authentication.

SAP Authenticator is required to enable two-factor authentication and to scan the QR code on your device. Versions of the iOS app are available in the Apple App Store (SM) and versions of the Android app are available in Google Play (TM).

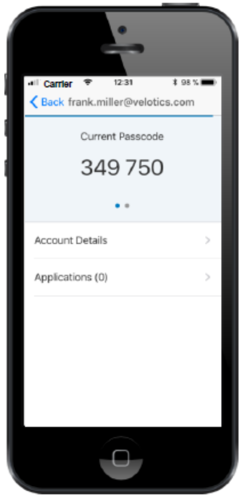
Apple and iTunes are trademarks of Apple Inc. App Store is a service mark of Apple Inc. Android and Google Play are trademarks of Google Inc.

1. Scan the key by tapping the "Scan QR Code" button in the SAP Authenticator app on your device, or enter the key manually

Your Secret Key

2. Once you have scanned or entered the key, enter the passcode generated by the SAP Authenticator app on your device below and click "Activate".

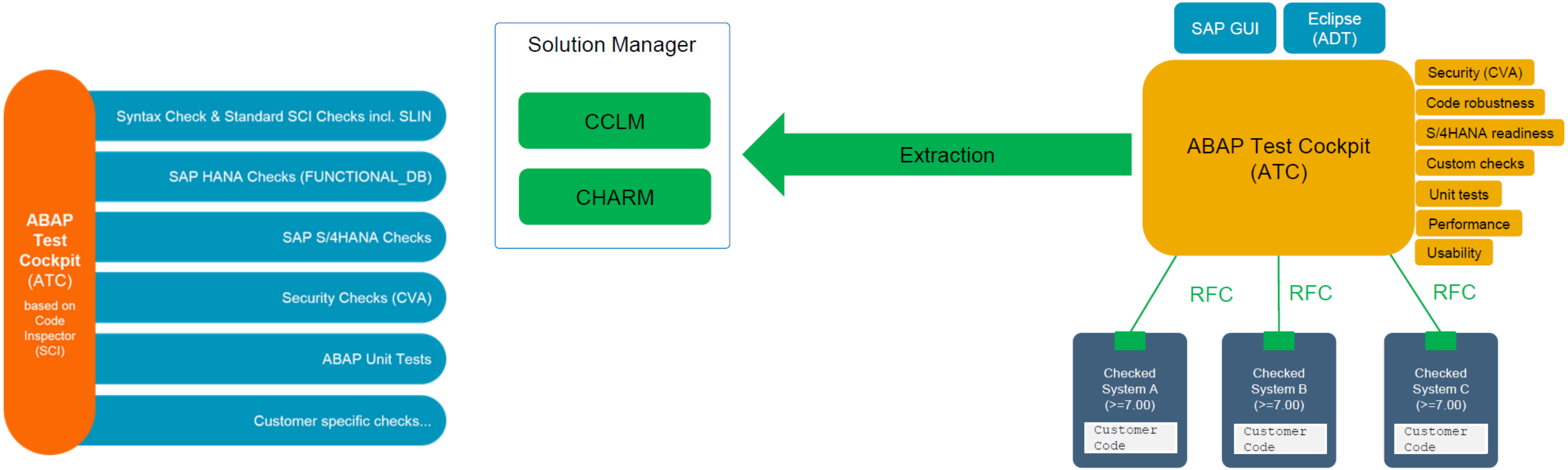
Passcode



2. The 13 layers of SAP Security by IBM

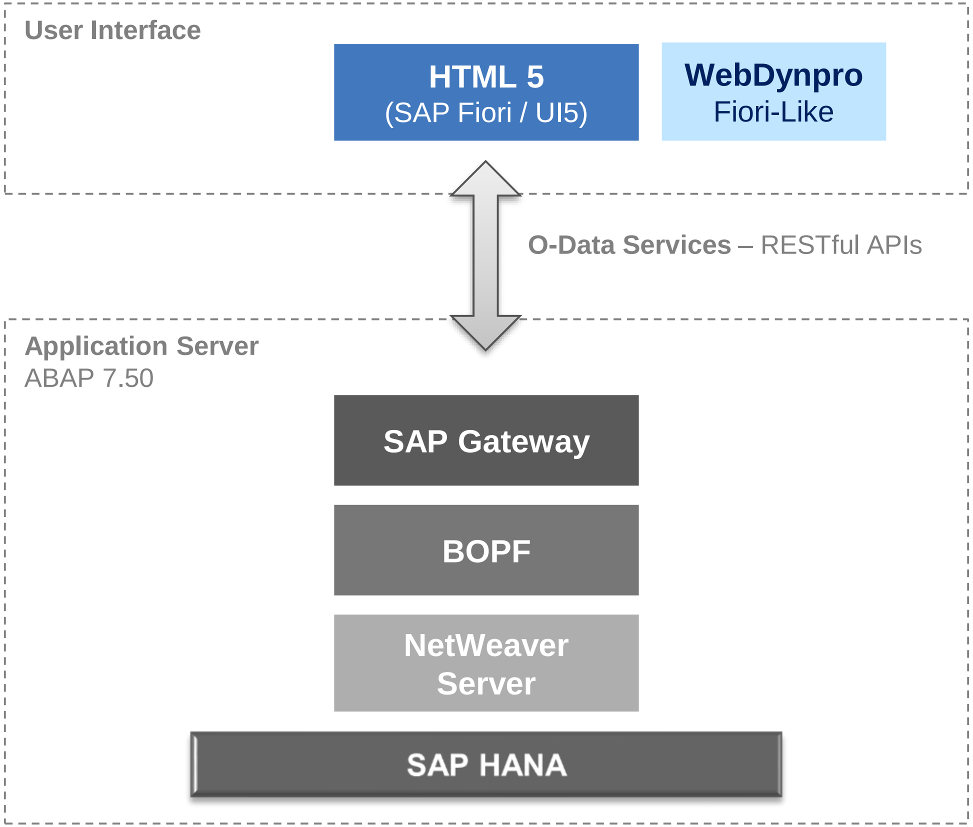
Layer 6 – Application Security: Based on **Code Inspector** and **Code Vulnerability Analyzer** (CVA)

- Implementation of **Code Scanning platforms** based on the integration of **SAP Code Inspector** and **SAP Code Vulnerability Analyzer (CVA)** for the enablement of an **ABAP Test Cockpit**, that allows the execution of remote code analysis from a central instance to detect performance and security issues over custom source code.
- This approach can be implemented on-premise for the customer, or provided as a service, from a central IBM instance.
- The usage of a central instance only requires a NetWeaver 7.51 system, with RFCs with the target systems



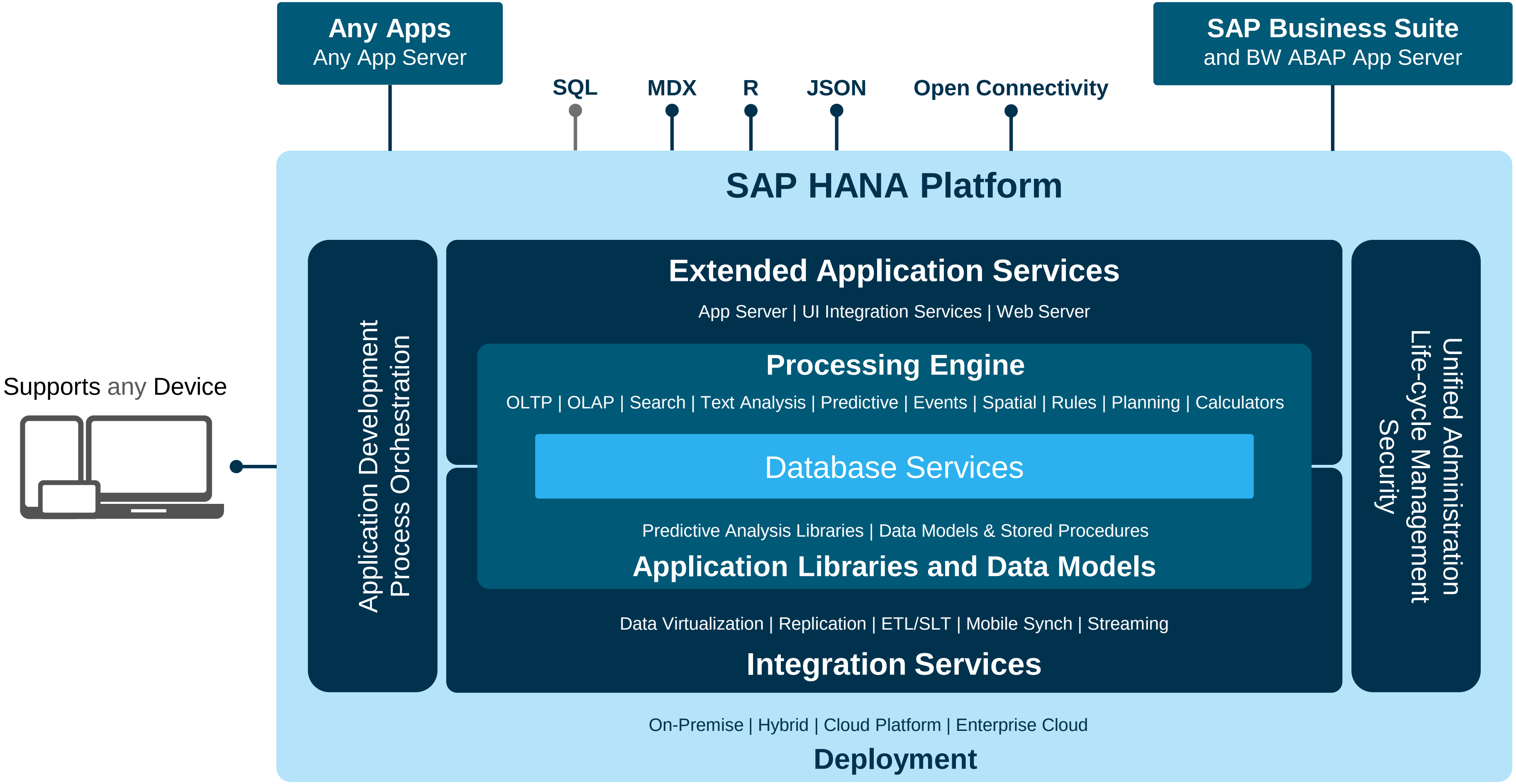
2. The 13 layers of SAP Security by IBM

Layer 7 – Application Server: How does it affect the new S/4 architecture to SAP Security?



2. The 13 layers of SAP Security by IBM

Layer 8 – Data Base Security: SAP HANA



Any Apps
Any App Server

SAP Business Suite
and BW ABAP App Server

SQL
MDX
R
JSON
Open Connectivity

Supports any Device

SAP HANA Platform

Application Development
Process Orchestration

Extended Application Services
App Server | UI Integration Services | Web Server

Processing Engine
OLTP | OLAP | Search | Text Analysis | Predictive | Events | Spatial | Rules | Planning | Calculators

Database Services

Predictive Analysis Libraries | Data Models & Stored Procedures
Application Libraries and Data Models

Data Virtualization | Replication | ETL/SLT | Mobile Synch | Streaming
Integration Services

Unified Administration
Life-cycle Management
Security

On-Premise | Hybrid | Cloud Platform | Enterprise Cloud
Deployment

2. The 13 layers of SAP Security by IBM

Layer 8 – Data Base Security: **SAP HANA**

❑ **Companies are migrating their "crown jewels" to the SAP HANA platform**. This includes:

- Enterprise-Critical and Financial data
- Executive data including plans for M&A, divestitures, executive hires, etc.
- Regulated data including personally identifiable information (PII) of customers, vendors, and employees

❑ **Data** that resided in multiple systems **now exists in only one repository**

❑ Customers are **leveraging SAP HANA's data compatibility** features and by integrating streaming data, Hadoop, and data from many other sources…

❑ **Security layers removed** → **Security now resides at the HANA layer, not the application layer**

- The **challenge** from a security viewpoint is that **users and applications now have direct access to the database**
- Database security represents the last line of defense for enterprise data

❑ **Incorrect authorizations assigned to users and roles**

- Elevated privileges could **allow direct changes to tables, views, and stored procedures**

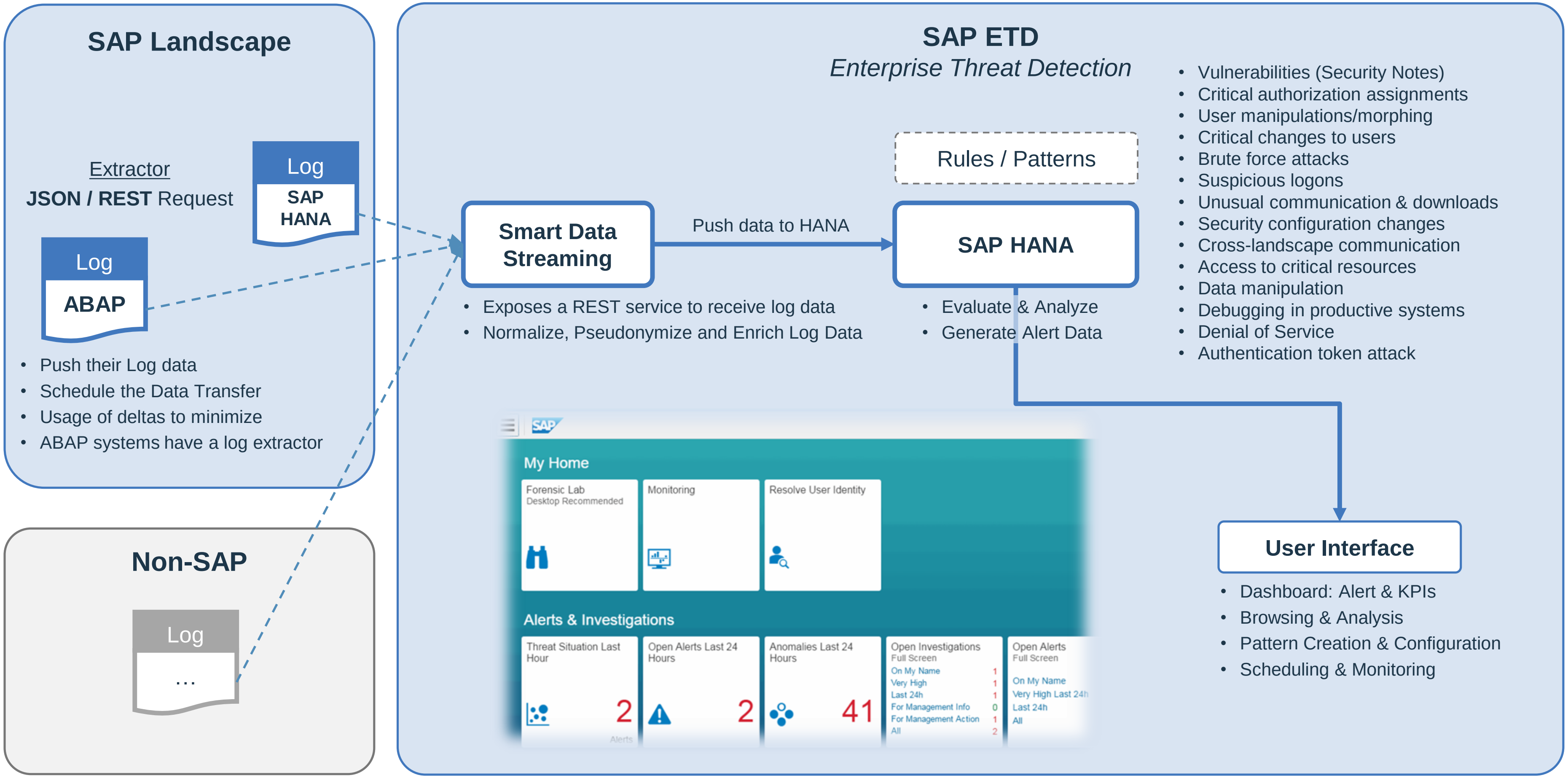
❑ Unauthorized access **more prevalent now than ever**

- SAP HANA is a **key focus area for targeted and insider attacks**

❑ **SAP HANA is now an "in scope" system from an internal and external audit standpoint**

2. The 13 layers of SAP Security by IBM

Layer 11 – Vulnerability Assessment: **SAP Enterprise Threat Detection** (ETD) – Security Breaches



SAP Landscape

Extractor
JSON / REST Request

- Push their Log data
- Schedule the Data Transfer
- Usage of deltas to minimize
- ABAP systems have a log extractor

Non-SAP

SAP ETD

Enterprise Threat Detection

Smart Data Streaming

- Exposes a REST service to receive log data
- Normalize, Pseudonymize and Enrich Log Data

SAP HANA

- Evaluate & Analyze
- Generate Alert Data

- Vulnerabilities (Security Notes)
- Critical authorization assignments
- User manipulations/morphing
- Critical changes to users
- Brute force attacks
- Suspicious logons
- Unusual communication & downloads
- Security configuration changes
- Cross-landscape communication
- Access to critical resources
- Data manipulation
- Debugging in productive systems
- Denial of Service
- Authentication token attack

Open Investigations	
On My Name	1
Very High	1
Last 24h	1
For Management Info	0
For Management Action	1
All	2

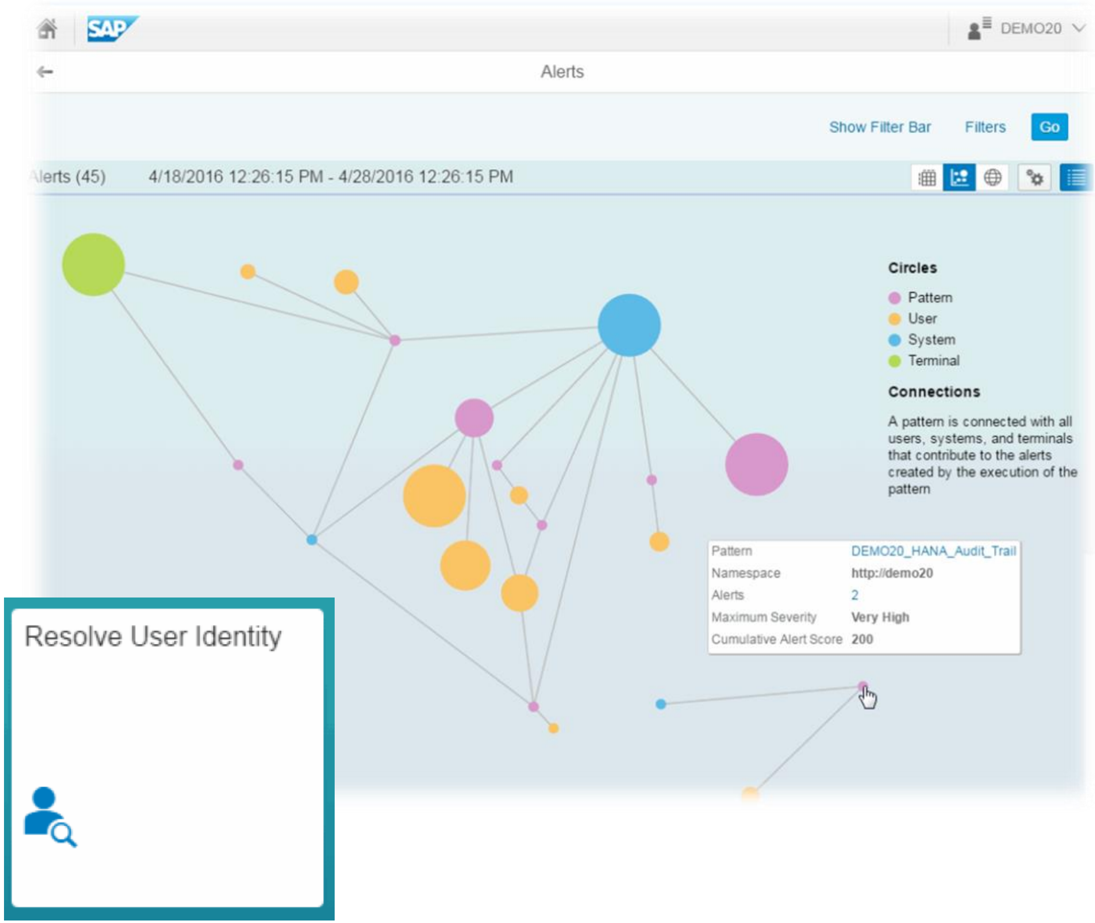
Open Alerts: On My Name, Very High Last 24h, Last 24h, All

User Interface

- Dashboard: Alert & KPIs
- Browsing & Analysis
- Pattern Creation & Configuration
- Scheduling & Monitoring

2. The 13 layers of SAP Security by IBM

Layer 11 – Vulnerability Assessment: **SAP Enterprise Threat Detection** (ETD) – Security Breaches



Circles

- ● Pattern
- ● User
- ● System
- ● Terminal

Connections

A pattern is connected with all users, systems, and terminals that contribute to the alerts created by the execution of the pattern

Pattern	DEMO20_HANA_Audit_Trail
Namespace	http://demo20
Alerts	2
Maximum Severity	Very High
Cumulative Alert Score	200

Forensic Lab

- Apply **filters to the normalized Log data** stored in the SAP HANA database.
- The **set of filters** user in the investigation is known as "path"
- The system allows visualize (in many ways) the filtered data to look for **standout values**
- Applying **predefined heuristic rules** (*modifiable*), can generate attack detection patterns from paths
- Based on defined thresholds, the system will show the **alerts**
- If the alert shows consistency to be true, then **data can be un-pseudonymized** to resolve user identity

3. CCM in Technical SAP Security

CCM principle can also be applied to SAP Security

3. CCM in Technical SAP Security

This concept can also be applied to the Technical SAP Security

SAP Process Control
CCM
1 single automatic control

SAP BIS
Advanced CCM
“n” automatic controls combined

SAP Enterprise Threat Detection
Advanced CCM

SAP HANA
DB and Sidecar that replicates SAP tables

IBM Security

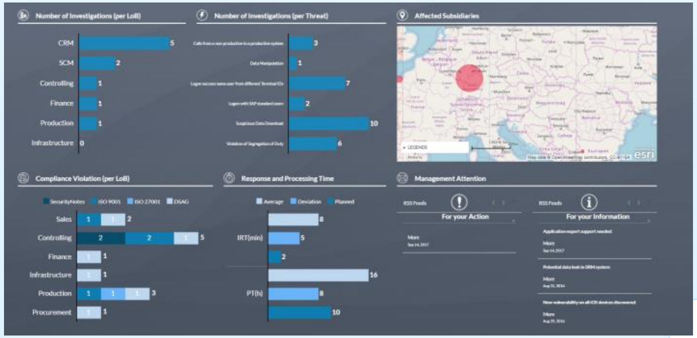
IBM SECURITY SCAN FOR SAP

Set of Controls to be Automated:
- IT General Controls (ITGCs)
- SAP Fiori
- SAP Netweaver
- SAP Gateway
- HANA Security
- RFCs

Europe CoC SAP Security & GRC
Madrid

September 28th, 2018

IBM


Number of Investigations (per LoB)
CRM 5
SCM 2
Controlling 1
Finance 1
Production 1
Infrastructure 0
Number of Investigations (per Threat)
Calls from a non-productive to a productive system 3
Data Manipulation 1
Logon success same user from different Terminal IDs 7
Logon with SAP standard users 2
Suspicious Data Download 10
Violation of Segregation of Duty 6
Affected Subsidiaries
LEGENDS
esri
Compliance Violation (per LoB)
SecurityNotes
ISO 9001
ISO 27001
DSAG
Sales 1 1 2
Controlling 2 2 1 5
Finance 1 1
Infrastructure 1 1
Production 1 1 1 3
Procurement 1 1
Response and Processing Time
Average
Deviation
Planned
IRT(min) 8 5 2
PT(h) 16 8 10
Management Attention
RSS Feeds
For your Action
For your Information
Application expert support needed
Potential data leak in SRM system
New vulnerability on all ICS devices discovered
More

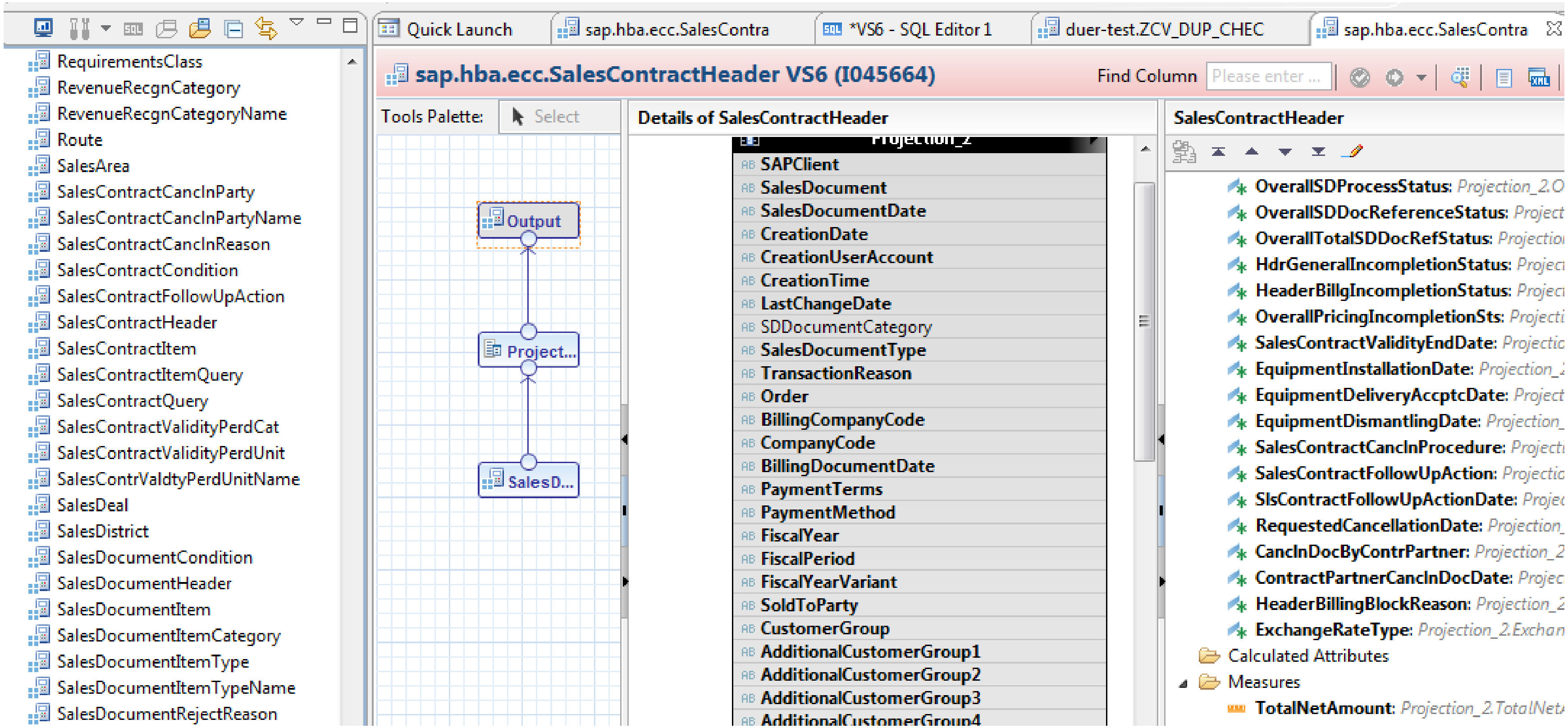
Security Dashboard
(SAP Analytics Cloud / SAP Digital Boardroom)

SAP
Customer
HANA powered

3. CCM in Technical SAP Security

SAP GRC Process Control

- SAP Process Control 12.0 allows the usage of the **SAP HANA Studio modeler** to create new HANA views that can be used as GRC PC business rules, or reuse existing previous existing HANA views that were not specifically created SAP Process Control



Quick Launch | sap.hba.ecc.SalesContra | *VS6 - SQL Editor 1 | duer-test.ZCV_DUP_CHEC | sap.hba.ecc.SalesContra

RequirementsClass
RevenueRecgnCategory
RevenueRecgnCategoryName
Route
SalesArea
SalesContractCanclnParty
SalesContractCanclnPartyName
SalesContractCanclnReason
SalesContractCondition
SalesContractFollowUpAction
SalesContractHeader
SalesContractItem
SalesContractItemQuery
SalesContractQuery
SalesContractValidityPerdCat
SalesContractValidityPerdUnit
SalesContrValdtyPerdUnitName
SalesDeal
SalesDistrict
SalesDocumentCondition
SalesDocumentHeader
SalesDocumentItem
SalesDocumentItemCategory
SalesDocumentItemType
SalesDocumentItemTypeName
SalesDocumentRejectReason

sap.hba.ecc.SalesContractHeader VS6 (I045664)

Find Column: Please enter ...

Tools Palette: Select

Details of SalesContractHeader

Projection_2

SAPClient
SalesDocument
SalesDocumentDate
CreationDate
CreationUserAccount
CreationTime
LastChangeDate
SDDocumentCategory
SalesDocumentType
TransactionReason
Order
BillingCompanyCode
CompanyCode
BillingDocumentDate
PaymentTerms
PaymentMethod
FiscalYear
FiscalPeriod
FiscalYearVariant
SoldToParty
CustomerGroup
AdditionalCustomerGroup1
AdditionalCustomerGroup2
AdditionalCustomerGroup3
AdditionalCustomerGroup4

SalesContractHeader

OverallSDProcessStatus: Projection_2.O
OverallSDDocReferenceStatus: Project
OverallTotalSDDocRefStatus: Projectio
HdrGeneralIncompletionStatus: Projec
HeaderBillgIncompletionStatus: Projec
OverallPricingIncompletionSts: Projecti
SalesContractValidityEndDate: Projectic
EquipmentInstallationDate: Projection_
EquipmentDeliveryAccptcDate: Project
EquipmentDismantlingDate: Projection_
SalesContractCanclnProcedure: Projecti
SalesContractFollowUpAction: Projectic
SlsContractFollowUpActionDate: Projec
RequestedCancellationDate: Projection_
CanclnDocByContrPartner: Projection_2
ContractPartnerCanclnDocDate: Projec
HeaderBillingBlockReason: Projection_2
ExchangeRateType: Projection_2.Exchan
Calculated Attributes
Measures
TotalNetAmount: Projection_2.TotalNet

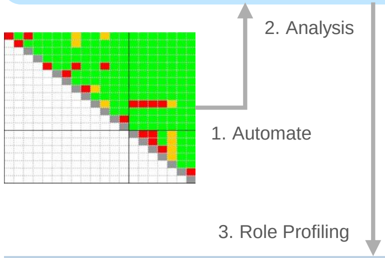
4. The new wave of Access Management

The Hybrid Compliant Identity Management (HCIdM)

4. The new wave of Access Management

SAP Access Control (GRC) – Main modules and functionalities

ARA
Access Risk Analysis



Warehouse Processing

Material Documents Overview

Post Goods Receipt for Purchase Order

Transfer Stock In-Plant

Post Goods Movement

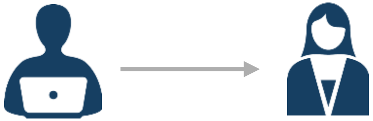
Output Material Documents

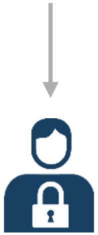
Transfer Stock Cross-Plant

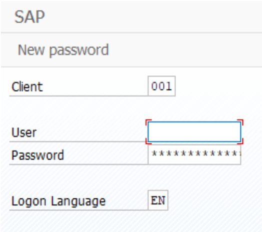
- Provides ad-hoc and WF driven SoD checks to ensure roles and UMR free of segregation of duties conflicts
- Standard SoD rule-set provided that includes S4 and Fiori apps
- Customised rule-sets are allowed

Get Clean

EAM
Emergency Access Management






SAP

New password

Client 001

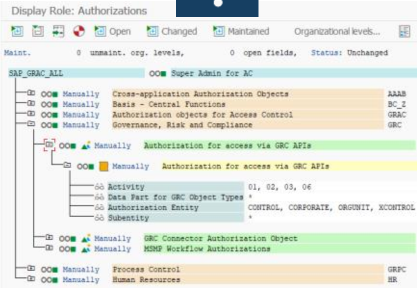
User

Password ***********

Logon Language EN

- Provides Firefighting functionalities to users that require an high-privileged access during a limited period of time
- All the activities are recorded and can be reviewed by the FF Controller
- Firefighting management in SAP is the #1 issue in all audit reports

BRM
Business Role Management

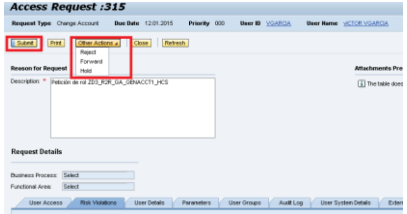

Display Role: Authorizations

```
Maint.          0  unmaint. org. levels,        0  open fields,   Status: Unchanged

SAP_GRAC_ALL              OO■ Super Admin for AC
  OO■ Manually   Cross-application Authorization Objects               AAAB
  OO■ Manually   Basis - Central Functions                             BC_Z
  OO■ Manually   Authorization objects for Access Control              GRAC
  OO■ Manually   Governance, Risk and Compliance                       GRC
     OO■ Manually   Authorization for access via GRC APIs
        OO■ Manually   Authorization for access via GRC APIs
              Activity                           01, 02, 03, 06
              Data Part for GRC Object Types     *
              Authorization Entity               CONTROL, CORPORATE, ORGUNIT, XCONTROL
              Subentity                          *
     OO■ Manually   GRC Connector Authorization Object
     OO■ Manually   MSMP Workflow Authorizations
  OO■ Manually   Process Control                                       GRPC
  OO■ Manually   Human Resources                                       HR
```

- Replaces the usage of PFCG t-code to manage SAP roles and profiles
- Does a prior check in ARA before each modification done in SAP roles
- Introduces new functionalities, as automatic naming convention, role classification in customized hierarchy, and "Business Roles" as an Identity

ARM
Access Request Management


Access Request :315

Request Type Change Account Due Date 12.01.2015 Priority 000 User ID VGARCIA User Name VICTOR VGARCIA

Reason for Request

Description: * Petición de rol ZD3_R2R_GA_GENACCT1_HCS

Attachments Pre

The table does

Request Details

Business Process: Select

Functional Area: Select

- Replaces the usage of SU01 t-code to manage SAP users
- Does a prior check in ARA before each modification done to UMR
- Introduces a WF driven provisioning process that manages single roles, composite roles and business roles, similarly as an IAM solution

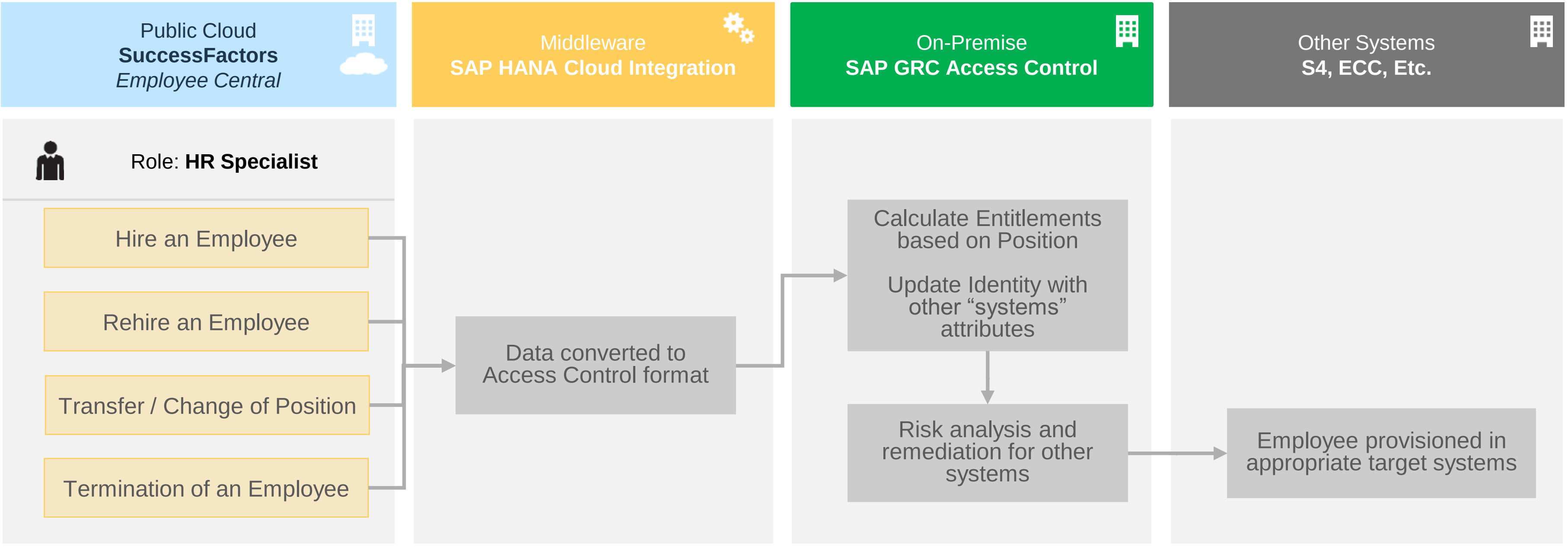
Real-Time Compliance → Continuous Monitoring that avoid generate new SoD conflicts

Stay Clean

4. The new wave of Access Management

Integration of **SAP Access Control** with **SAP SuccessFactors** (Employee Central Driven Process)

- Success Factors (Employee Central) can start and drive the provisioning / deprovisioning process, but adding the connectivity with SAP GRC Access Control via SAP HANA Cloud Integration.
- This process ensures a provision free of SoD conflicts for all the SAP systems in-scope.



Public Cloud
SuccessFactors
Employee Central

Middleware
SAP HANA Cloud Integration

On-Premise
SAP GRC Access Control

Other Systems
S4, ECC, Etc.

Role: **HR Specialist**

Hire an Employee

Rehire an Employee

Transfer / Change of Position

Termination of an Employee

Data converted to Access Control format

Calculate Entitlements based on Position

Update Identity with other "systems" attributes

Risk analysis and remediation for other systems

Employee provisioned in appropriate target systems

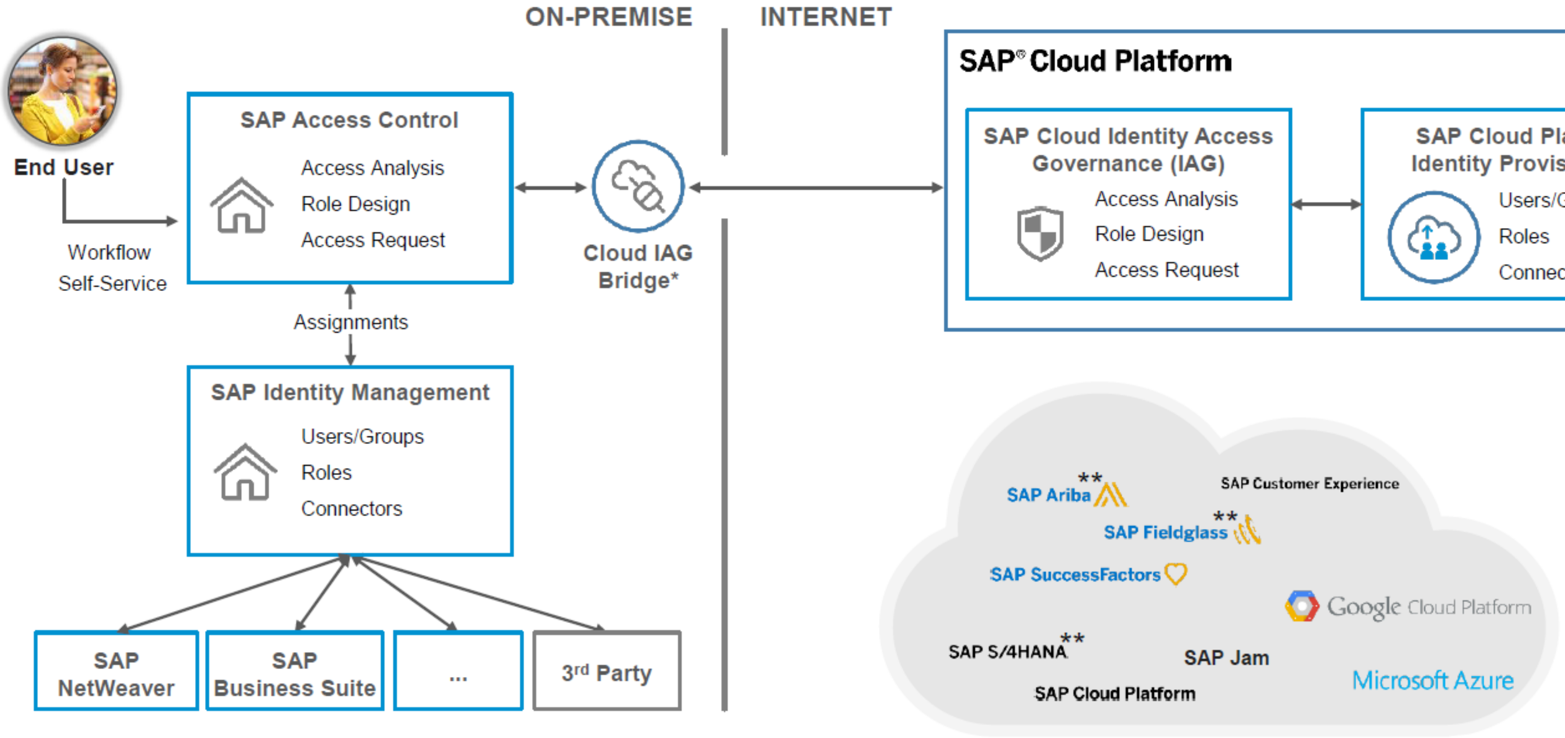
Legend: Process step (mainly manual) | Process step (mainly automatic)

* Examples (illustrative) – uses employee master data

4. The new wave of Access Management

Hybrid **Compliant** Identity and Access Provisioning: SAP IDM + SAP Access Control

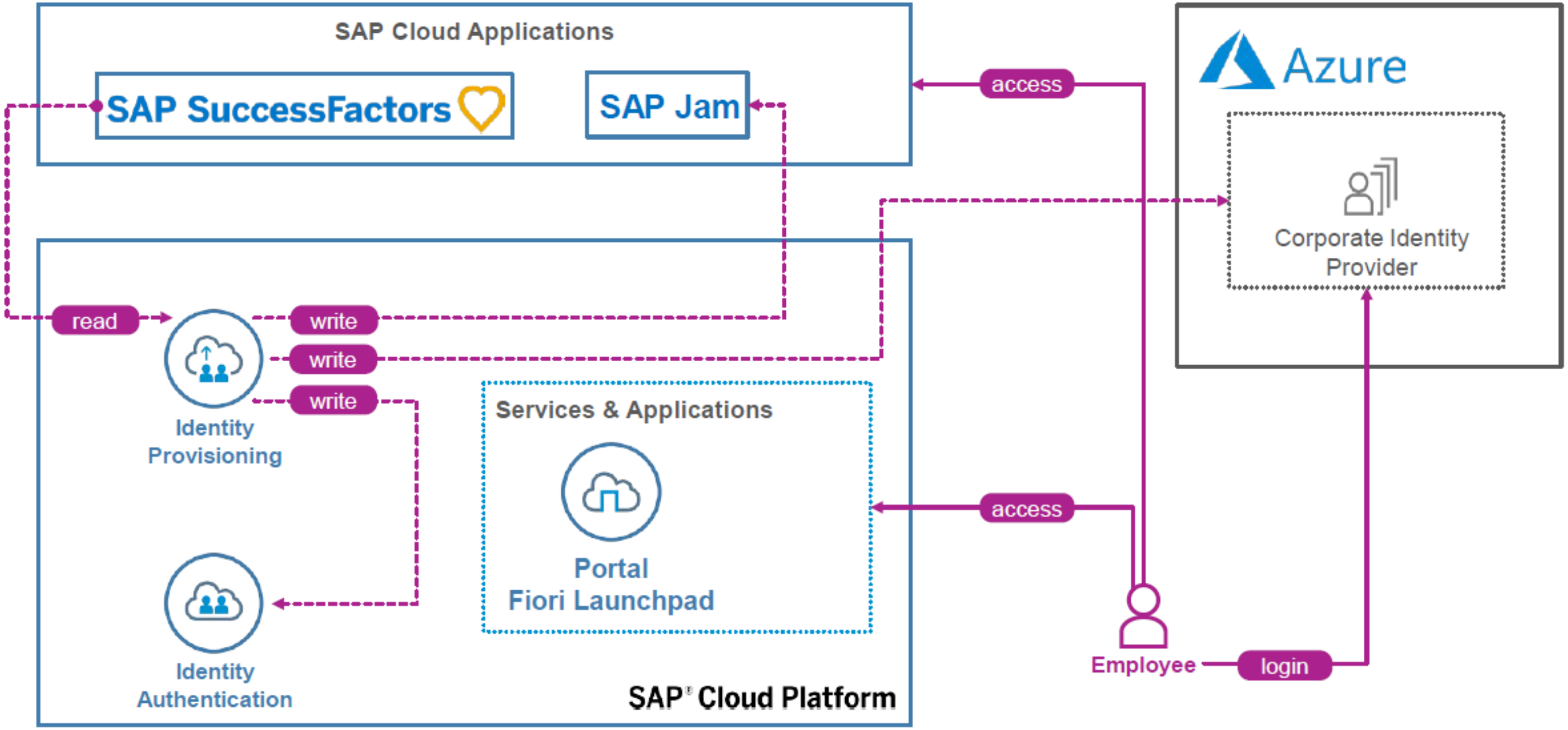
- The following is the recommended landscape for an Hybrid **Compliant** Identity Management approach
- In this scenario SAP Access Control is connected to the on-premise SAP Identity Management, and also to the Cloud IAG Bridge, to provide SoD checks for on-premise and cloud applications respectively



4. The new wave of Access Management

SuccessFactors driven provisioning process with a Corporate Identity Provider (Azure LDAP)

- The following shows an approach based on the usage of SAP SuccessFactors (as we have seen in Employee Central for SAP GRC) to drive the provisioning process, reading and updating information from / to the Azure LDAP



5. Changes in the SAP S/4HANA Authorization Model

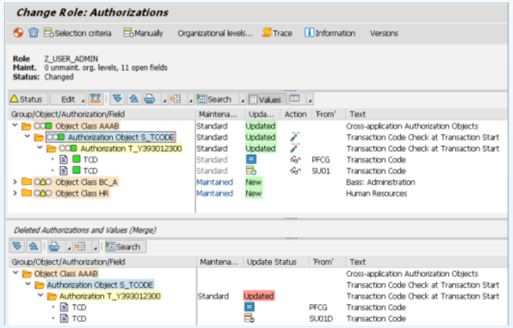
How does it change the SAP authorizations management in S/4?

5. Changes in the SAP S/4HANA Authorization Model

Authorizations in SAP S/4HANA Cloud

SAP S/4HANA Cloud (Public SAP Cloud)

- There is no **PFCG** t-code
- The **permissions** are managed directly through Fiori apps
- Hierarchical structure of authorizations:
  - ❑ **Business Users**
  - ❑ **Business Roles** (E.g. Sales Manager)
  - ❑ **Business Catalogs** (E.g. Sales Order Processing)
  - ❑ **Permissions** – Write (W) / Read (R) – (E.g. Sales Organization)

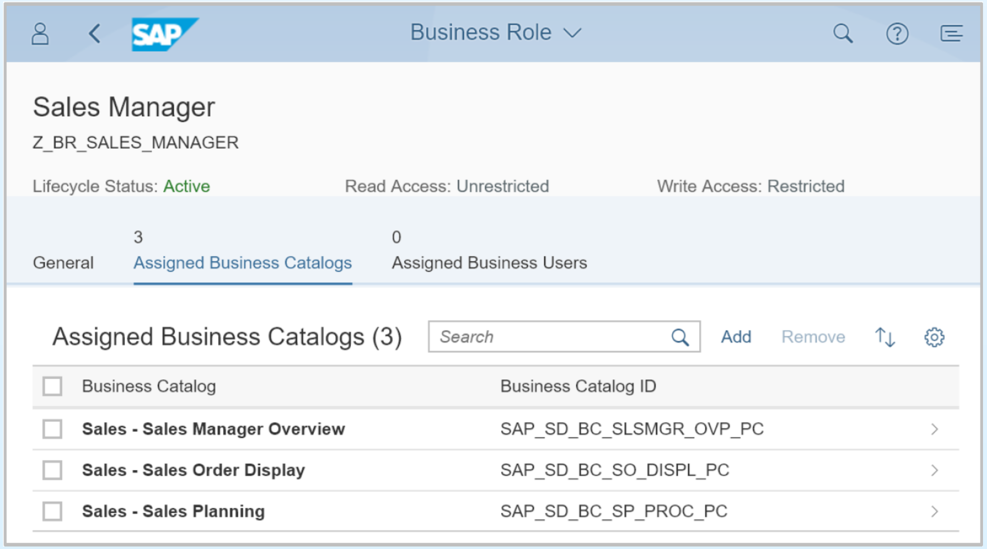


Role Z_USER_ADMIN
Maint. 0 unmaint. org. levels, 11 open fields
Status: Changed

Group/Object/Authorization/Field	Maintena...	Upda...	Action	'From'	Text
Object Class AAAB	Standard	Updated			Cross-application Authorization Objects
Authorization Object S_TCODE	Standard	Updated			Transaction Code Check at Transaction Start
Authorization T_Y393012300	Standard	Updated			Transaction Code Check at Transaction Start
TCD	Standard			PFCG	Transaction Code
TCD	Standard			SU01	Transaction Code
Object Class BC_A	Maintained	New			Basis: Administration
Object Class HR	Maintained	New			Human Resources

Deleted Authorizations and Values (Merge)

Group/Object/Authorization/Field	Maintena...	Update Status	'From'	Text
Object Class AAAB				Cross-application Authorization Objects
Authorization Object S_TCODE				Transaction Code Check at Transaction Start
Authorization T_Y393012300	Standard	Updated		Transaction Code Check at Transaction Start
TCD			PFCG	Transaction Code
TCD			SU01D	Transaction Code



Sales Manager
Z_BR_SALES_MANAGER

Lifecycle Status: Active   Read Access: Unrestricted   Write Access: Restricted

General   3 Assigned Business Catalogs   0 Assigned Business Users

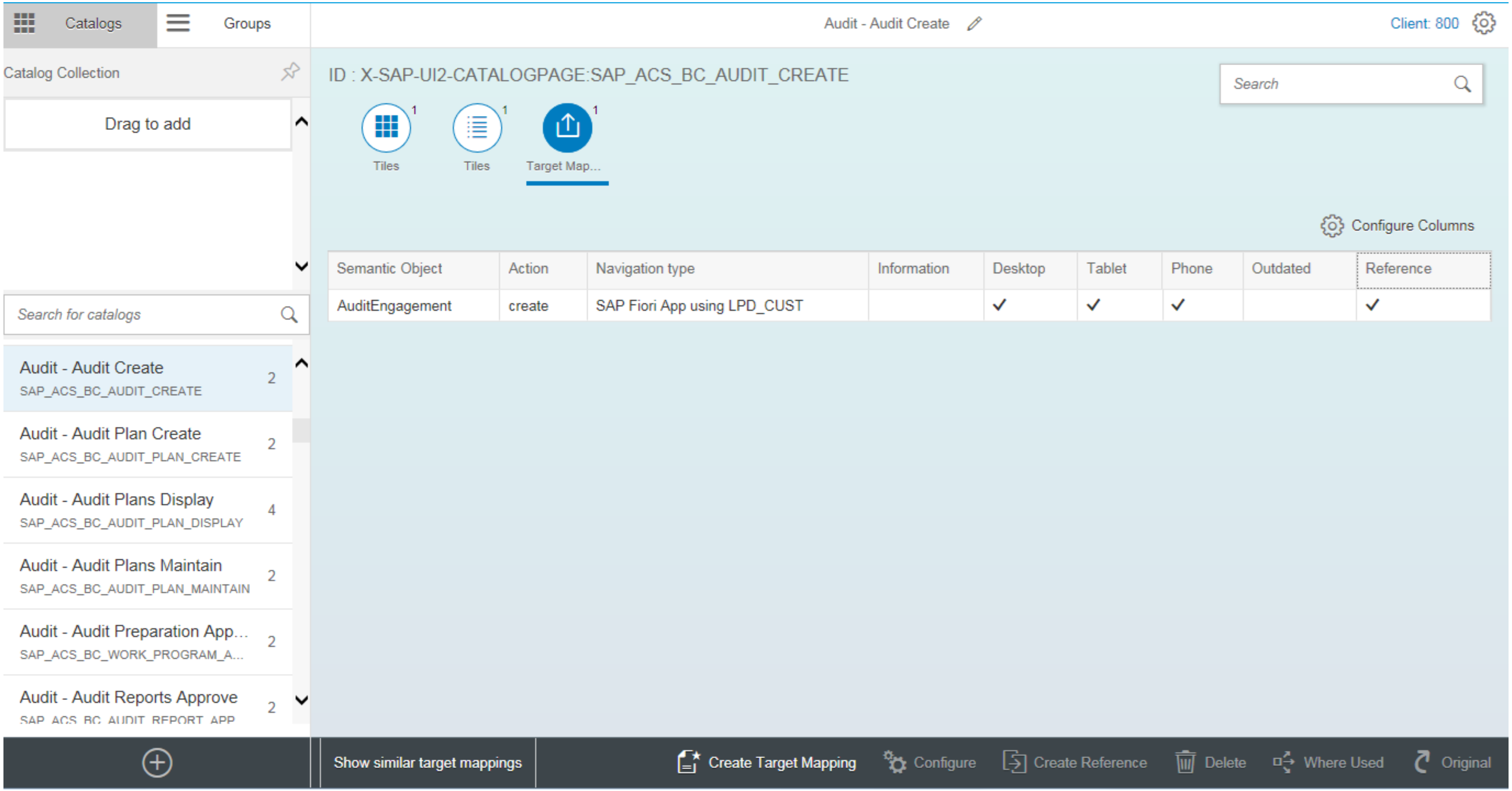
Assigned Business Catalogs (3)   Search

	Business Catalog	Business Catalog ID
□	**Sales - Sales Manager Overview**	SAP_SD_BC_SLSMGR_OVP_PC
□	**Sales - Sales Order Display**	SAP_SD_BC_SO_DISPL_PC
□	**Sales - Sales Planning**	SAP_SD_BC_SP_PROC_PC

- How is authorization management?
  - ❑ Creation of **Business Roles** taking advantage of the templates provided by SAP
  - ❑ Modify assignment to **Business Catalogs**
  - ❑ Restrict **Permissions** (W/R)
  - ❑ Assign **Business Roles** to **Users**
- The underlying idea is that **SAP provides a PFCG role** per each **Business Catalog**
- The **Business Roles** determine the access to the different applications, reading those from the Business Catalogs

5. Changes in the SAP S/4HANA Authorization Model

SAP Fiori UI5 Launchpad Designer



ID : X-SAP-UI2-CATALOGPAGE:SAP_ACS_BC_AUDIT_CREATE

Semantic Object	Action	Navigation type	Information	Desktop	Tablet	Phone	Outdated	Reference
AuditEngagement	create	SAP Fiori App using LPD_CUST		✓	✓	✓		✓

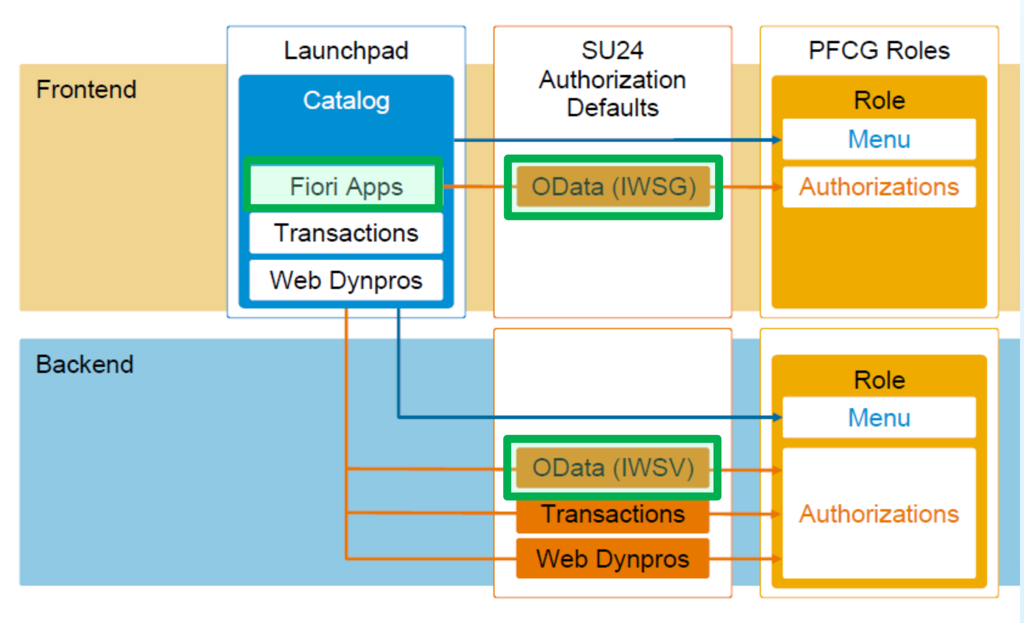
Audit - Audit Create SAP_ACS_BC_AUDIT_CREATE	2
Audit - Audit Plan Create SAP_ACS_BC_AUDIT_PLAN_CREATE	2
Audit - Audit Plans Display SAP_ACS_BC_AUDIT_PLAN_DISPLAY	4
Audit - Audit Plans Maintain SAP_ACS_BC_AUDIT_PLAN_MAINTAIN	2
Audit - Audit Preparation App... SAP_ACS_BC_WORK_PROGRAM_A...	2
Audit - Audit Reports Approve SAP_ACS_BC_AUDIT_REPORT_APP	2

5. Changes in the SAP S/4HANA Authorization Model

Authorizations in SAP S/4HANA On-premise

SAP S/4HANA On-premise (Private / Hybrid Cloud)

- Yes! There is the **PFCG** t-code
- It brings an hybrid authorization model, that mixes “the old” and “**the new**”…



Launchpad

SU24 Authorization Defaults

PFCG Roles

Frontend

Catalog

Fiori Apps

Transactions

Web Dynpros

OData (IWSG)

Role

Menu

Authorizations

Backend

OData (IWSV)

Transactions

Web Dynpros

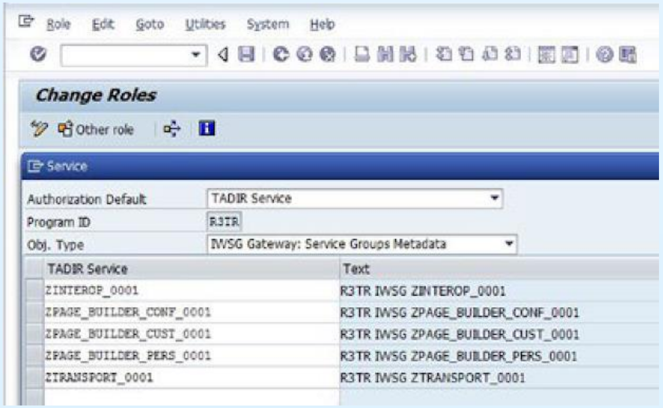
Role

Menu

Authorizations

New components in PFCG roles:

- Menu → Authorization Default: TADIR
- Program ID: R3TR
- Object Type: (OData Services)
  - IWSG – Gateway Service Group Metadata
  - IWSV – Gateway Business Suite Enablement Service



Authorization Default	TADIR Service
Program ID	R3TR
Obj. Type	IWSG Gateway: Service Groups Metadata

TADIR Service	Text
ZINTEROP_0001	R3TR IWSG ZINTEROP_0001
ZPAGE_BUILDER_CONF_0001	R3TR IWSG ZPAGE_BUILDER_CONF_0001
ZPAGE_BUILDER_CUST_0001	R3TR IWSG ZPAGE_BUILDER_CUST_0001
ZPAGE_BUILDER_PERS_0001	R3TR IWSG ZPAGE_BUILDER_PERS_0001
ZTRANSPORT_0001	R3TR IWSG ZTRANSPORT_0001

5. Changes in the SAP S/4HANA Authorization Model

So… How I am going to manage now my authorizations model with SAP S/4HANA?

Greenfield implementation

- Standard roles provided by SAP
- Roles provided by consulting firms, as the ones included in the “IBM Impact” template

Bluefield / Brownfield implementation

- Keep the “old” client roles, doing some adjustments to include new S/4 functionalities
- Add “Business Catalogs” on-top of the old client roles, to enable new “SAP Fiori” functionalities

6. Q&A

Questions & Answers

6. Q&A

Questions and Answers

IBM Contacts

Victor Garcia Rodriguez

- Associate Partner
- Phone: +34 682 38 44 08
- Mail: victor.garcia.rodriguez@ibm.com

Raffaella Cannone

- Managing Consultant
- Phone:+39 349 6075255
- Mail: raffaella.cannone@it.ibm.com

IBM Security

THANK YOU!

SÍGUENOS EN:

ibm.com/security

securityintelligence.com

xforce.ibmcloud.com

@ibmsecurity

youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.