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
# Table of Contents

The 13 layers of SAP Security by IBM

- **SAP Security: The other side of the Compliance “coin”** [3]
- **The 13 layers of SAP Security** [7]
- **Continuous Control Monitoring in SAP Security** [17]
- **The new wave of Access Management** [20]
- **Changes in the SAP S/4HANA Authorization Model** [25]
- **Questions & Answers** [30]
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

<table>
<thead>
<tr>
<th>1. Governance</th>
<th>Internal Control, Internal Audit, Enterprise Risk and Regulation Affairs: Integration and Automation of the Three Lines of Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Access Management</td>
<td>Segregation of Duties, Identity and Role Management: User Access complying with Regulatory Requirements (E.g. SOX)</td>
</tr>
<tr>
<td>3. Data Privacy</td>
<td>GDPR (and others): Data Retention and Data Deletion, Data Portability, Data Field Masking, Access Logging to Personal Data</td>
</tr>
<tr>
<td>7. Application Server</td>
<td>SAP Server configuration: Security Parameters of all Clients // Secured Services // Patching Level // OSS Notes</td>
</tr>
<tr>
<td>8. Database Security</td>
<td>SAP HANA: Secured access to SAP HANA Views and Schemas // Integration with data lakes // Ensure no open paths to access data</td>
</tr>
<tr>
<td>11. Vulnerability Assessment</td>
<td>OS users (broad privileges) // SAP log analysis and integration with SIEM solution // Integration of antivirus into SAP</td>
</tr>
<tr>
<td>12. Infrastructure Security</td>
<td>Configuration of physical / logical devices: Firewall and Gateways // OS and Applications Logs</td>
</tr>
<tr>
<td>13. Physical Security and Hosting</td>
<td>Standard Controls Coverage (SOC reports) // Compliance Level of each Cloud platform // Ad-hoc Security audits // Physical hacking</td>
</tr>
</tbody>
</table>
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

- **92%** indicated an SAP breach would be serious, very serious or catastrophic.
- **65%** said their SAP System was breached at least once in the past 24 months.
- Average cost to take SAP offline was **$4.5M** per incident.
- **47%** indicated they were “not confident” or had “no confidence” that they could detect an SAP breach within a year.
- **59%** believe Cloud, SAP HANA, SAP Fiori, IoT all increase likelihood of an attack.

Ponemon Institute


- **92%** indicated an SAP breach would be serious, very serious or catastrophic.
- **65%** said their SAP System was breached at least once in the past 24 months.
- Average cost to take SAP offline was **$4.5M** per incident.
- **47%** indicated they were “not confident” or had “no confidence” that they could detect an SAP breach within a year.
- **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

1. Governance
   - SAP GRC Process Control
   - Greenlight Regulation Management Cyber Governance Solution
   - SAP GRC Risk Management

2. Access Management
   - IBM IAM
   - SAP Identity Management
   - SAP GRC Access Control
   - ERP Maestro
   - Greenlight AVM
   - NextLabs DAM

3. Data Privacy
   - IBM GDPR
   - SAP RAL (Access Log)
   - UI Logging / Masking
   - SAP ILM (Information Lifecycle Management)

4. Business-IT Monitoring
   - IBM Cloud
   - SAP GRC Process Control
   - SAP BIS Business Integrated Screening
   - SAP ETD Enterprise Threat Detection

5. Authentication
   - SAP Single Sign-On
   - SAP SNC (Secure Network Communication)
   - SAP Authenticator (2-factor)

6. Application Security
   - IBM DAS
   - SAP Solution Manager
   - SAP Code Inspector / Vulnerability Analyzer

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

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)
    - OS Users root, broad privileges
    - VSI SAP Antivirus Integration

11. Vulnerability Assessment
    - Onapsis Security Platform
    - SAP ETD (Enterprise Threat Detection)
    - Firewall
    - Gateways SAP / Application Level
    - SNC ACL Access Control Lists
    - Logs OS and Applications

12. Infrastructure Security
    - SOC-1: ICFR

13. Physical Security and Hosting
    - 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)

![Image showing Single Sign-On and Two Factor Authentication process](image-url)
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

SAP HANA Platform

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
On-Premise | Hybrid | Cloud Platform | Enterprise Cloud

Deployment

Any Apps
Any App Server

SAP Business Suite and BW ABAP App Server

Supports any Device
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

- **Log**
  - SAP HANA
  - ABAP

Non-SAP

- **Log**
  - ... (indicates a placeholder for additional information)

SAP ETD

- **Enterprise Threat Detection**

  - **Rules / Patterns**
    - 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

  - **SAP HANA**
    - Exposes a REST service to receive log data
    - Evaluate & Analyze
    - Generate Alert Data

  - **Smart Data Streaming**
    - Push data to HANA
    - Normalize, Pseudonymize and Enrich Log Data

User Interface

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

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

- **Generate Alert Data**
- **Evaluate & Analyze**
- **SAP HANA**
- **User Interface**

- **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

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 SCAN FOR SAP
List of Controls to be Automated:
- IT General Controls (ITGCs)
- SAP TFS
- SAP NetWeaver
- SAP Gateway
- HANA Security
- RFCs

Europe CoC SAP Security & GRC
Madrid

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.
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

1. Automate
2. Analysis
3. Role Profiling

- 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

**EAM**
Emergency Access Management

- 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

- 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

- 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**

**Get Clean**

**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.

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)

- 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
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”…

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
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: raffella.cannone@it.ibm.com
THANK YOU!

SÍGUENOS EN:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube.com/user/ibmsecuritysolutions

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.