SAP Cloud Security Framework

Theory and Practice

Michal Marko, SAP CZ
Presales Senior Specialist for Cloud Platform & Technology

PUBLIC
Agenda

What is SAP Cloud
- Delivery and Deployment models
- Portfolio

SAP Cloud Secure
- Trust Center
- Certification & Standards
- Contractual framework
- Data Centers & Infrastructure

Story & Experience

Summary & Links
What is SAP Cloud?
Delivery, Deployment Models & Portfolio
Definition* of cloud deployment model

**Private cloud**
- The Service is assigned to one dedicated customer (single-tenant)
- Access via protected network channel (Virtual Private Network)
- Operations by customer or "Managed-Service" agreement
- May be hosted "On-premise" or with service provider

**Public cloud**
- Systems are shared between multiple customer (multi-tenant)
- Service usage by self-service access and tools
- Operations by service provider

**Hybrid cloud**
- Mix of multiple deployment model
- Integration through standardized or specific interfaces ensuring access and data transfer

* Analog to definition of cloud by the National Institute of Science and Technology (NIST)
SAP Cloud deployment model

SAP Cloud Secure

- SAP Data Center
- SAP Managed Operations
- SAP Support

A mix of “On-premise” and at least one cloud model is named “Mixed environment”
SAP Cloud Solution portfolio

Hana Enterprise Cloud

SAP Cloud Applications

SAP Cloud Platform

One Cloud Infrastructure
SAP Cloud Secure
High Level Overview
Security, privacy, and compliance in the cloud – we keep your data safe

Your business is built on trust, and you expect the same from your software provider. As a leading software provider and a cloud company, we’re dedicated to building – and keeping – our customers’ trust.

Cloud Service Status
Discover the uptime and availability of SAP’s cloud services with access to real-time insights.

Security
Rest assured that your data is protected with a cloud security foundation based on the highest quality standards.

Data Center
Visit our data centers and see state-of-the-art technologies and rigorous security methodologies.
Layer of assurance

**Contract**
- Data processing agreement to meet applicable local data privacy regulations globally

**Audit and Certification**
- Service Organization Control (SOC) reports and certifications to provide independent evidence for security, availability, confidentiality, data protection, and quality

**Policies, directives, and standards**
- Integrated management system for information security, data protection, and service delivery
- Comprehensive security architecture covering applications, processing systems, and data center
Management System of **standards and best practices**

<table>
<thead>
<tr>
<th>Transparency</th>
<th>Certification</th>
<th>Financial Controls</th>
<th>Operations and Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ISO 27001**</td>
<td>SOC 1 (SSAE18 / ISAE 3402)</td>
<td>SOC 2, SOC 3 (AT 101 / ISAE 3000)</td>
</tr>
<tr>
<td></td>
<td>ISO 22301**, ISO 9001** BS10012</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Data Protection</th>
<th>Data Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BS 10012 ISO 27018</td>
<td>EU General Data Protection Regulation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ISO 9000 ISO25010</td>
<td>ISO 20000</td>
<td>ISO 22300</td>
<td>ISO 27034 OWASP</td>
<td>SANs, ISO CERT, NIST</td>
<td>ISO 27040</td>
<td>ISO 27035</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Foundation</th>
<th>Code of Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ISO 27002</td>
</tr>
</tbody>
</table>

* The Management systems are used across all SAP Cloud Secure services, execution of independent certification and audit depend on service and organizational unit respectively. Details available at [http://go.sap.com/corporate/de/company/innovation-quality/excellence.html](http://go.sap.com/corporate/de/company/innovation-quality/excellence.html)

Compliance

Get the assurance you need to know that our cloud offerings meet the latest compliance and security standards. We regularly check compliance through external reviews and audits and follow one common framework, including data security and privacy regulations, worldwide.

ISO/BS Certificates

SAP has developed and implemented an integrated framework based on several international standards. This approach provides a consistent, secure service that meets customer and applicable regulatory requirements. We address client satisfaction and continuous, as well as secure operation of our services, through
SAP’s Data Protection Management System combines the various requirements relevant for data protection and privacy in two documents

- **General book**: General rules and descriptions valid for entire organizations
- **LoB appendix**: Definition of scope and work instructions valid for employees in this LoB
Layer of assurance

**Contract**
- Data processing agreement to meet applicable local data privacy regulations globally

**Audit and Certification**
- Service Organization Control (SOC) reports and certifications to provide independent evidence for security, availability, confidentiality, data protection, and quality

**Policies, directives, and standards**
- Integrated management system for information security, data protection, and service delivery
- Comprehensive security architecture covering applications, processing systems, and data center
Globally applicable Data Processing Agreement (DPA) based on European General Data Protection Regulation, one of the most comprehensive privacy regulation. Uniform application and control of this comprehensive data privacy regulation is consistent throughout the sub-processor chain.

SAP observes changes of local data privacy regulation globally and invests to keep our service in a way that our customer can continue to use it in compliance.

Additional cloud service offerings to cover stricter data privacy requirements and special customer demands; like storage and transfer of data in / from EU locations, only, US Federal Government environment, Australian or Russian data residency etc.

https://www.sap.com/about/cloud-trust-center/cloud-service-level-agreements.html
Cloud Contract

The contract for cloud services from SAP consists of three main building blocks. The order form, data processing agreement, and general terms and conditions are generally the same for any cloud service on our price list, while the cloud service description is a product-specific collection of terms.

Order form
The order form is your ordering document to subscribe to business cloud services from SAP. It defines the commercial terms and lays out the agreement structure.
View sample order form

Cloud Service Description
SAP delivers the cloud service to all customers in a uniform manner. Find out the product-specific terms, the support policy, and operational availability of the cloud service.
Product supplement ›
Support policy ›
Service level agreement ›

Data Processing Agreement
Based on the instruction of the data processor handling personal data uploaded into the cloud service, SAP implements and maintains technical and organizational measures to adequately protect the personal data.
Data processing agreement ›
Data center location ›

General Terms and Conditions
The general terms and conditions (GTC) document describes the essential legal terms that apply to the chosen cloud service including usage rights, customer data, warranties, confidentiality, and limitations of liability provisions.
General terms and conditions ›
Consulting service supplement ›
Financing supplement ›
What is Cloud Security Framework?

“This Cloud Security Framework, which is part of SAP’s Documentation as defined in the SAP General Terms and Conditions for Cloud Services [8] and may be updated from time to time, governs the security controls and measures provided for the production (PRD) environments of SAP Cloud solutions and respective modules provided by SAP as listed in Section 2.3”

It’s a document which applicable to all SAP Cloud Solutions

SAP CLOUD:
SECURITY FRAMEWORK
VERSION 2.3.1 (FEBRUARY 27, 2018)
SAP GLOBAL SECURITY

SAP MAY CHANGE THIS CLOUD SECURITY FRAMEWORK WITHOUT NOTICE OR CONSENT.

Document Classification: Customer
## Technical & organizational measures (TOM) at a glance

<table>
<thead>
<tr>
<th>TOM</th>
<th>Measures (samples)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Video and sensor surveillance, access logging, intruder alarm systems</td>
</tr>
<tr>
<td>System Access Control</td>
<td>Password policy, strong authentication, access management tool</td>
</tr>
<tr>
<td>Data Access Control</td>
<td>Authorization concepts, SAP security policies and standards, security checks and penetration tests</td>
</tr>
<tr>
<td>Data Transmission Control</td>
<td>SAP security policy (confidentiality), network security, encryption</td>
</tr>
<tr>
<td>Data Input Control</td>
<td>Security Incident Management, 24 x 7 Security Monitoring Center, SIEM</td>
</tr>
<tr>
<td>Job Control</td>
<td>Segregation of duties, subcontractor compliance / certification</td>
</tr>
<tr>
<td>Availability Control</td>
<td>Business continuity management, disaster recovery plans / testing</td>
</tr>
<tr>
<td>Data Separation Control</td>
<td>Multi-tenancy, separate system landscapes, access restrictions</td>
</tr>
<tr>
<td>Data Integrity Control</td>
<td>Security patch management, malware management process</td>
</tr>
</tbody>
</table>
SAP Cloud Secure Data Centers

- Data Center on level III or IV
- SAP Data Centers around the world
  - 14 countries, 30 locations, 40 DCs
- Benefit from local regulations
  - (e.g. strong German & EU regulations)
- Low latency speeds-up access
- Customer can choose
  - Region of data storage
  - EU-only operations available
  - preferred datacenter partner

**+ Premium Partner Model for HANA Enterprise Cloud**
10+ Premium Partner: 33+ data centers in 16+ countries

*SAP Cloud Secure data center overview *

* Not all Cloud Solutions are available in all Data Center; for the availability of Cloud Solutions please compare the official availability matrix
Data Center – SAP Data Center level (availability) definition

- SAP Cloud solutions and customer data needs to be operated in a:
- SAP Data Center level III, III+ or IV classified Data Center
- SAP checks on site the compliance to the SAP Data Center minimum physical security standard that covers topics like:
  - Perimeter & location security
  - Building entry point security
  - Building security
  - Access controls & monitoring
    - General access and
    - Access to dedicated SAP areas
  - Fire protection
  - Electrical power supply
  - Certifications of the Data Center provider

<table>
<thead>
<tr>
<th>Minimum availability requirements</th>
<th>level I</th>
<th>level II</th>
<th>level III</th>
<th>level III+</th>
<th>level IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand-alone Data Center building necessary</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Amount of external electrical power suppliers</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Amount of transformers to power the Data Center</td>
<td>n</td>
<td>n</td>
<td>n+1</td>
<td>n+1</td>
<td>2n</td>
</tr>
<tr>
<td>UPS battery system necessary</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Minutes UPS must provide power</td>
<td>0</td>
<td>5</td>
<td>&gt;10</td>
<td>&gt;10</td>
<td>&gt;10</td>
</tr>
<tr>
<td>Amount of UPS systems necessary</td>
<td>n</td>
<td>n</td>
<td>n+1</td>
<td>n+1</td>
<td>2n</td>
</tr>
<tr>
<td>(Diesel-) Generators needed</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Amount of cooling systems needed</td>
<td>n</td>
<td>n</td>
<td>n+1</td>
<td>n+1</td>
<td>2n</td>
</tr>
<tr>
<td>Server cooling is independent from an office AC</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fire detection system needs to be installed</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fire extinguishing system must be installed</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>On-site response time of Data Center personnel</td>
<td>&lt;48h</td>
<td>&lt;8h</td>
<td>&lt;1h</td>
<td>&lt;1h</td>
<td>&lt;1h</td>
</tr>
<tr>
<td>Available WAN network connection lines</td>
<td>1</td>
<td>n+1</td>
<td>n+1</td>
<td>n+1</td>
<td>2n</td>
</tr>
<tr>
<td>Available LAN network connection lines</td>
<td>n</td>
<td>n+1</td>
<td>n+1</td>
<td>2n</td>
<td>2n</td>
</tr>
</tbody>
</table>

n = all components are used for operation; no spare component; no backup or redundancy;
n+1 = exactly one additional component is available to replace a failed component;
2n = every component has a backup/spare component; full redundancy
UPS = uninterruptible power supply
AC = air condition
SAP Cloud Secure
A bit of experience
SAP Cloud Portfolio WS
Portal Options WS
HANA Cloud Platform WS 1
Proof of Technology 1MD
SAP Cloud Platform WS 2

Sold

- NW & BW onPrem
- NW & BW onPrem HCP
- HCP & ERP

Integration, Users, Custom Fiori, Mobile
PoC 1 Neo & Cust. Java
PoC 2 CF & Cust. Java

Users ??? Authorization ??? Authentication ??? LDAPs/IDPs/SAML2.0/Oauth

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2016</td>
<td>November 2016</td>
<td>March 2017</td>
<td>September 2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SAP Cloud Secure

Summary
Confidence in SAP Cloud Secure service through transparency

Comprehensive Contracts
Privacy, security framework, and applicable local regulations

Independent Audits
Service Organization Control reports certifications

Cyber Defense
Multiple layers of defense
Holistic: Prevent, detect, and react

Secure Cloud Model
Holistic approach
Secure architecture
Thank you

Need for more information? SAP Cloud Trust Center

Michal Marko, michal.marko@sap.com