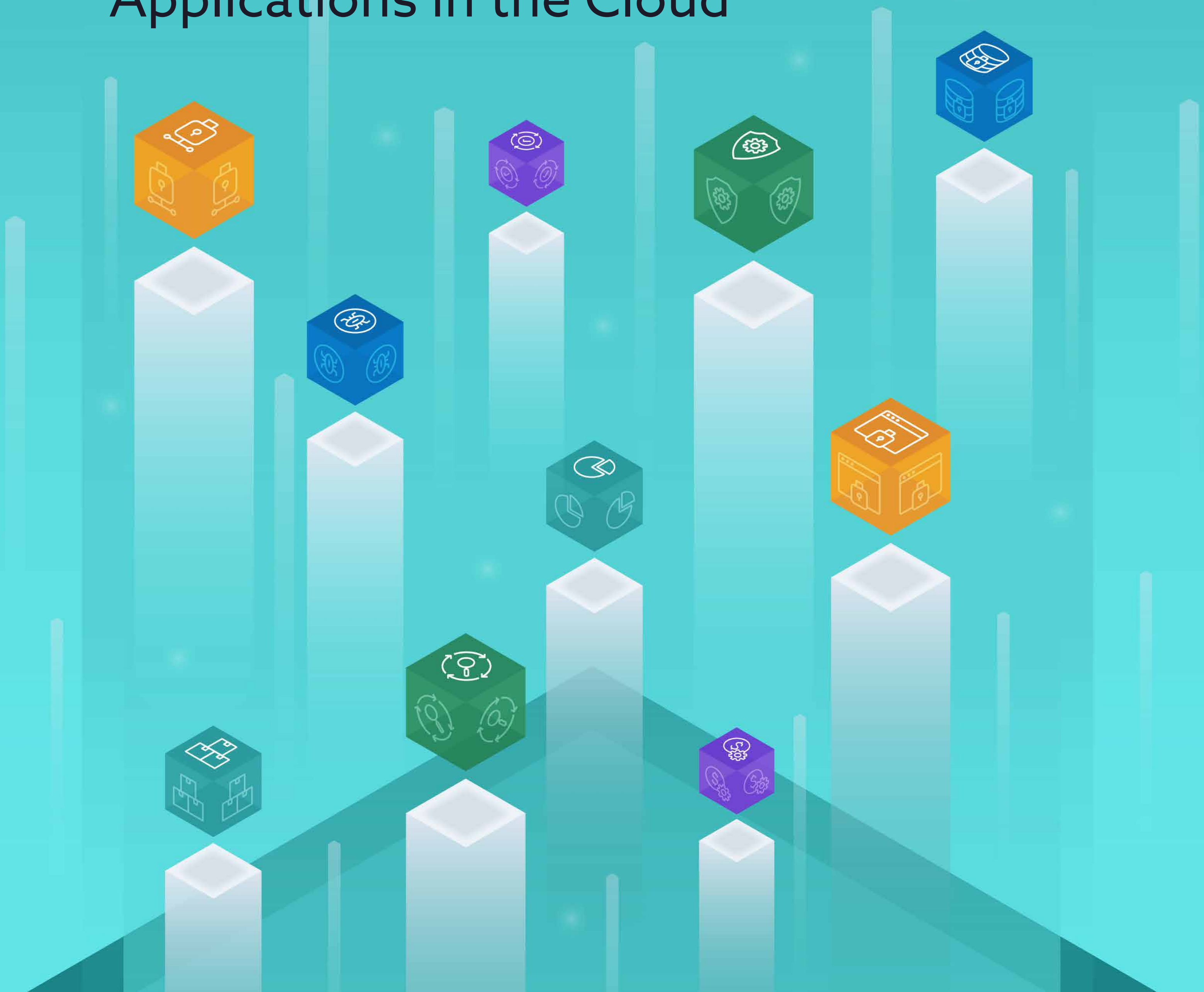
CSA cloud security alliance®

# Critical Controls Implementation for SAP (Part 1)

## Helping Organizations Securely Migrate to and Operate ERP Applications in the Cloud



# Acknowledgments

## Lead Authors:

Juan Perez-Etchegoyen
Victor Chin
Sergio Abraham
Hugh Fraser
Thomas Kastner
Fredrik Pihl
Michael Roza
Charlie Singh
Frederik Weidemann

## CSA Global Staff:

Victor Chin
Shamun Mahmud
AnnMarie Ulskey

# Table of Contents

Introduction ........................................................................................................ 5

How To Use This Document ................................................................................ 5

Top 20 Critical Controls for Cloud ERP Customers ............................................ 5

Critical Controls Implementation for SAP ......................................................... 6

Controls Implementation ..................................................................................... 7

APP01 - Secure Landscape .................................................................................. 7

APP02 - Baseline Secure Configurations ............................................................ 9

APP03 - Security Vulnerabilities .........................................................................11

INT01 – Secure Integrations and API .................................................................12

DAT01 – Continuous Monitoring ........................................................................ 14

DAT02 – Data Separation .................................................................................... 16

DAT03 – Data Encryption .................................................................................... 18

BUS01 -  Inventory of Business Assets, Data and Processes .............................. 20

BUS02 - Business Process Controls .................................................................... 22

BUS03 - Continuous Compliance ........................................................................ 23

# Introduction

The CSA ERP Security working group aims to help organizations securely migrate to and operate ERP Applications in cloud environments by developing industry best practices. To achieve that goal, we have developed the Top 20 Critical Controls for Cloud ERP Customers, which was released on June 10, 2019.

At the same time, we understand that security configurations and vulnerabilities for cloud ERP Applications can be difficult to navigate as there is currently no framework that aligns with standard controls. Furthermore, ERP applications are so complex and diverse that for any guidance document to be truly useful, from an implementation perspective, we need to address specific technologies.

The Critical Controls Implementation for SAP is the first document in a series of implementation documents we hope to develop that focuses on specific ERP technologies. The documents will be released in two parts. The first part of the document will provide controls implementation guidance for the following controls:

APP01 - Secure Landscape
APP02 - Baseline Secure Configurations
APP03 - Security Vulnerabilities
INT01 – Secure Integrations and API
DAT01 – Continuous Monitoring
DAT02 – Data Separation
DAT03 – Data Encryption
BUS01 - Inventory of Business Assets, Data and Processes
BUS02 - Business Process Controls
BUS03 - Continuous Compliance

The following sections will provide more details regarding how the two documents are different and their uses.

# How To Use This Document

Both documents focus on the different aspects of securing a cloud ERP application. In the Top 20 Critical Controls for Cloud ERP Customers, a more general approach is provided, whereas in the Critical Controls Implementation for SAP, the working group has taken a more technical and granular approach.

## Top 20 Critical Controls for Cloud ERP Customers

In the previous document, the working group elaborated on 20 critical controls that are required to secure cloud ERP applications. The following information is provided in that document:

- Domain: The domain assigned to the control
- Control Identification (ID): Unique name for the control
- Control Description: A description of the control and how it should be addressed
- Control Objectives: A description of what the control seeks to achieve
- Threats and Risks: Threats mitigated by the control, including those defined in the Treacherous 12: Top Threats to Cloud Computing 2016 report
- Related CCM Controls: If applicable, the IDs of the controls, as defined in the CSA CCM

## Critical Controls Implementation for SAP

In this document, the working group focuses on providing guidelines on controls implementation as well as a set of checklists for SAP administrators. The controls implementation and the checklists apply to SAP NetWeaver(C) ABAP(C)-based Applications, and are generic enough to apply to all current versions, providing a detailed description of the control implementation, that can be complemented with external references that are also incorporated. The Control Implementation guidelines provide a detailed description of the control implementation and, combined with the Top 20 Critical Controls document previously released by the CSA, explains who would be typically responsible in an IaaS or SaaS scenario. However, please note that the actual responsibility for security depends on your contract with your supplier.

These checklists act as guidance only. The checklists provide general steps as well as some direction on how to carry out the implementation of the controls. The Checklist aims to be as technical as possible by providing SAP transaction numbers and other equivalent details. However, it is not feasible to provide that level of detail for a few controls. For example, BUS-03 (Continuous Compliance) is one such control. Instead, general guidance is provided. Lastly, specific references to SAP documentation are also provided.

# Controls Implementation

| | |
|---|---|
| **Domain** | Cloud ERP Application |
| **Control ID** | **APP01 - Secure Landscape** |
| **Technology Stack** | SAP NetWeaver ABAP |
| **Versions** | All |
| **Control Implementation** | The landscape in SAP NetWeaver Applications is composed of multiple SAP Systems that have diverse roles such as Sandbox, Development, QA or Production, to name a few. The security of the overall landscape is paramount to the security of the data that is hosted in the production system.<br>In general terms, access to lower-risk systems such as development should not be potentially used to access a higher-risk system such as production. This means that as much as possible, all systems in the landscape should be separated (with different access controls) and secured with the same level and standards of protection. |
| **Checklist** | 1. Make sure users in development are not authorized to access data in production without proper evaluation of their authorizations. As a general rule, assign authorizations that are as restrictive as possible across the landscape, independently of the system role (also known as the least privilege principle).<br>2. Make sure no RFC Destinations are configured from lower-risk systems to higher-risk systems, using stored credentials. For this, use transaction SM59, which can provide the login information. Exemptions may be connections to the TMS Controller and Solution Manager as long as they follow the least privilege principle.<br>3. Ensure S_RFCACL is properly assigned to users and restricted as much as possible in production environments. Use transaction SUIM to search for users and roles assigned with S_RFCACL. |

4. Configure strong passwords for transport-related accounts such as TMSADM. Avoid using any default password for these accounts. Additionally, make sure the transport-related accounts are assigned only with the S_A.TMSADM profile. Use transaction SA38 and report RSUSR003 to identify the password of user TMSADM.
5. Ensure that right controls for insecure transport requests and insecure code are configured in the transport management system so it is not possible to move insecure objects into production.
6. Make sure the right approval process is set in the transport system, so all changes are properly approved by the right individuals before being moved across the landscape. Use transaction STMS to set up and validate the right approval process.
7. Ensure that any storage system used for the Transport Management System (Typically Common Transport Directory) is secured. If it is NFS or SMB based shares, these shares should be properly secured to avoid unauthorized access and modification of transport-related data.
8. Configure the "System Change Option" appropriately, according to the role each system fulfills in the transport process. This can be achieved globally (SE03/SE06) or per client (SCC4). Productive clients must be set to "not changeable".

**References**

- https://apps.support.sap.com/sap/support/knowledge/preview/en/1568362

| | |
|---|---|
| **Domain** | Cloud ERP Application |
| **Control ID** | **APP02 - Baseline Secure Configurations** |
| **Technology Stack** | SAP Netweaver ABAP |
| **Versions** | All |
| **Control Implementation** | SAP Applications are complex as they are based on several components that interact with each other. These components are extensively configurable, and overall, SAP Systems are customizable and configurable. Approximately 10% of the configurations that can be modified and maintained have a security impact.<br>The following components must be securely configured in SAP Applications:<br>• SAP Application Server<br>• SAP HTTP Interface<br>• SAP Gateway<br>• SAP Message Server<br>• SAP Management Console |
| **Checklist** | 1. Secure password policies configurations to match the corporate password policies. This can be achieved by maintaining the profile parameters through transaction RZ10 (maintaining both global and instance-specific profiles) or maintaining the user-defined security policies through transaction SECPOL.<br>2. Secure critical profile-parameters configurations using transaction RZ10 such as (but not limited to):<br>a. No_automatic_user_sapstar = 1<br>b. RFC/callback_security_method = 3<br>c. Login/password_downwards_ compatibility = 0<br>3. Secure the diverse component ACL configurations such as:<br>a. SAP Gateway sec info and reg info ACL files<br>b. SAP Message Server ms acl info ACL file |

4. Reduce the number of HTTP services that are enabled through transaction SICF.
5. Restrict access to SAP tables (SAP Applications can have up to 70,000 tables depending on its version and product). Be sure to:
    a. Configure an authorization group for all tables that don't have an authorization group assigned (Authorization Group unassigned or &NC&).
    b. Restrict S_TABU_DIS AND S_TABU_NAM authorization objects so these objects protect access to the most critical tables.
    c. Restrict SE11, SE16, SM30 and SM31 to address standard and custom tables.

**References**

- Secure Configuration of SAP NetWeaver Application Server Using ABAP
- SAP NetWeaver Application Server for ABAP Security Guide

| | |
|---|---|
| Domain | Cloud ERP Application |
| Control ID | **APP03 - Security Vulnerabilities** |
| Technology Stack | SAP Netweaver ABAP |
| Versions | All |
| Control Implementation | On the second Tuesday of each month, SAP will release the security patches addressing security vulnerabilities that were either discovered internally by SAP or reported by external researchers. All of the patches must be evaluated, and a risk-based decision must be made, depending on the risk appetite of the organization as well as the potential business impact of each particular vulnerability.<br>In addition, SAP guarantees that these security notes can be applied if the system is running on a Support Package Stack (SPS) not older than 18 months. |
| Checklist | 1. Connect to security notes in the SAP launchpad: https://launchpad.support.sap.com/#/securitynotes<br>2. Get the list of SAP Security Notes released by SAP.<br>3. Categorize the "Vulnerability Trends Over Time" (i.e SAP: Vulnerability Statistics).<br>4. Identify the components affected by the SAP Security Notes as well as the SAP Systems that are affected by them.<br>5. Apply the relevant patches either through SNOTE or any other upgrade mechanism available to the technology stack (i.e. using the SPAM transaction).<br>6. Ensure that the SPS level is not older than 18 months (recommendation). |
| References | • SAP NetWeaver Application Server for ABAP Security Guide<br>• CVE https://www.cvedetails.com/vendor/797/SAP.html |

| | |
|---|---|
| **Domain** | Integrations |
| **Control ID** | **INT01 – Secure Integrations and API** |
| **Technology Stack** | SAP Netweaver ABAP |
| **Versions** | All |
| **Control Implementation** | The extensive integration of ERP applications with outside applications and data sources is common practice because of the nature of processes supported by these systems. In a typical ERP environment, there are interfaces and connections between different solutions as well as different environments. If improperly secured, these integrations are ripe for abuse, and production information and data risks may be easily compromised.<br>The management of interfaces across different ERP environments should address the following considerations:<br>1. Maintain an inventory of all interfaces, including the type of data that is exchanged and the technical details of the connections, such as protocol, user, business owner, authorizations and encryption details.<br>2. Avoid the use of insecurely provisioned interfaces, such as broad trust relationships or the utilization of usernames and passwords that others can leverage.<br>3. Always apply the "least privilege" principle to define the privileges that technical users will be granted for various interfaces.<br>4. If possible, encrypt all interfaces that exchange regulated or sensitive data between applications.<br>5. Avoid setting up interfaces from systems of lower security (such as development) to systems with higher security (such as production) whenever possible.<br>6. If secrets are used to set up the interfaces (i.e., API keys, passwords, certificates), establish the proper management process to govern those secrets (maintain/change/rotate if needed). |

7. Ensure RFC Callback security in all systems, especially when systems from a higher risk classification connect to systems with a lower classification (e.g. Prod calls Dev)

For IaaS, PaaS—and possibly SaaS service models—this control is the security responsibility of the cloud customer.

### Checklist

1. Define a unique identifier for integration and add it in your inventory of all integrations.
2. Use the principles of security by design and security by default. Design for mutual authentication between applications using client certificates, if possible.
3. Perform system hardening of public-facing components, including applications and infrastructure.
4. Create separate DMZ network segments, hosting securely configured SAP Web Dispatchers for publicly exposed integrations and API.
5. Incoming and Outgoing integration requests should be managed by a web application firewall or web proxy.
6. "Protect data-in-transit using protocols and strong crypto ciphers.
7. Enforce the principle of "least privilege" on the technical account used for the integration, to reduce consequences in case of a security breach.
8. Perform a pentest of the published integrations before business go-live, including initial vulnerability scan of the API. Run a basic network vulnerability scan, supporting CVSS rating, to measure your current situation. For publicly exposed systems, patch all vulnerabilities having CVSS score 4 and higher.

### References

- SAP Process Integration Security Guide
- Security Information SAP Web Dispatcher
- CIS 20 Critical Security Controls

| | |
|---|---|
| **Domain** | Cloud ERP Data |
| **Control ID** | **DAT01 – Continuous Monitoring** |
| **Technology Stack** | SAP Netweaver ABAP |
| **Versions** | All |
| **Control Implementation** | SAP Applications are complex and built on top of multiple components. To understand what is happening within an SAP Application, multiple sources of data must be enabled and analyzed. This has to be driven by a continuous monitoring program which includes an incident response program with the following components:<br>1. Enable the logs and traces that are relevant for SAP Applications (such as Security Audit Log and HTTP access log), sending them to a centralized log and security server.<br>2. Implement a process to review the logs periodically, preferably using a SIEM tool, so a timely response is possible.<br>3. Implement an incident response process so whenever an incident is identified across SAP applications, the proper teams are involved to contain the incident.<br>In diverse versions of SAP Applications, even Cloud multitenant, Read Access Logging (RAL) can be used to log who had accessed sensitive data; this access logging is enabled by the company per their definition of sensitive data. |
| **Checklist** | Determine which data must be logged under which circumstances. The organization must define which legal, compliance or security requirements to apply and which data must be logged.<br>1. Ensure that the following logs are enabled in SAP applications by incorporating this in the baseline configuration of every new instance of SAP:<br>• Security Audit Log (through transaction SM19)<br>• SAP Gateway Log (through transaction SMGW) |

- SAP Table Change logging (by enabling parameter rec/client and transaction SE13)
- HTTP access log (SMICM)
- Message server log
- Change documents
- Read Access Log

NOTE: Enable security-relevant events that are meaningful to your organization and keep in mind that enabling all might pose a performance and storage impact. Additionally, it is important to understand which data must be logged under which circumstances (e.g. salary information, Social Security number, or bank account)

2. Implement a process to review the logs periodically by analyzing the generated events against a list of previously defined potentially insecure behaviors. The generated logs can be accessed using the following transactions:

   - Security Audit Log (through transaction SM20)
   - SAP Gateway Log (through transaction SMGW)
   - SAP Table Change logging (through transaction SCU3)
   - HTTP access log
   - Message server log
   - Change documents

Implement a process to escalate and contain incidents in SAP Applications. This might involve actions such as:

- Locking a user account (Transaction SU01)
- Changing users' passwords (Transaction SU10)
- Further reviewing access logs and any other source of information from a consolidated point of view

**References**

- SAP Audit and Logging
- The SAP Security Audit Log
- Activate/Deactivate Table Change Logging
- Performance Problems through Table Logging
- Performance: Log Table DBTABLOG Increases in Size Due to KONP
- Read Access Logging

| | |
|---|---|
| Domain | Cloud ERP Data |
| Control ID | **DAT02 – Data Separation** |
| Technology Stack | SAP Netweaver ABAP |
| Versions | All |
| Control Implementation | Business data is critically important in ERP applications. This data is typically stored in a database and provides access to multiple users and application servers. Additionally, in a typical ERP landscape, there are numerous environments (i.e., development, quality assurance, and production), as well as tenants.<br>Data must be segregated appropriately in ERP systems and environments. In other words, production data should not be available in non-production environments, and any data segregation should be executed appropriately at the application level (i.e., concepts of systems, clients, tenants or company codes).<br>Consider the following during the implementation of the ERP application:<br>1. Build the landscape in layers, with firewall separation of the production system, testing system and the development systems.<br>2. Separate production data from non-production data and avoid copying production data from production environments without proper sanitization.<br>3. Properly configure and implement any client or tenant separation—particularly when the cloud customer configures it—so that no user has access to both production and non-production tenant.<br>Regardless of the service model, this control is the responsibility of the cloud customer. |

**Checklist**

1. Build a landscape with clear separation of development, test, quality assurance (optional) and production to implement controlled change management. Use transaction STMS to develop and check the proper set-up of all the transport mechanisms.
2. Implement logical separation of production and non-production network.
3. Consider subzoning of production area depending on information trust domains.
4. Implement a management network with jumphosts and patch servers for privileged administration. Multi-factor authentication should be implemented.
5. Implement a DMZ for external access. Consider having an inner DMZ even for internal access depending on the threat model.
6. Monitor infrastructure and applications using a SIEM solution

**References**

- SAP NetWeaver Security Guide
- SAP NetWeaver Security Guide 7.5
- Using Multiple Network Zones
- SAP Cloud Platform Connectivity

| | |
|---|---|
| **Domain** | Cloud ERP Data |
| **Control ID** | **DAT03 – Data Encryption** |
| **Technology Stack** | SAP Netweaver ABAP |
| **Versions** | SAP NetWeaver All Versions<br>CommonCryptoLib v8.5 |

**Control Implementation**

Business data stored and processed by the ERP application is its most crucial component. Sensitive data at rest must be encrypted and classified to avoid unauthorized access according to predefined rules and policies. Avoid encrypting business data with the same key. The organization must first define data governance policies, such aswhat data should be encrypted and what should not (i.e., encryptionof all business data could render the ERP application useless).

Concerning ERP data, adhere to the following guidelines:

1. Data should be encrypted while at rest and when stored in the database or any other location.
2. Encrypt data during transmission to the end-user. If the interface is web-based (as it is for the majority of ERP applications), then make sure to implement transport-level encryption with robust protocols and ciphers.
3. If using encryption keys and certificates, ensure the proper process is in place to maintain, issue, revoke and control access to these keys and certificates.
4. Database encryption will not protect you from injection attacks but may impact cost and performance, thus it should be thoroughly analyzed.
5. Offline ERP data should be encrypted and password protected using a standard protocol such as AES-256 (or better) having a password matching the strength, i.e. 24 characters random generated password.

For IaaS, this control is the responsibility of the cloud customer.

For PaaS and SaaS, the customer must conduct due diligence and ensure the cloud provider is adequately protecting their data.

### Checklist

1. Secure data-at-rest on server-server by enabling full disk encryption in the operating system.
2. Secure data-at-rest on the client-side by enabling full disk encryption in the operating system.
3. If using SAP HANA Database, leverage standard encryption mechanisms for all the information in the data area and log volume area using SAP HANA administrator.
4. Secure data-in-transit by enabling SNC protocol for SAP GUI applications, using SSO and configure for protocol Kerberos and AES-128.
5. Secure data-in-transit by enabling secure communication in SAP Web Dispatcher using strong protocols and crypto ciphers, i.e TLS1.2 with AES-128.
6. Run a basic network vulnerability scan, supporting CVSS rating, to measure your current situation. For publicly exposed systems, patch all vulnerabilities having CVSS score 4 and higher.
7. Authorize a file compression software supporting AES-256 encryption to protect offline data.

### References

- SAP NetWeaver Security Guide
- Setting up SSL on Application Server ABAP
- CommonCryptoLib 8 cryptographic algorithms
- Security Information SAP Web Dispatcher
- SAP HANA Encryption
- Ecrypt CSA - Algorithms, Key Size and Protocols Report, 2018
- Commercial National Security Algorithm Suite and Quantum Computing FAQ

| | |
|---|---|
| **Domain** | Business Processes |
| **Control ID** | **BUS01 - Inventory of Business Assets, Data and Processes** |
| **Technology Stack** | SAP Netweaver ABAP |
| **Versions** | All |
| **Control Implementation** | Business data stored and processed by the ERP application is its One of the most challenging parts of operating business applications at scale is to have the right level of visibility around the data and the processes that each application is supporting. Having a clear inventory of these components is the starting point to understand where the crown jewels are in an organization, and to be able to provide the right governance and controls around those components.<br>Implement an inventory of applications, data and processes which serve as a single source of truth in regard to business processes. |
| **Checklist** | 1. Before starting, the business should provide or walk through the 'business process flow'. Risks should be identified in the process flow to which controls are applied. For all automated controls in the process flow, an asset is identified that supports/provides the control point.<br>This Asset list when compiled is critical to the business as it documents the "assets" critical to the survival of the business.<br>2. Identify all the technical components and SAP Applications that build up the SAP environment. Incorporate non-SAP Applications if these are also critical components of the business processes running through SAP.<br>3. If the company is using a single source of truth (inventory/repository) for SAP applications, make sure it is properly maintained and up to date. If there are many inventories/repositories, identify all and create a process to condense all the information. Some options for these repositories are SLD and LMDB. |

| | |
|---|---|
| | 4. With the functional leads, identify the key business processes that are supported by each SAP Application and document. This should be a key input to identify the overall criticality of an SAP System.<br>5. Check the process for creating new SAP Systems as well as all existing environments to validate if these were purposely created and if the right approvals were in place.<br>6. Validate that the right stakeholders (IT, BASIS, Information Security) are aware of the service agreements regarding updates of security configurations, software components and patches across SAP Applications.<br>7. Implement software components and patch management process that can provide visibility on missing patches and outdated software components.<br>8. Check the Software components that are installed on each SAP System (System-->Status) and keep an inventory of all systems and business processes, capturing the importance to the business of each technical asset. |
| **References** | • SAP System Landscape Directory<br>• Landscape Management Database |

| | |
|---|---|
| Domain | Business Processes |
| Control ID | **BUS02 - Business Process Controls** |
| Technology Stack | SAP Netweaver ABAP |
| Versions | All |
| Control Implementation | SAP Applications support several critical business processes. Controls must be put in place to ensure that no fraudulent activities can be executed by abusing existing or elevated privileges. |
| Checklist | 1. Together with the business process owners, identify critical steps on each one of the critical business processes.<br>2. Identify the systems involved, particularly the SAP Applications that are supporting these processes, including the systems running on the cloud.<br>3. Identify system interfaces and define the purpose of each of them. Filter and/or disable those systems' interfaces that are not required:<br>a. Delete RFC Destinations (Transaction SM59)<br>b. Enable UCON (Unified Connectivity, transaction UCONCOCKPIT)<br>c. Disable ICF Services (Transaction SICF)<br>d. Filter system ports<br>4. Develop specific business controls for business steps that require moving data among environments<br>a. Extra authorizations/privileges (Through PFCG roles modification)<br>b. Approvals from managers<br>5. Implement a process that involves automatic processes controls as well as the monitor for the usage of interfaces related to the business processes. |
| References | • End to End Business Processes in SAP |

| | |
|---|---|
| **Domain** | Business Processes |
| **Control ID** | **BUS03 - Continuous Compliance** |
| **Technology Stack** | SAP Netweaver ABAP |
| **Versions** | All |
| **Control Implementation** | Due to the nature of data and processes that SAP Applications support, it is key to maintain certain levels of compliance with the regulations that are applicable to the data, processes and industry that the organization is operating in.<br>Implement a process that ensures continuous compliance and can work as a centralized view to monitor control effectiveness in real time. |
| **Checklist** | 1. Identify compliance and regulatory standards that are affecting the SAP Applications.<br>2. Identify the specific key controls that must be in place.<br>3. Identify the required testing procedures to validate the operating effectiveness of those controls.<br>4. Develop automated testing procedures that can validate controls effectiveness 24x7.<br>5. Implement an alerting mechanism to address audit findings as soon as they happen. |
| **References** | • https://en.wikipedia.org/wiki/Continuous_monitoring<br>• https://en.wikipedia.org/wiki/Continuous_auditing<br>• https://en.wikipedia.org/wiki/Regulatory_compliance |