U.S. FDA TITLE 21 CFR PART 11 COMPLIANCE ASSESSMENT OF SAP NetWeaver® AUDIT MANAGEMENT FUNCTIONALITY

Disclaimer

These materials are subject to change without notice. SAP AG's compliance analysis with respect to SAP® software performance based on U.S. FDA Title 21 CFR Part 11: (i) in no way expresses the recognition, consent, or certification of SAP software by the U.S. Food and Drug Administration; and (ii) applies to certain components of SAP audit management functionality only as stated herein. The customer is solely responsible for compliance with all applicable regulations, and SAP AG and its affiliated companies ("SAP Group") have no liability or responsibility in this regard. These materials are provided by SAP Group for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

CONTENTS

SUMMARY

Based upon SAP AG's interpretation of the U.S. Food and Drug Administration (FDA)Title 21 CFR Part 11 rule and the functions and features discussed within this document, SAP AG believes that the audit management functionality of the SAP NetWeaver® platform fully complies with FDA Title 21 CFR Part 11. (Audit management functionality was formerly part of the SAP Product Lifecycle Management application.)

FDA TITLE 21 CFR PART 11 ASSESSMENT

Audit Management

Audit management functionality is available in all SAP® solutions based on the SAP NetWeaver® platform, such as the SAP Product Lifecycle Management, SAP ERP, SAP Supplier Relationship Management, and SAP Customer Relationship Management applications.

This investigation is valid for all releases using SAP Web Application Server 6.10 or higher and the SAP NetWeaver Application Server component (see SAP Notes service, reference 937139).

Security

Depending on the release, the audit management functionality is built on either SAP NetWeaver Application Server or SAP Web Application Server. Therefore, all security features of SAP NetWeaver Application Server or SAP Web Application Server are valid for the audit management functionality. Both fulfill the FDA Title 21 CFR Part 11 security requirements. In the section titled "Compliance of Audit Management with FDA Title 21 CFR Part 11," the statements for SAP NetWeaver Application Server are valid for SAP Web Application Server as well.

Electronic Records

FDA Requirements

The FDA requires the ability to log and track changes made to business objects and dependent objects in a compliant software environment. The computer system must provide functionality to log changes, and to log the creation and deletion applied to business objects and to dependent objects such as configuration data. The minimal necessary information the system must provide is:

- Old value of an attribute of the changed business object
- New value of this attribute
- Person who changed the value
- Date and time of change
- Action (create, modify, delete)

Change, Status, and Authorization Management of Audit Components

The administrative data of all data object types can be viewed according to the person making the change ("created by" or "last changed by"), when an object was created, or the latest change ("created on," "last changed on"). In addition, change documents can be created for all data-object types (components) used in the software. The change document creation must be switched on in the configuration of the system. For the time stamp, the **application server time** is used within the change documents. The change itself is tracked as well. Changes in short texts are tracked; in long texts, only changes in SAP script are indicated. SAP script can be customized so that existing texts can only be extended, but not changed. Thus long texts can be tracked as well.

Status management is available for the audit management functionality. The status sequence is predefined in the system (system status) and can be supplemented by the user (user status). The current status can be viewed and checked at any time.

The efficient authorization check can be refined to the point that system users can execute only the functions directly relevant to their tasks. The authorization check as delivered by the standard software is very granular by itself, although, if necessary, a business add-in (BAdI) (PLM_AUDIT_AUTH_CHECK) enables enhancement of the authorization functionality.

Versioning of audit components is also possible. For example, the audit object is copied completely and the new external identification indicates that it is a new version of the original audit component. The original audit component is locked via status management and is now considered an old version of the object. During BAdI implementation for audit objects, an automatic versioning of the external identifiers after copying of an object can be considered.

Digital Signature

In audit management, signatures play a role at least in one part. The audit result is reported in an audit report. Normally, both the auditor and the audited party sign the audit report, which they have agreed on and printed. In the system, this signature is represented by a status of the **audit** data object. If the signature itself must be documented and verified, you can scan the signed report into the system and assign the resulting document to the audit. You can also use digital signatures for signature verification purposes if the technical prerequisites for the identification of the signing parties exist in your system.

Audit management provides the BAdI PLM_AUDIT_SIGNATURE to allow the integration of any signature method. SAP provides the encapsulated digital signature tool, which offers functionality in compliance with FDA Title 21 CFR Part 11. It can be implemented with minimal effort in a customer project. The prerequisite is an SAP basis release 6.20. Audit management functionality is ready for the implementation of a single-stage signature strategy.

Audit management is part of the SAP-ABA layer, as is the digital signature tool. A display function for the digital signature protocol must be realized in a customer project as well: it can be programmed in analogy to transaction DSAL, which is available in the SAP application layer. You can find further details concerning the encapsulated digital signature tool in SAP Notes 700495, which includes an attachment of the related implementation guide.

Compliance of Audit Management Functionality with FDA Title 21 CFR Part 11

The following table summarizes how audit management functionality complies with each requirement of Part 11.

Part 11 Clause	SAP Assessment of Audit Management
11.10(a)	The data object types of the audit management functionality provide adequate audit trails that can be reviewed for information. These records are secured from unauthorized access.
11.10(b)	All electronic records generated in audit management functionality are accurate, complete, and presented in a human-readable format. Audit management electronic records can be printed or exported into several industry-standard formats such as Adobe PDF and XML.
11.10(c)	All electronic records within audit management functionality can be maintained in the active database or archived to accommodate all required retention periods even when software is upgraded. Access to these records is secured using standard SAP® authorization profiles. In addition, audit management functionality maintains the link between electronic signatures executed to electronic records even after archiving.
11.10(d)	Robust security administration and authorization profiles assure system access. Changes to security profiles are recorded in the SAP NetWeaver® Application Server (SAP NetWeaver AS) component.
11.10(e)	Audit management functionality can be configured so that electronic records are generated for creating, modifying, or deleting data. If configured accordingly, these records are date- and time-stamped and include the user ID of the individual who is logged onto the system and performed the action. The electronic change documents will maintain the old and new values of the changed fields and the user who generates the record. Complementing the requirement in 11.10(c), all electronic records can be maintained in the active database or archived to accommodate all required retention periods. In addition, audit management functionality maintains the link between electronic signatures executed to electronic records.
11.10(f)	Via the status management functionality within audit management, the proper sequence of operations as required by the applicable regulation can be enforced.
11.10(g)	SAP NetWeaver AS executes authority checks in conjunction with its robust security administration and authorization profiles to ensure that only authorized individuals can access the system, electronically sign a record, and access or perform the operation at hand. SAP NetWeaver AS also records changes to authorization profiles.
11.10(h)	N/A

Part 11 Clause	SAP Assessment of Audit Management
11.10(i)	The product innovation life cycle for SAP development requires that all personnel responsible for developing and maintaining SAP NetWeaver AS have the education, training, and experience to perform their assigned tasks. A wide range of additional education and training offerings and regular assessments of individual training requirements ensure a process of continuous learning for SAP staff involved in the development and support of all SAP software.
11.10(j)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the computer system.
11.10(k)	N/A
11.30	For open systems, SAP NetWeaver AS supports interfaces with complementary software partners that supply cryptographic methods such as public key infrastructure (PKI) technology.
11.50(a)	The encapsulated signature tool can be implemented in agreement with FDA Title 21 CFR Part 11 with minimal effort in a customer project. The following information is captured: ▪ Printed name of the signer ▪ System date and time when the signature was executed ▪ The meaning (such as review, approval, responsibility, or authorship) associated with the signature
11.50(b)	N/A
11.50(b)	The encapsulated signature tool can be implemented to satisfy these requirements.
11.70	The encapsulated signature tool can be implemented to satisfy these requirements.
11.100(a)	The encapsulated signature tool can be implemented to satisfy these requirements.
11.100(b)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the computer system.
11.100(c)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the computer system.
11.200(a)(1)	SAP NetWeaver AS requires two distinct components – a user ID and a password – to perform any electronic signature. By design, SAP NetWeaver AS does not support continuous sessions where only a single component is necessary subsequent to the first signing.
11.200(a)(2)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the computer system.
11.200(a)(3)	SAP NetWeaver AS user and security administration functions ensure that the attempted use of an individual's electronic signature by anyone other than the genuine owner requires the collaboration of two or more individuals.
11.200(b)	SAP NetWeaver AS provides a certified interface to biometric devices such as fingerprint and retinal scanning devices. Certified vendors are listed in the SAP partner directory on the SAP Service Marketplace extranet.
11.300(a)	SAP NetWeaver AS user and security administration functions provide the necessary controls to ensure that no two individuals have the same combination of identification code (user ID) and password.
11.300(b)	SAP NetWeaver AS can be configured to force users to change passwords at various intervals and provides system checks to prevent users from repeating passwords or using combinations of alphanumeric characters that are included in the user ID. User IDs can also be invalidated when necessary, such as when an employee leaves the company.
11.300(c)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the computer system.
11.300(d)	SAP NetWeaver AS fulfills this requirement and behaves as demanded by the requirement.
11.300(e)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the computer system.

REFERENCES

For more information, look up the following references, many of which are found in the SAP Service Marketplace extranet (authorization required):

- help.sap.com: SAP NetWeaver 2004 Security Guide
- help.sap.com: SAP NetWeaver 2004s Security Guide
- SAP Web Application Server Security Guide (ABAP and Java) (SAP NetWeaver 2004)
- SAP White Paper "Complying with U.S. FDA Title 21 CFR Part 11 for the Life Sciences Industry"
- SAP White Paper "SAP NetWeaver – Providing the Building Blocks for Effective Governance, Risk, and Compliance Management"
- SAP Notes 700495 attachment "Digital Signature Tool – Implementation Guide"
- FDA Title 21 CFR Part 11 Electronic Records; Electronic Signatures: Final Rule, March 1997
- Product Description "Audit Management," Karl F. Westermann on SAP Service Marketplace
- help.sap.com: Audit Management
- Audit Management: Availability of software component – SAP Notes 937139

Authors: Dr. Anja Modler-Spreitzer and Dr. Christoph Roller, IBU Consumer Products & Life Sciences, SAP AG

www.sap.com/contactsap

50 083 541 (07/03)

THE BEST-RUN BUSINESSES RUN SAP™