FDA 21 CFR Part 11 - White Paper

U.S. FDA Title 21 CFR Part 11 Compliance Assessment of ELOprofessional and ELOenterprise ECM Software

Disclaimer

These materials are subject to change without notice. ELO Digital Office GmbH´s compliance analysis with respect to ELO software performance based on 21 CFR Part 11: (i) in no way expresses the recognition, consent, or certification of ELO software by the United States Food and Drug Administration; and (ii) applies to certain components of ELOprofessional and ELOenterprise only as stated herein. The customer is solely responsible for compliance with all applicable regulations, and ELO Digital Office GmbH has no liability or responsibility in this regard. These materials are provided by ELO Digital Office GmbH for informational purposes only, without representation or warranty of any kind, and ELO Digital Office GmbH shall not be liable for errors or omissions with respect to the materials. The only warranties for ELO Digital Office GmbH 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

1 Overview of the most important compliance features

The following provides an overview of the most meaningful features in ELO Software that cover the central requirements in 21 CFR Part 11.

1.1 Electronic records

ELO Software can be configured so that existing records are versioned, cannot be changed, and cannot be deleted, in order to keep fixed all steps in changes to records or to choose to preserve electronic records permanently.

ELO Software is designed for long-term archiving and supports by default conversion to print formats including TIFF, CCITT, Fax G4 and PDF, which allows stored information to be read now and in the future.

1.2 Audit trail

In order to generate a complete verification for all stored records, the entire lifecycle of a record is recorded from creation to disposition (Record Life Cycle Management). In detail, this means that all processes that generate, change, or delete records are stored along with the date, time, and user identification.

By saving user actions and linking them to files, all relevant file actions down to simply viewing a file can be traced to specific persons and can be tracked back and proven without doubt.

The same applies to the allocation of user permissions to files and repository structures. Each assignment of permissions and changes to same are logged for users and user groups. Naturally, inheritance mechanisms for user rights make it easier to work and keep an overview and are taken into account in these logs.

With this, ELO Software allows the perfect reconstruction of the course of user permission assignments and allows, for example, for verification and transparent reporting of segregation of duties.

The verification records can be viewed at any time by authorized users, and contain all information required for complete and unrestricted electronic verification.

Complete copies can be provided to auditors in readable or electronic format, auditors can also be given a portable ELO repository to take with them that is identical to the original, or they can be given a comprehensive look into the existing repository through corresponding user permissions.

The traceability in regard to changes to electronic records and user rights is, in any case, ensured.

1.3 Security

ELO Software exceeds the security requirements of 21 CFR Part 11 through a series of preventive and detective measures.

In addition to the traditional password-user identification pairs to attain access permissions, passwords can be assigned limited periods of validity and be given defined requirements for password length and structure. This allows requirements for upper and lower-case letters, numbers, and special characters to be enforced, in order to make authentication more secure and to apply existing password rules or company policies. To minimize risk, information about passwords is stored using cryptographic security.

Numerous additional protection mechanisms enable unauthorized access attempts to the ELO Software system to be recognized, made more difficult, and prevented. Reports that log unauthorized access attempts at a level of detail that includes the IP address, as well as time delay and attempt limitation components that make failed attempts at password entry limited and more difficult, are important elements in effective protection of authorizations.

To maintain the integrity of stored information, changes to the content of records that were made without the cooperation of the ELO Software can be securely proven through the automatic use of cryptographic keys.

With higher security requirements, it is possible to encrypt some or all electronic records according to the requirements of the organization, in order to make the use of ELO Software even more secure in open systems, such as when outsourcing an archive to external service providers.

1.4 Permissions concept

The fundamental permissions concept used by the ELO Software performs permission checks in combination with a robust security management and user profile system, in order to only allow authorized persons access to electronic records and signatures.

System access is restricted to authorized persons. It is possible to assign defined action rights to record structures and electronic records to individuals and groups. Inheritance of these rights into subordinate record structures and links to logical functions for multiple assignments makes it easier to assign authorizations and to retain an overview of authorizations.

The use, integration, and application of pre-existing permission and authorization concepts from Active Directory systems like LDAP into the ELO Software system is part of normal practices of use.

1.5 Electronic signatures

To uniquely assign record editing to users, connections between electronic signatures and electronic records are automatically and permanently established and maintained, which equates electronic signatures to written signatures.

When doing so, of course, recognized encryption methods guarantee that these connections are not excised, copied, or otherwise transferred or able to be falsified by ordinary means.

ELO Software uses every signature as unique to one individual, does not reuse the signature, and does not reassign it to anyone else, in order to keep the electronic signature analogous to the written signature.

In order to reduce time-based aspects in regard to attempted misuse of electronic signatures, the entry of user identification and password is required for each signature in a continuous session. If a continuous session is interrupted, it is again necessary to enter one's identification code and password.

For the highest security requirements for digital signatures, ELO Software may also be used in combination with encapsulated digital signature software. The integration of the signature software can occur over existing, defined interfaces with the ELO Software or in other ways.

1.6 Workflow

For use in predefined work processes and to ensure quality requirements on work products, such as with tiered approval policies or the double verification principle, ELO Software possesses comprehensive abilities to define, display, and run workflows to edit electronic records.

Document editing processes that occur in sequence or in parallel are supplemented by mechanisms for case decision, delegation, substitution, and escalation, as well as warnings when the time allotted to processing documents has been exceeded. This ensures that typical work situations are kept under control and that the work and document flow can proceed according to policy.

The editing status of each electronic document can be specified through a freely defined document status at each work step. All permitted work steps can be defined, and each document status valid for a work step can be viewed and audited, resulting in subsequent actions being determined and known at all times.

For auditing purposes, all work steps and the status are logged and saved in the order in which processing occurs. They can be viewed by authorized users at any time. The same applies to the workflow itself: every change to its schematic progression can be logged, stored, and viewed.

2 Assessment Scope

All FDA Title 21 CFR Part 11 investigations have been carried out for the ECM Suite 9, ELOprofessional 9, and ELOenterprise 9, and apply to these and all future versions of ELOprofessional and ELOenterprise unless stipulated otherwise. This software is referred to as ELO Software in the following.

3 About software properties

Enterprise Content Management (ECM) software must fulfill a large number of requirements in order to be successful on the market. In doing so, it is especially meaningful to adhere to the regulatory requirements, which can, for example, be completely different depending on the country, sector, or area of use of the software. As a result, the software must possess sufficient properties to accord to all desired requirements.

ELO Digital Office GmbH cannot, however, provide "validated software" as a manufacturer of Enterprise Content Management (ECM) software, because many requirements of FDA 21 CFR Part 11 go beyond functional software properties, affecting the operative and technical use by the users. A validation can only be undertaken in a concrete application case and environment.

ELO Digital Office GmbH understands itself to be obligated to provide the users of its software in industries regulated by the Food and Drug Administration (FDA) with the best possible preconditions and reliable information about the ability to validate its software and IT systems. This is why ELO Digital Office GmbH provides information on the existing software properties for each functional software requirement in FDA 21 CFR Part 11.

With this high degree of transparency, we provide the users of our software the ability and comfort to confirm in detail the compliance with the requirements of FDA 21 CFR Part 11 directly with existing software properties. This means you can use this assessment report optimally for all validation and audit processes.

4 FDA Title 21 CFR Part 11 Compliance Statement

On the basis of the interpretation of the FDA Title 21 CFR Part 11 rule of the U.S. Food and Drug Administration and the functions and features discussed within this document, ELO Digital Office GmbH is confident that the ELO Software applications fully comply with FDA Title 21 CFR Part 11.

5 General Principles

ECM systems are typically run together with database systems, and in some cases with special closed software and/or hardware components to increase authorial identification and/or data integrity. ELO Software then provides the software properties that other systems and components are unable to provide to fulfill the requirements of FDA 21 CFR Part 11.

6 How ELO Software complies with FDA Title 21 CFR Part 11

The following table summarizes how ELO Software complies with each requirement of Part 11.

Part 11 Clause	ELO Software Assessment Findings
§11.10 (a)	ELO Software can be configured to store performed activities with an electronic signature centrally in a database. Activities are recorded along with the date, time, user, and additional attributes in a readable format. The database can be viewed by authorized persons at any time and contains all information required for a proper audit trail. If the contents of electronic recordings are altered after creation without the cooperation of the ELO Software, this can be securely proven.
§11.10 (b)	ELO Software possesses the ability to generate accurate and complete copies of all records in electronic form. ELO Software possesses the ability to generate accurate and complete copies in human readable form for printable records. Standards-compliant conversions into the TIFF, CCITT, Fax G4, and PDF print formats are supported. Direct display of many document types is possible through the application that created the document.
§11.10 (c)	Information on electronic records is kept and archived in a database in order to ensure all required retention periods are fulfilled, even if the software is updated. The ELO Software establishes a long-term connection between electronic signatures and electronic records and makes this connection permanent.
§11.10 (d)	ELO Software supports limiting system access to authorized individuals by enabling the assignment of defined action rights to record structures and electronic records to individuals and groups. Inheritance of these rights into subordinate record structures and logical functions for multiple assignments makes it easier to assign authorizations and to retain an overview of authorizations. Alternatively, ELO Software supports the use of existing permission concepts by connecting to and using existing Active Directory systems (such as LDAP).

Part 11 Clause	ELO Software Assessment Findings
§11.10 (e)	ELO Software automatically records to a database all processes that create, modify, or delete electronic records with the date, time, and user ID. ELO Software can be configured so that existing records are versioned, cannot be changed, and cannot be deleted. The versioning of electronic records makes changes in subsequent editing steps displayable and understandable in detail.
§11.10 (f)	ELO Software possesses the comprehensive ability to define, display, and run workflows to process electronic records. The document status, which mirrors the current processing state of the electronic record or subsequent actions, as well as permitted editing steps can be defined, displayed, and audited. Orderly document processing is supplemented by mechanisms for delegation, substitution, and escalation, as well as warnings when the time allotted to processing documents has been exceeded. For auditing purposes, all work steps and the status are logged and saved in the order in which processing occurs.
§11.10 (g)	ELO Software performs permission checks in combination with its robust security management and permission profiles in order to ensure that only authorized persons have access to electronic records and signatures. ELO Software allows the progression of access rights to electronic records to be reconstructed.
§11.10 (h)	This clause covers a procedural requirement for customers and is not related to functions or capabilities of ELO Software.
§11.10 (i)	Employees of ELO Digital Office GmbH are assigned tasks corresponding to their education, technical knowledge, and experience. Most employees of the Development department possess degrees in Informatics. All new employees receive training on the products, processes, and the company. ELO Academy provides employees and business partners with a comprehensive palette of introductory and advanced product training. Additional and advanced qualifications are planned and undertaken by all employees. Business partners are only allowed to offer products to end customers after previously undergoing product training.
§11.10 (j)	This clause covers a procedural requirement for customers and is not related to functions or capabilities of ELO Software.

Part 11 Clause	ELO Software Assessment Findings
§11.10 (k)	ELO Digital Office GmbH provides in-program documentation, appropriate manuals, and additional documentation for each version of the ELO Software, including for updates, and therefore fulfills its role in providing proper system documentation.
§11.30	ELO Software supports the use of open systems through the ability to encrypt electronic records and to sign them with complementary and encapsulated signature software. Defined interfaces are available for the signature software, which can be integrated into ELO Software and is provided by software partners. Other signature software can be adapted for use as well.
§11.50 (a)	Electronic signatures contain the name of the person signing the document, as well as the date and time the signature was applied. The meaning (such as review, approval, responsibility, or authorship) associated with the signature is the duty of the company that implements the ELO Software and is not related to the functions or abilities of the ELO Software.
§11.50 (b)	The electronic signature, along with the person who signed the document and the date and time, is stored along with every electronic record. Electronic records may be searched, displayed, and printed by signer, date, and additional criteria. ELO Software possesses the ability to generate accurate and complete copies of all records in electronic form.
§11.70	ELO Software automatically links electronic signatures with their respective electronic record. ELO Software ensures that this link is not excised, copied, or otherwise transferred or able to be falsified by ordinary means. The requirement for handwritten signatures executed to electronic records is based upon biometric devices and is not related to functions or capabilities of ELO Software.
§11.100 (a)	ELO Software uses every signature as unique to one individual, does not reuse the signature, and does not reassign it to anyone else. Additionally, this clause covers procedural requirements for customers.
§11.100 (b) - (c)	These clauses cover procedural requirements for customers and they are not related to functions or capabilities of ELO Software.

Part 11 Clause	ELO Software Assessment Findings
§11.200 (a1)	Two distinct components are always required for the electronic signature: an identification code (user ID) and a password. Every signature of a continuous session with controlled system access requires the entry of the identification code and the password. If a continuous session is interrupted, it is again necessary to enter the identification code and the password.
§11.200 (a2)	This clause covers a procedural requirement for customers and is not related to functions or capabilities of ELO Software.
§11.200 (a3)	The documented and instructed security concept of the ELO Software contains measures that ensure that the attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals.
§11.200 (b)	This clause covers a requirement for electronic signatures based upon biometric devices and is not related to functions or capabilities of ELO Software.
§11.300 (a)	ELO Software maintains the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
§11.300 (b)	ELO Software supports password security measures by providing the ability to limit the time of password validity and to define specific requirements for password length and structure. Information about passwords is saved cryptographically. User access can be blocked. Additionally, this clause covers procedural requirements for customers.
§11.300 (c)	This clause covers a procedural requirement for customers and is not related to functions or capabilities of ELO Software.
§11.300 (d)	ELO Software enables the detection of attempts of unauthorized use and provides configurable protection measures that record, make more difficult, and hinder the use of passwords and/or identification codes by unauthorized persons. Additionally, this clause covers procedural requirements for customers.

7 Reference and Related Documents

a) Reference Documents

- Title 21 FDA Part 11 Electronic Records; Electronic Signatures; Food and Drug Administration Department of Health and Human Services, March 1997
- Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application; U.S. Department of Health and Human Services, Food and Drug Administration et al., August 2003

b) Related Documents

The ELO SupportWeb (http://forum.elo.com/supportweb/, registration required) provides additional support documentation for use, in particular:

- Manuals and
- FDA 21 CFR Part 11 - Notes on implementation