EU Annex 11 Compliance Assessment

Veeva delivers regulated content management applications for every major part of a life sciences company, from R&D, to clinical trials, quality and manufacturing, and global regulatory approvals.

Veeva R&D applications are built on the Vault Platform, and designed to manage regulated documents for life sciences organizations, as well as produce secure and compliant audit trails and electronic signatures in accordance with Eudralex GMP Volume 4 Annex 11, the FDA's 21 CFR Part 11, and other industry compliance standards and guidance.

These standards and guidance define regulatory compliance requirements for the validation and maintenance of computer systems used for managing regulated records that are mandated as part of life sciences product development and marketing activities.

As a modern cloud provider, Veeva deploys and maintains software applications that satisfy predicate rule requirements such as those found in GLP (Good Laboratory Practices), GCP (Good Clinical Practices), and CGMP (Current Good Manufacturing Practices).

About this Document

The purpose of this document is to provide clarification and guidance for customers regarding the applicability of the Eudralex GMP Volume 4 Annex 11 requirements to Veeva processes, personnel, and products. Each section and sub-text of EU Annex 11 was evaluated for relevance to Veeva practices and Veeva Vault. Where applicable, a statement of compliance is recorded.

Customer responsibilities have been highlighted where applicable. Full compliance may require a function or feature implemented in Veeva software products, or a service Veeva performs in support of customers' predicated activity.

About EU Annex 11

In June of 2011, the European Commission (Health and Consumer Directorate) updated the Computerised System Annex to the EU EudraLex GMP, Volume 4. According to the agency, the Annex "*has been revised in response to the increased use of computerised systems and the increased complexity of these systems*."

Annex 11 is divided into 17 sections, and describes application controls (e.g., audit trails), process controls (e.g., incident management), and quality management philosophies that are to be implemented for computerized systems used in GMP activities.

Annex 11 Controls

Annex 11 Section	Annex 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
1. Risk Management					
§1. Risk Management	Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerized system.	Veeva has implemented a comprehensive Computer Systems Validation (CSV) program codified in policy and further detailed in procedure. CSV deliverables are reviewed and approved by the Veeva Quality Unit. All software releases included a validation risk and impact assessment. Our risk management policies and procedures define the requirements and approach to risk management and clearly delineate its applicability throughout the product lifecycle.	—	X	—
		Customers are responsible for the demonstration that the product has been configured in their environment and has been risk-assessed for its impact on patient safety, data integrity, and product quality.	—	—	X
2. Personnel					
§2. Personnel	There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT.	Veeva procedures clearly define roles and responsibilities across related processes. Process inputs and outputs are defined in procedure. Service Level Agreements (SLAs) are in place between Veeva and its customers to define the roles and responsibilities.	—	X	X

Annex 11 Section	Annex 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
	All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	Veeva has implemented policies, procedures, and training processes to ensure the qualification of staff who develop and maintain Electronic Records and Electronic Signatures (ERES) systems. Training records are maintained and demonstrate the qualification of individuals in relation to their assigned duties.	—	X	—
		We advise that customers provide training to end users of the system in order to conform to this section of the regulation. Veeva professional services assists customers in meeting this requirement by providing “train the trainer” services as a standard part of our implementation.	—	—	X
3. Suppliers and Service Providers					
§3.1	When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.	Formal agreements have been established with all service providers. SLAs are in place between Veeva and its customers to define the roles and responsibilities.	—	X	X
§3.2	The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	Supplier management has been defined in Veeva policies and procedures. Veeva performs audit and vendor assessments on it suppliers and has adopted a risk-based model for scheduling and scoping a supplier audit.	—	X	—
		Veeva allows its customers to perform their due diligence either through a supplier questionnaire or on-site audit.	—	X	X
§3.3	Documentation supplied with commercial off-the-	As part of each release, Veeva provides a comprehensive	—	X	—

Annex 11 Section	Annex 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
	shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	collection of validation documents to all customers on request.			
		We advise customers to review release notes and all accompanying validation deliverables to ensure customer requirements are met and the system is fit for use.	—	—	X
§3.4	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	The records of our audit management program, including supplier management, are maintained in the Veeva QMS and are available for inspections on request.	—	X	—
4. Validation					
§4.1	The validation documentation and reports should cover the relevant steps of the lifecycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	As part of each release, Veeva provides a comprehensive collection of validation documents that cover the relevant steps of system lifecycle and risk assessment.	—	X	—
		Customers are responsible for demonstrating that the system has been configured to meet their business requirements and is fit for use. This demonstration may come in the form of a PQ or UAT and must be performed under the customer's QMS.	—	—	X
§4.2	Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	Veeva policies and procedures define change and deviation management. A formal deviation observation is conducted prior to implementation in a production environment.	—	X	—
§4.3	An up-to-date listing of all relevant systems and their GMP functionality (inventory) should be available.	Customers should maintain a listing of all relevant systems and their GMP functionality. Veeva maintains a comprehensive inventory of all systems and software used in the product development and maintenance process.	—	X	X

Annex 11 Section	Annex 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
	For critical systems an up-to-date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.	Customers should maintain up-to-date descriptions for critical systems. Veeva Vault specifications and diagrams define and confirm the hardware and software components, interfaces, and security measures that make up the system.	X	—	X
§4.4	User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact.	The Veeva Vault Business Requirements Definition (BRD) documents describe the "required functions of the computerized system" based on a validation impact assessment that evaluates the GxP relevance of the functions in question.	—	X	—
	User requirements should be traceable throughout the lifecycle.	User requirements, defined in our BRDs, are traceable both forwards and backwards throughout the lifecycle.	—	X	—
§4.5	The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.	Veeva has established a customer audit program to allow regulated users to perform their regulatory due diligence. In addition to hosting on-site audit, Veeva has implemented a remote audit capability to allow customers access to select documents in support of their own inspectional obligations.	—	X	—
§4.6	For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the lifecycle stages of the system.	Veeva has established Key Process Indicators (KPI) to measure quality and performance against all published Key Process Areas (KPA) within our QMS.	—	X	—
§4.7	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered.	Test methods and scenarios are clearly defined in the Veeva Vault validation project plan and further detailed in validation test scripts.	—	X	—
	Automated testing tools and test environments should have documented assessments for their adequacy.	Veeva automated testing tools have documented assessments of adequacy. The vendors for testing tools are evaluated through our supplier management program.	—	X	—

Annex 11 Section	Annex 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
§4.8	If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	Data migration, if required, is performed by our professional services group, or by a third party integrator. Data verification requirements and methods should be documented within the customer's quality framework.	—	—	X
5. Data					
§5. Data	Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	Veeva Vault uses encryption to ensure the security of all data transfers and digital certificates to ensure authenticity.	X	—	—
6 Accuracy Checks					
§6 Accuracy Checks	For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	Veeva products can enforce correct data entry in accordance with customer system rules and configurations that map to business processes and data entry risks.	—	—	X
7. Data Storage					
§7.1	Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.	Veeva has implemented a common, secure architecture for all its products to ensure accurate and ready retrieval throughout the records retention period.	X	—	—
		Veeva hosts and operates its software on servers located in secure data centers.	—	X	—
§7.2	Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	Customer data is protected through monitored incremental and full backups and a routinely tested disaster recovery policy.	—	X	—

Annex 11 Section	Annex 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
8. Printouts					
§8.1	It should be possible to obtain clear printed copies of electronically stored data.	Veeva Vault allows for documents stored within the system to be printed. Veeva Vault reports are configurable to display and print information stored in the system, including associated metadata.	X	—	—
§8.2	For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	Reports are configurable for records stored in Veeva Vault, including those that support batch release, to display and print information on the version history indicating if any of the data has been changed since the original entry.	X	—	—
9. Audit Trails					
§9. Audit Trails	Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail").	Veeva Vault provides functionality to "*record all GMP-relevant changes and deletions.*" The system-generated audit trail is accessible to the system administrator for review.	X	—	—
	For change or deletion of GMP-relevant data the reason should be documented.	Veeva Vault audit trails are system-generated, and capture the reason for a change to data.	X	—	—
	Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	Veeva Vault audit trails are available to customer system administrators and can be reviewed at will.	X	—	—
10. Change and Configuration Management					
§10. Change and Configuration Management	Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	Change management is applied to all releases of Veeva software products. Our policies and procedures define the process for ensuring that system changes and configurations are performed in a controlled manner. Any changes made to our products, both corrective and perfective, are documented, reviewed, and approved prior to implementation in a production environment.	—	X	—

Annex 11 Section	Annex 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
		Changes to customer-specific configurations of Veeva Vault must be documented within the customer's change management program.	—	—	X
11. Periodic evaluation					
§11. Periodic evaluation	Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Periodic review requirements for computerized systems have been defined in Veeva policy and procedure. Periodic review of Veeva Vault is performed every two years, and includes an evaluation of "*deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports*."	—	X	—
12. Security					
§12.1	Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	Veeva software products are hosted in world-class, secure facilities. Data center vendors, and their facilities, are audited against SSAE16, and have physical controls in place such as proximity badges, biometrics, and 24/7 security.	—	X	—
		Veeva Vault enforces user ID and password access and provides for role-based security profile configurations, ensuring that only authorized individuals have access to system functions.	X	—	—
§12.2	The extent of security controls depends on the criticality of the computerised system.	Veeva Vault is designed with security controls that can be configured by customers in accordance with their security policies.	X	—	—
		Customers may configure Veeva Vault to conform to their security policies, and define roles and privileges to align with their business requirements.	—	—	X
§12.3	Creation, change, and cancellation of access authorisations should be recorded.	Veeva Vault has a system-generated, secure audit trail that captures user entries and actions associated with the creation, modification, and deletion of system records. The audit trail information is available to system administrators for review and	X	—	—

Annex 11 Section	Annex 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
		download.			
§12.4	Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	Veeva Vault provides functionality to "*record the identity of operators entering, changing, confirming or deleting data including date and time.*" This is performed by a system-generated audit trail that is accessible to the system administrator for review.	X	—	—
13. Incident Management					
§13. Incident Management	All incidents, not only system failures and data errors, should be reported and assessed.	Veeva policies and procedures ensure that all incidents are defined, reported, and addressed. Customers can report incidents via our customer portal.	—	X	—
	The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	Veeva CAPA policies and procedures define the process for driving corrective and preventative actions in response to critical incidents.	—	X	—
14. Electronic Signature					
§14. Electronic Signature	Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.	The signature manifestation associated with signed records in Veeva Vault includes (a) the printed name of the signer; (b) the date and time when the signature was executed; and (c) the meaning of the signature. The system enforces the consistent application of these components. Vault prevents all system users, including administrators, from excising, copying, or otherwise transfering electronic signatures through ordinary means.	X	—	—
15. Batch release					
§15. Batch release	When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record	Veeva Vault includes a role-based security model that can be configured to record and restrict system access to "Qualified Persons."	X	—	—

Annex 11 Section	Annex 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
		We advise customers to review their policies and procedures and modify them accordingly to ensure that the user roles and profiles are configured to conform to their company's security requirements.	—	—	X
	This should be performed using an electronic signature.	Veeva Vault allows for full ERES-compliant electronic signature functionality.	X	—	—
16. Business Continuity					
§16. Business Continuity	For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system).	Veeva maintains fully redundant hardware and software configurations in separate, geographically distinct data centers. Customer data is automatically replicated between primary and secondary data centers at regular intervals.	X	—	—
		Our business continuity and disaster recovery plans ensure the continuity of business processes facilitated by Veeva Vault.	—	X	—
	The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports.	Our disaster recovery plans define the "time required to bring the alternative arrangements" for Veeva Vault in the form of a Recovery Point Objective (RPO) and Recovery Time Objective (RTO) from the disaster declaration.	—	X	—
	These arrangements should be adequately documented and tested.	Veeva performs periodic disaster recovery exercises in accordance with established, documented plans.	—	X	—
17. Archiving					
§17. Archiving	Data may be archived. This data should be checked for accessibility, readability and integrity.	Veeva does not archive data for customers into a separate archival system. During the contracted engagement with Veeva, customer data is maintained in the same secure and accessible repository as active documents.	—	—	X
	If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	Upgrades to Veeva Vault are tested to ensure that all existing system data can be retrieved. Additionally, data can be retrieved via the Vault API.	X	—	—

Terms and Definitions

Term	Definition
API	Application Programming Interface
CFR	Code of Federal Regulations (US)
Cloud	Remote computing via the Internet with little local resource use
CSV	Computerized System Validation
ERES	Electronic Records and Electronic Signatures
GCP	Good Clinical Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
QMS	Quality Management System
HR	Human Resources
PQ	Performance Qualification
UAT	User Acceptance Testing
Vault	Veeva's Regulated Content Management System

References

EudraLex Good manufacturing practices, Volume 4, Annex 11.