Audit Checklist

SaaS
Cloud Service Providers

Name and Role	Date
Authors: Dr Wolfgang Schumacher Michael Wegmann	01- 01-
Technical Review: Yves Samson Dr Andreas Mangel On behalf of the ECA IT Working Group (Cloud Computing Team)	01- 01-
Approved by: Oliver Schmidt On behalf of ECA	01-

Contents

Document Revision History

Version	Date	Reason for Change	Status
V 1.0		New Document	Released

Instructions: Respond to every question in the "Response" column with one of the following acceptable answers: Yes (Y), No (N), or Not Applicable (N/A). Document and identify supporting material that was examined for each question. Enter comments in the cases where further clarification or explanation of observations may be needed.

SECTION 1: OVERVIEW

No.	Question	Response / Comments
a.	Provide overview of visit including objectives and goals:	Review cloud service provider processes and documentation for infrastructure/platform qualification, Change Management, SDLC (Requirements, Development, Testing, Deployment, and Maintenance), Part 11 & Annex 11 compliance, Data Exchange, Security, and Technology.
b.	What are the types of products and services the cloud service provider markets?	
c.	What is the cloud service provider's commitment to FDA & EMA (as applicable) regulated companies? Does the provider understand the regulations, constraints and standards especially for GxP – regulated data and adhere to highly regulated process driven environment?	
d.	Does the provider have any life science company clients that stores GxP data on their cloud? Can cloud service provider provide references?	

SECTION 2: INFRASTRUCTURE OVERVIEW

No.	Question	Response	Objective Evidence/Comments
a.	Is the infrastructure (e.g. servers, LAN components, databases, etc) commissioned (tested) and documented as per GAMP5 standards?	☐ Y ☐ N ☐ N/A	

SECTION 3: PLATFORM OVERVIEW			
No.	**Question**	**Response**	**Objective Evidence/Comments**
a.	Is the platform (e.g. global and shared APIs, etc) commissioned (tested) and documented as per GAMP5 standards?	☐ Y ☐ N ☐ N/A	

SECTION 4: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) OVERVIEW			
No.	**Question**	**Response**	**Objective Evidence/Comments**
4.1	**Methodology**		
a.	Is a formal SDLC methodology (e.g. documented requirements, specifications, test scripts) comprised of procedures, endorsed by management and used for all system development projects?	☐ Y ☐ N ☐ N/A	
b.	Is there a procedure for software/hardware/ platform changes (e.g. bug fixes, enhancements)?	☐ Y ☐ N ☐ N/A	
c.	What is the frequency of changes of each type?	☐ Y ☐ N ☐ N/A	
d.	How are release cycles documented and communicated to clients?	☐ Y ☐ N ☐ N/A	
e.	How much time do clients have to perform the impact assessment on their application and ready for unit testing?	☐ Y ☐ N ☐ N/A	
f.	Do hardware or software changes follow the same methodology as initial development of the product?	☐ Y ☐ N ☐ N/A	
g.	Does the release process for enhancements include full documentation of new functions by updating operating manuals and release notes?	☐ Y ☐ N ☐ N/A	
h.	Who performs an impact assessment of platform changes on applications?	☐ Y ☐ N ☐ N/A	

SECTION 4: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) OVERVIEW			
No.	**Question**	**Response**	**Objective Evidence/Comments**
i.	Does the client have enough knowledge and information about the change to assess the impact?	☐ Y ☐ N ☐ N/A	
j.	How are installations/changes of database, infrastructure partitioning and platform being documented?	☐ Y ☐ N ☐ N/A	
k.	If testing after a specific Platform Release fails, what is the process around this? Testing may pass for one client or organization (or application within Organization) and may not pass for us or others? E.g. Customer A testing passes, Customer B testing fails, what are the options for customer B? Can the customer B continue with previous version?	☐ Y ☐ N ☐ N/A	
4.1.2	**Application of Written Controls**		
	Is there evidence that the software development methodology was implemented through formal documentation for:		
a.	defining and documenting software requirements, designing & building software, integration of software components, testing of components and integrated product, and release and support of product?	☐ Y ☐ N ☐ N/A	
4.1.3	**Technical Review During Development**		
	Are technical reviews performed during hardware / software development, including:		
a.	Requirements analysis, designs, & coding?	☐ Y ☐ N ☐ N/A	
b.	Product test plans and scripts?	☐ Y ☐ N ☐ N/A	

SECTION 4: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) OVERVIEW			
No.	**Question**	**Response**	**Objective Evidence/Comments**
c.	Analysis of test results?	☐ Y ☐ N ☐ N/A	
d.	Are reported review outcomes used to support improvements to the software process?	☐ Y ☐ N ☐ N/A	
4.2 Source Code			
4.2.1 Source Code Annotation			
	How is source code and versions controlled?		
a.	Are there any established coding standards?	☐ Y ☐ N ☐ N/A	
4.3 Testing			
4.3.1 Procedural Controls			
a.	Are there procedures describing the testing process?	☐ Y ☐ N ☐ N/A	
	Do the testing procedures describe:		
b.	How test documents are developed and managed?	☐ Y ☐ N ☐ N/A	
c.	What types and levels of testing are required?	☐ Y ☐ N ☐ N/A	
	Do the procedures identify the organizational groups responsible for:		
d.	Testing, reviewing results, distribution of results, maintenance of test documentation, and release of products based on test results?	☐ Y ☐ N ☐ N/A	
	Do the procedures describe:		
e.	How testing errors are recorded, tracked and resolved?	☐ Y ☐ N ☐ N/A	
f.	Use of automated testing tools?	☐ Y ☐ N ☐ N/A	

SECTION 4: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) OVERVIEW			
No.	**Question**	**Response**	**Objective Evidence/Comments**
g.	How to manage testing information within a testing tool environment?	☐ Y ☐ N ☐ N/A	
h.	How software tools used in the testing process are evaluated and selected?	☐ Y ☐ N ☐ N/A	
4.3.2	**Test Document and Structure**		
a.	Is testing documented in approved Test Plans?	☐ Y ☐ N ☐ N/A	
	Do test plans or test design documentation contain the following information: Traceability to the component's design and requirements specifications? Criteria for acceptance/release of test component?		
	Do completed test protocols contain the following information:		
b.	Documented test cases with defined inputs, expected outputs, and actual outputs?	☐ Y ☐ N ☐ N/A	
c.	Documentation of traceability of test cases to specifications?	☐ Y ☐ N ☐ N/A	
d.	Error log or reference to error tracking identifier?	☐ Y ☐ N ☐ N/A	
e.	Results summary?	☐ Y ☐ N ☐ N/A	
f.	Analysis?	☐ Y ☐ N ☐ N/A	
g.	Approval/release (before and after execution)?	☐ Y ☐ N ☐ N/A	
h.	Tester identification and date?	☐ Y ☐ N ☐ N/A	
	How are test deviations managed and tracked?		

SECTION 4: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) OVERVIEW			
No.	**Question**	**Response**	**Objective Evidence/Comments**
4.3.3	**Product Engineering**		
	Do testing documents exist for:		
a.	Unit, integration, and system level testing?	☐ Y ☐ N ☐ N/A	
4.3.4	**Structural and Functional testing**		
a.	Do documents for testing demonstrate that testing strategies employ methods that challenge the constructs of logic within software code (white-box or structural testing)?	☐ Y ☐ N ☐ N/A	
b.	Do documents for testing demonstrate that testing strategies employ methods which treat software components as a "black boxes" challenging only the inputs to the software component and judging its behavior by the output results (functional testing)?	☐ Y ☐ N ☐ N/A	
c.	Are product errors, found during testing, used as feedback for the improvement of software processes?	☐ Y ☐ N ☐ N/A	
4.4	**Issue Tracking and Management**		
a.	Is there a help desk (e.g. incident tracking, bug tracking) process which involves customer reported bugs, process to prioritize and implement bug fixes, customer communication to inform about their bug fixes and engage them for testing and acceptance? Explain.	☐ Y ☐ N ☐ N/A	
b.	Does the cloud service provider have procedures to notify the customer of known problems?	☐ Y ☐ N ☐ N/A	

SECTION 4: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) OVERVIEW			
No.	**Question**	**Response**	**Objective Evidence/Comments**
	Do these procedures escalate proactive notification for problems relating to:		
c.	Data collection?	☐ Y ☐ N ☐ N/A	
d.	Processing of data?	☐ Y ☐ N ☐ N/A	
e.	Display of information?	☐ Y ☐ N ☐ N/A	
f.	Computer security?	☐ Y ☐ N ☐ N/A	
g.	Safety?	☐ Y ☐ N ☐ N/A	
4.5 Deployment			
a.	Are there installation/deployment procedures and documentation?	☐ Y ☐ N ☐ N/A	
4.6 Maintenance			
a.	Are there maintenance processes and documentation associated with the platform and database?	☐ Y ☐ N ☐ N/A	

SECTION 5: CHANGE MANAGEMENT			
No.	**Question**	**Response**	**Objective Evidence/Comments**
a.	Are changes to infrastructure documented?	☐ Y ☐ N ☐ N/A	
b.	Are changes to platform documented?	☐ Y ☐ N ☐ N/A	
c.	Are database changes documented?	☐ Y ☐ N ☐ N/A	
d.	Are application changes documented?	☐ Y ☐ N ☐ N/A	
e.	What is the frequency of changes of each type?	☐ Y ☐ N ☐ N/A	
f.	What types of changes are scheduled and are customers informed?	☐ Y ☐ N ☐ N/A	
g.	Are changes made without pre-	☐ Y ☐ N ☐ N/A	

SECTION 5: CHANGE MANAGEMENT			
No.	**Question**	**Response**	**Objective Evidence/Comments**
	notification?		
h.	Are impact assessments conducted for changes?	☐ Y ☐ N ☐ N/A	
i.	Is there a regression testing strategy? If so, how is the strategy determined?	☐ Y ☐ N ☐ N/A	

SECTION 6: QUALITY MANAGEMENT (STANDARDS AND PROCESSES)			
No.	**Question**	**Response**	**Objective Evidence/Comments**
a.	Is there a documented Quality System?	☐ Y ☐ N ☐ N/A	
b.	Are there procedures related to: - SDLC - Qualification (Infrastructure, Platform) - Incident Management - CAPA - Change Management - Release Management	☐ Y ☐ N ☐ N/A	
c.	Documentation control – Are procedures approved? Is there version control?	☐ Y ☐ N ☐ N/A	

SECTION 7: SECURITY			
7.1 Security (Physical & Logical)			
a.	How is platform security managed? What type of contractual agreements will be there with the cloud service provider for access privileges?	☐ Y ☐ N ☐ N/A	
b.	Is the cloud service provider certified for information security (ISEC) (SAS 70, SSAE16, HIPAA)?	☐ Y ☐ N ☐ N/A	
c.	How does the client perform testing related to prevention of unauthorized access?	☐ Y ☐ N ☐ N/A	
d.	Can the client control their application and related infrastructure and database components or limited to our application alone?	☐ Y ☐ N ☐ N/A	

SECTION 8: DATA			
8.1 Data Privacy			
a.	How is data managed and controlled (how data privacy of individual clients is assured against un-authorized access or tampering,	☐ Y ☐ N ☐ N/A	

SECTION 8: DATA			
	etc)?		
b.	Will the data encryption of key data elements be possible at the database level?	☐ Y ☐ N ☐ N/A	
c.	How will the platform provide application level privacy?	☐ Y ☐ N ☐ N/A	
8.2 Data Integrity			
a.	Is there a documented process to verify the integrity of client data?	☐ Y ☐ N ☐ N/A	
8.3 Backup / Restore			
a.	Is there a documented process for the backup and restoration of client data?	☐ Y ☐ N ☐ N/A	
b.	If so, is this process periodically re-verified?	☐ Y ☐ N ☐ N/A	
8.4 Storage			
a.	Is there off-site storage of client data?	☐ Y ☐ N ☐ N/A	

SECTION 9: RELEASE AND CONFIGURATION MANAGEMENT			
No.	**Question**	**Response**	**Objective Evidence/Comments**
9.1 General			
9.1.1 Identification of Items			
a.	Is there a release and a configuration management process?	☐ Y ☐ N ☐ N/A	
b.	Is the repository used to manage and control access to the CM items?	☐ Y ☐ N ☐ N/A	
c.	Are access privileges set according to a defined procedure?	☐ Y ☐ N ☐ N/A	
d.	Are CM tools utilized in the implementation of CM? Are there release management tools utilized?	☐ Y ☐ N ☐ N/A	

SECTION 9: RELEASE AND CONFIGURATION MANAGEMENT			
No.	**Question**	**Response**	**Objective Evidence/Comments**
e.	Are tools used for CM selected and approved for use through formal methods to assess tool suitability?	☐ Y ☐ N ☐ N/A	
9.1.2	**Management of Change**		
a.	Are change requests and problem reports for all configuration items/units initiated, recorded, reviewed, approved, and tracked according to a documented procedure?	☐ Y ☐ N ☐ N/A	
b.	Are traceability methods sufficient to enable restoration of a previous work item for finished product?	☐ Y ☐ N ☐ N/A	
9.1.3	**Version Management**		
a.	Is there a written method that describes a schema for establishing versions of CM items?	☐ Y ☐ N ☐ N/A	
	Does the schema define a methodology for:		
b.	Major releases, maintenance releases, individual HW/SW items, & custom work?	☐ Y ☐ N ☐ N/A	
c.	Do version management procedures ensure that links are clearly established between documentation and records and the related HW and SW versions?	☐ Y ☐ N ☐ N/A	
9.1.4	**Status of Configuration Management Items**		
a.	Is the status of configuration items/units recorded according to a documented procedure?	☐ Y ☐ N ☐ N/A	

SECTION 10: REGULATORY COMPLIANCE SUPPORT (21 CFR Part 11 & EudraLex Volume 4 Annex 11)

A. Subpart B – Electronic Records

Electronic Records Systems; Closed Systems			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**
11.10(a)	**System must be validated to ensure accuracy, reliability, and consistent intended performance and the ability to discern invalid or altered records.**		
1.	• Is the system validated? Validation/ Qualification of Infrastructure, Platform Framework (including virtualization and datacenter), and application.	☐ Y ☐ N ☐ N/A	
11.10(b)	**System must be capable of producing accurate and complete copies of electronic records in both human readable and electronic form for inspection, review and copying by the FDA.**		
2.	• Does the system have the ability to print and view the entire contents of the database for user accounts and transaction data?	☐ Y ☐ N ☐ N/A	
3.	• Can the system generate all reports and records electronically in a format that can be put on portable medium (e.g. compact disc) or transferred electronically?	☐ Y ☐ N ☐ N/A	
4.	• Are procedures in place to describe how to accomplish the retrieval of records and re-formatting of records?	☐ Y ☐ N ☐ N/A	
11.10(c)	**Records must be protected to enable their accurate and ready retrieval throughout their retention period.**		
5.	• Are records protected within the system to prevent unauthorized modification or deletion?	☐ Y ☐ N ☐ N/A	
6.	• Are records backed up so they can be retrieved in a disaster? Is there a backup/restore SOP?	☐ Y ☐ N ☐ N/A	
7.	• If records are archived, is there an archive SOP? Does it address restoration; testing the archive and dearchive function; regeneration of storage media; archive of metadata?	☐ Y ☐ N ☐ N/A	
8.	• Is the records retention period for electronic records controlled and maintained for the required retention period of the predicate rule?	☐ Y ☐ N ☐ N/A	

9.	• Is anti-malware software loaded and regularly updated to prevent malware corrupting data?	☐ Y ☐ N ☐ N/A	
11.10(d)	**System access must be limited to authorized individuals.**		
10.	• Is a username/password (or other logical security) required to access the system?	☐ Y ☐ N ☐ N/A	
11.	• Is the physical access to the system controlled?	☐ Y ☐ N ☐ N/A	
12.	• Is there a security SOP? Does it include physical and logical security (application security, network security, access authorization, creating new accounts, modifying accounts, deleting/disabling accounts, periodic checking of access and approval by System Owner)?	☐ Y ☐ N ☐ N/A	
13.	• Does the system have different levels of access based on user responsibilities (if appropriate)? How is this documented and controlled?	☐ Y ☐ N ☐ N/A	
11.10(e)	**There must be a secure, computer generated, time stamped audit trail that independently records the date and time of operator entries and actions that create, modify, or delete electronic records.**		
14.	• Does the platform support generation of an automatic computer generated electronic audit trail recording who, what, and when?	☐ Y ☐ N ☐ N/A	
15.	• Is the audit trail generation completely transparent to, and outside the control and access of users (except for view – only access)?	☐ Y ☐ N ☐ N/A	
16.	• Is the time local to the activity (i.e. server)? Is the time checked periodically?	☐ Y ☐ N ☐ N/A	
17.	• Is system clock protected from unauthorized change?	☐ Y ☐ N ☐ N/A	
18.	• Upon making a change to an electronic record, is previously recorded information still available? Are all previous values available?	☐ Y ☐ N ☐ N/A	
11.10(g)	**Perform authority checks of users (for access and use privileges)**		

19.	• Are there checks in place to ensure that only authorized individuals can use the system, (electronically sign records), access the operation or computer system input or output device, alter a record, or perform other operations?	☐ Y ☐ N ☐ N/A	
11.10(h)	**Use device checks to verify validity of data input (as appropriate)**		
20.	• If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g., system console, specific instrument because of calibration/ maintenance records, specific physical location) does the system check the validity of the source of any data or instructions received?	☐ Y ☐ N ☐ N/A	
11.10(i)	**Verify training of system users, developers, and maintenance staff** **(See Section 11: TRAINING/EDUCATION)**		
11.10(j)	**Establish and follow written accountability policies against falsification of records or signatures**		
	For systems not using Electronic Signatures, this section does not apply. For Electronic Signature systems, see following page.		
11.10(k) **(1)**	**Control access to, and use of, system operation and maintenance documents (including SOPs)**		
21.	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	☐ Y ☐ N ☐ N/A	
11.10(k) **(2)**	**Implement change control for audit trails for system documentation changes (including SOPs)**		
22.	Is there formal revision and change control procedures to maintain an audit trail that documents the lifecycle of development and modification of systems documentation?	☐ Y ☐ N ☐ N/A	
Electronic Records Systems; Open Systems			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**
11.30	**Implement document encryption & digital signature (suggested)**		

23.	Are controls in place to ensure record authenticity, integrity, and confidentiality from the point of record creation to the point of receipt? • Is record authenticity, integrity, and confidentiality required? • Is document encryption used? • Are digital signature standards used?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	

B. Subpart C – Electronic Signatures

Accountability			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**
11.10(j)	**Establish and follow written accountability policies against falsification of records or signatures**		
24.	• Is there a written policy in place that holds individuals accountable and responsible for actions initiated under their electronic signature?	☐ Y ☐ N ☐ N/A	

Signature Manifestations			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**
11.50(a)	**Signed electronic records must contain: name, date/time of signing, and meaning of signature.**		
25.	• Do signed electronic records contain information associated with the signing that clearly indicates: 1. Printed name of the signer (full name)? 2. Role/job title of the signer? 3. Date and time when the signature was executed? 4. Meaning of the signing (e.g. approval, review, responsibility, or authorship) associated with the signature?	☐ Y ☐ N ☐ N/A	
26.	• Is date and time applied by the computer? Is the time local to the signing? Is the time checked periodically? Is it protected from unauthorized change? Is time recorded to the second?	☐ Y ☐ N ☐ N/A	

27.	• Is the meaning of approval defined in an SOP?	☐ Y ☐ N ☐ N/A	
28.	• Does it identify if one user is signing on behalf of another?	☐ Y ☐ N ☐ N/A	
11.50(b)	**Items in 11.50 (a) must appear in every human readable form of the electronic record**		
29.	• Does the printed name, date, time, and signature meaning appear in every human readable form of the electronic record e.g., all displays and printed reports?	☐ Y ☐ N ☐ N/A	
30.	• Does the signature information appear immediately if the record is viewed after it is signed?	☐ Y ☐ N ☐ N/A	

Signature/Record Linking			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**
11.70	**Electronic signatures….executed to electronic records shall be linked to their respective electronic records**		
31.	Are electronic signatures and handwritten signatures executed to electronic records linked to their respective electronic records to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means? • Is the record and signature linked? • Is the signature protected to prevent transfer to another record? • Is the signed record protected to prevent changes after signing? • If the record is changed, is the signer prompted to re-sign following the change? • Are signature changes recorded in the audit trail?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	

General Requirements			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**
11.100 (a)	**Electronic signatures shall be unique and shall not be reused or reassigned**		

32.	• Is each electronic signature unique to one individual?	☐ Y ☐ N ☐ N/A	
33.	• Are there means to prevent an electronic signature from being reused by, or reassigned to, anyone else?	☐ Y ☐ N ☐ N/A	
34.	• Is a history of the assignment and identity of electronic signatures maintained?	☐ Y ☐ N ☐ N/A	
11.100 (b)	**Organizations must verify identity of individuals receiving electronic signatures.**		
35.	• Is the identity of an individual verified before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature? (to include temporary or contract employees)	☐ Y ☐ N ☐ N/A	
36.	• If identification verification is performed, is the verification made by an in-person ID verification such that individuals are required to show/prove identity to receive usernames and passwords? OR • Is there a paper trail of signatures such as the supervisor requesting and authorizing the assignment?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
37.	• Is there a procedure for re-issuing forgotten passwords?	☐ Y ☐ N ☐ N/A	
11.100 (c)	**Electronic Signature Certification**		
38.	• Has the company notified the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures?	☐ Y ☐ N ☐ N/A	
39.	• If electronic signatures are being used, can additional certification or testimony be provided that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature? • Is there any documentation to support that individuals understand that e-signatures are the legally binding equivalent of their handwritten signature?	☐ Y ☐ N ☐ N/A	

Electronic Signature Components and Controls Non-biometric Signatures			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**

11.200 (a)(1)	**Non-biometric E-signatures must have at least two components**		
40.	• Is the signature made up of at least two distinct identification components, such as an identification code and password?	☐ Y ☐ N ☐ N/A	
11.200 (a)(1)(i)	**Continuous session: First signing must use all components; subsequent signings can use one (private) component**		
41.	• Are there documented definitions specific to the system that defines continuous and non-continuous sessions?	☐ Y ☐ N ☐ N/A	
11.200 (a)(1)(ii)	**Non-Continuous session: each signing must use all components**		
42.	• When an individual executes one or more signings not performed during a single, continuous period of controlled system access, is each signing executed using all of the electronic signature components? • Is the period of continuous use defined? • Does the system log-off after a period of inactivity? • Is a password protected screen saver utilized? • Are all e-signature components required for all signings?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
11.200 (a)(2)	**Non-biometric Electronic Signatures must be used only by genuine owner**		
43.	• Are non-biometric signatures used only by their genuine owners?	☐ Y ☐ N ☐ N/A	
44.	• Are there procedures and training to reinforce that non-biometric e-signatures are to be used only by their genuine owners e.g., not shared, not loaned, not borrowed, not posted etc.?	☐ Y ☐ N ☐ N/A	
11.200 (a)(3)	**Attempted use of non-biometric Electronic Signatures requires collaboration of two or more people**		
45.	• Are non-biometric signatures administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals? • Could one person working alone "forge" another person's e-signature?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	

46.	• Are there mechanisms in place to prevent compromised e-signatures even if a user leaves their token or card unattended?	☐ Y ☐ N ☐ N/A	

Electronic Signature Components and Controls - Biometric Signatures			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**
11.200 (b)	**Biometric Electronic signatures must be usable only by genuine owner**		
47.	• If biometric electronic signatures are used, are they designed to ensure that they cannot be used by anyone other than their genuine owners?	☐ Y ☐ N ☐ N/A	

Controls for Identification Codes/Passwords			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**
11.300 (a)	**Maintain uniqueness of "ID Code + Password" combination**		
48.	• Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals can have the same combination of identification code and password? • Is uniqueness ensured historically as well as currently? • Does the process of assigning accounts ensure uniqueness? • Does the system prevent re-use of usernames?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
11.300 (b)	**Periodically check ID Code and Password issuances**		
49.	• Are controls in place to periodically check, recall, or revise (e.g., to cover such events as password aging) password issuance?	☐ Y ☐ N ☐ N/A	
50.	• Do passwords periodically expire and need to be revised? If no, are procedures in place to force periodic changes of passwords?	☐ Y ☐ N ☐ N/A	
51.	• Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	☐ Y ☐ N ☐ N/A	

52.	• Is access to a system periodically checked to ensure that only authorized users have access?	☐ Y ☐ N ☐ N/A	
11.300 (c)	**Manage lost or stolen tokens, cards, or other devices, and manage replacement issues**		
53.	• Are there loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls? • Is loss management addressed by SOP? What is the procedure for reporting potentially compromised tokens, cards, etc.? • Does the SOP address temporary replacements?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
11.300 (d)	**Prevent unauthorized use of passwords & ID codes; detect and immediately report any such attempts**		
54.	• Are there transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management? • Are break-in attempts monitored in real-time?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
55.	• Are "attempts at unauthorized use" defined?	☐ Y ☐ N ☐ N/A	
56.	• Is the reporting procedure addressed in an SOP? Is "immediate and urgent" defined? Is the procedure for notifying management defined and when?	☐ Y ☐ N ☐ N/A	
57.	• Is access frozen after a number of unsuccessful attempts to log in? How is this recorded? How monitored?	☐ Y ☐ N ☐ N/A	
11.300 (e)	**Test devices (e.g., tokens, cards) initially & periodically for proper function and possible unauthorized alteration**		

58.	Are there procedures covering the initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner?	☐ Y ☐ N ☐ N/A	

EudraLex Volume 4 Annex 11			
Ref.	**Requirement**	**Response**	**Objective Evidence / Comments**
1.	**Risk Management** Is risk management 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, are decisions on the extent of validation and data integrity controls based on a justified and documented risk assessment of the computerised system?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
2.	**Personnel** **(See Section 11: TRAINING/EDUCATION)**		

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, do formal agreements exist between the manufacturer and any third parties, and these agreements include clear statements of the responsibilities of the third party? 3.2 Is the competence and reliability of a supplier key factors when selecting a product or service provider? Is the need for an audit based on a risk assessment? 3.3 Is documentation supplied with commercial off-the-shelf products reviewed by regulated users to check that user requirements are fulfilled? 3.4 Is quality system and audit information relating to suppliers or developers of software and implemented systems made available to inspectors on request?	☐ Y ☐ N ☐ N/A	

4.	**Validation**		
	4.1 Does the validation documentation and reports cover the relevant steps of the life cycle?	☐ Y ☐ N ☐ N/A	
	Do manufacturers justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment?	☐ Y ☐ N ☐ N/A	
	4.2 Does validation documentation include change control records (if applicable) and reports on any deviations observed during the validation process?	☐ Y ☐ N ☐ N/A	
	4.3 Is there a current listing of all relevant systems and their GMP functionality (inventory) available?	☐ Y ☐ N ☐ N/A	
	For critical systems is there a current 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 available?	☐ Y ☐ N ☐ N/A	
	4.4 Do User Requirements Specifications describe the required functions of the computerised system and based on documented risk assessment and GMP impact?	☐ Y ☐ N ☐ N/A	
	Are user requirements traceable throughout the life-cycle?	☐ Y ☐ N ☐ N/A	
	4.5 Does the regulated user take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system?	☐ Y ☐ N ☐ N/A	
	Is the supplier assessed appropriately?	☐ Y ☐ N ☐ N/A	
	4.6 For the validation of bespoke or customised computerised systems is there a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system?	☐ Y ☐ N ☐ N/A	
	4.7 Is evidence of appropriate test methods and test scenarios demonstrated?		
	Are system (process) parameter limits, data limits and error handling?	☐ Y ☐ N ☐ N/A	
	Do automated testing tools and test environments have documented assessments for their adequacy?	☐ Y ☐ N ☐ N/A	
	4.8 If data are transferred to another data format or system, does validation include checks that data are not altered in value and/or meaning during this migration process?	☐ Y ☐ N ☐ N/A	

5.	**Data** Do computerised systems exchanging data electronically with other systems include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks?	☐ Y ☐ N ☐ N/A	
6.	**Accuracy Checks** For critical data entered manually, is there an additional check on the accuracy of the data? Is the check performed by a second operator or by validated electronic means? Is the criticality and the potential consequences of erroneous or incorrectly entered data to a system covered by risk management?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
7.	**Data Storage** 7.1 Is data secured by both physical and electronic means against damage? Is stored data checked for accessibility, readability and accuracy? Is access to data ensured throughout the retention period? 7.2 Are regular back-ups of all relevant data performed? Is the integrity and accuracy of backup data and the ability to restore the data checked during validation and monitored periodically?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
8.	**Printouts** 8.1 Is it possible to obtain clear printed copies of electronically stored data? 8.2 For records supporting batch release is it possible to generate printouts indicating if any of the data has been changed since the original entry?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	

9.	**Audit Trails** Is consideration 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")? For change or deletion of GMP-relevant data is the reason documented? Are audit trails available and convertible to a generally intelligible form and regularly reviewed?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
10.	**Change and Configuration Management** Are any changes to a computerised system including system configurations made only in a controlled manner in accordance with a defined procedure?	☐ Y ☐ N ☐ N/A	
11.	**Periodic evaluation** Are computerised systems periodically evaluated to confirm that they remain in a valid state and are compliant with GMP? Do such evaluations include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	

12.	**Security** 12.1 Are physical and/or logical controls in place to restrict access to computerised system to authorised persons? Do suitable methods of preventing unauthorised entry to the system include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas? 12.2 Does the extent of security controls depend on the criticality of the computerised system? 12.3 Is the creation, change, and cancellation of access authorisations recorded? 12.4 Are management systems for data and for documents designed to record the identity of operators entering, changing, confirming or deleting data including date and time?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
13.	**Incident Management** Are all incidents, not only system failures and data errors, reported and assessed? Is the root cause of a critical incident identified and form the basis of corrective and preventive (CAPA) actions?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
14.	**Electronic Signature** Are electronic records signed electronically? Do electronic signatures: a. have the same impact as hand-written signatures within the boundaries of the company? b. permanently link to their respective record? c. include the time and date that they were applied?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	

15.	**Batch release** When a computerised system is used for recording certification and batch release, does the system allow only Qualified Persons to certify the release of the batches? Does the computerised system clearly identify and record the person releasing or certifying the batches using an electronic signature?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
16.	**Business Continuity** For the availability of computerised systems supporting critical processes, are provisions made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system)? Is the time required to bring the alternative arrangements into use based on risk and appropriate for a particular system and the business process it supports? Are these arrangements adequately documented and tested?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	
17.	**Archiving** Data may be archived. Is this data checked for accessibility, readability and integrity? If relevant changes are to be made to the system (e.g. computer equipment or programs), then is the ability to retrieve the data ensured and tested?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	

SECTION 11: TRAINING / EDUCATION			
No.	**Question**	**Response**	**Objective Evidence/Comments**
11.1	**General**		
11.1.1	**Controls**		

SECTION 11: TRAINING / EDUCATION			
No.	**Question**	**Response**	**Objective Evidence/Comments**
a.	Is there a written procedure for training?	☐ Y ☐ N ☐ N/A	
b.	Does the training procedure require that personnel be trained and qualified in procedures related to their job function(s)?	☐ Y ☐ N ☐ N/A	
11.1.2	**Training / Education Records**		
a.	Does the cloud service provider maintain written records of training/education?	☐ Y ☐ N ☐ N/A	
b.	Are these records consistently maintained and up to date?	☐ Y ☐ N ☐ N/A	
11.1.3	**Training / Education Responsibilities**		
a.	Is there an individual or group assigned responsibility for training/education?	☐ Y ☐ N ☐ N/A	
11.1.4	**Level of Access and Defined Responsibilities**		
a.	Do all personnel have the appropriate level of access and defined responsibilities to carry out their assigned duties?	☐ Y ☐ N ☐ N/A	

SECTION 12: TECHNOLOGY ENVIRONMENT			
No.	**Question**	**Response**	**Objective Evidence/Comments**
12.1	**General**		
a.	If client's application is deployed in one of cloud service provider's environments (shared with other client applications):	☐ Y ☐ N ☐ N/A	
b.	How is the client assured that changes made to one application does not impact others e.g. platform parameter data, metadata or shared code snippets, etc?	☐ Y ☐ N ☐ N/A	
c.	What is the frequency of changes made and are changes categorized? If so, what	☐ Y ☐ N ☐ N/A	

SECTION 12: TECHNOLOGY ENVIRONMENT			
No.	**Question**	**Response**	**Objective Evidence/Comments**
	are the categories?		
d.	How is the data segregated so that others do not have access (read/write/update) to client data within the organization?	☐ Y ☐ N ☐ N/A	
e.	If client application is deployed on Global COMPANY organization, how does it affect the daily limits, e.g. bandwidth, queries executions, emails sending, data storage, data downloads/uploaded e.g. to datamarts or from other apps etc. - how these limits will be shared among the apps on COMPANY Global Org.	☐ Y ☐ N ☐ N/A	
f.	Is there a data backup and restore policy available? How the data could be restored from backup? Is it possible to restore for our applications only or all the applications in the Global COMPANY Organization impacted or impacts all apps on the platform?	☐ Y ☐ N ☐ N/A	
12.2	**Application Release Management Including Deployment Process**		
a.	How are these environments different (or same) in terms of sharing database or hardware or data center?	☐ Y ☐ N ☐ N/A	
b.	What are the application and data replication and failover strategies?	☐ Y ☐ N ☐ N/A	
c.	How is the data maintained/synchronized between environments (data refresh strategies)?	☐ Y ☐ N ☐ N/A	
d.	Are unit tests execution conducted in Production and Sandbox environments? If so, who executes? How about additional environments and non-destructive testing?	☐ Y ☐ N ☐ N/A	

SECTION 12: TECHNOLOGY ENVIRONMENT			
No.	**Question**	**Response**	**Objective Evidence/Comments**
12.3	**Technology**		
a.	Would there be any restrictions for data exchange (client internal or external hosted) in and out of cloud service provider's environment using ETL tools Informatica PC?	☐ Y ☐ N ☐ N/A	
b.	What are the integration methodologies including database layer?	☐ Y ☐ N ☐ N/A	
c.	Can there be integration with reporting platforms for analytics (e.g. BI tools such as BusinessObjects)?	☐ Y ☐ N ☐ N/A	
d.	Are there restrictions or governance on resource utilization e.g. CPU/Memory utilization, batch data loads and number rows retrieved/committed to database?	☐ Y ☐ N ☐ N/A	
e.	What is the licensing model: Initial Setup (users/transactions/DB sizing etc) and Annual Support and Maintenance costs?	☐ Y ☐ N ☐ N/A	
12.4	**Contractual Agreements**		
a.	Are there contractual agreements in place with cloud service provider as related to longevity of client data and applications on the platform? Service level agreements?	☐ Y ☐ N ☐ N/A ☐ Y ☐ N ☐ N/A	