Understanding and Achieving 21 CFR Part11 and EU Annex 11 Compliance

The U.S. Food and Drug Administration's (FDA) and European Union's (EU) regulations for life sciences are mostly interrelated. Organizations utilizing digital tools, automated processes, or transitioning to electronic systems need to comprehend the regulations in the U.S. FDA's 21 CFR Part 11 and the EU's guidelines, Annex 11.

Both guidelines are intended to facilitate Good Manufacturing Practice (GMP) and have been designed to ensure compliance and uphold the quality of computerized data systems in the life science industry. While there are many similarities between Annex 11 and Part 11, the two guidance are comparatively different.

To understand it even simpler, below is a comparison table highlighting key differences between CFR Part 11 and EU Annex 11:

Table 1: High-Level Comparison of Annex 11 and Part 11

Highlights	21 CFR Part11	EU Annexure11
Scope	Electronic records and signatures employed in FDA-regulated activities by life sciences and other entities.	Relevant to and based on validation according to GMP, GDP, GLP, GCP, and medical devices.
Focus	The use of electronic signatures and records in open or closed computer systems.	Quality management of computerized systems from a risk-based standpoint.
Objective	The stored electronic records and signatures must be equally reliable and trustworthy as paper documents and wet signatures.	Quality management of computerized systems from a risk-based standpoint.
Relevance and Validation	Relevant to and based on validation according to GMP, GDP, GLP, GCP, and medical devices.	Relevant to GMP but referenced in other areas as well.

Table 2: Similarities and Difference between Annex 11 vs Part-11 Section

ANNEX 11 SECTION	PART-11 SECTION
Principle	11.2(b)- Implementation 11.10(a)- Validation
1. Risk Management	Not Covered
2. Personnel	11.10(i)- Personnel
3. Suppliers and Service Providers	Not Covered
3.1 Formal Agreements	Not Covered
3.2 Audit Supplier	Not Covered
3.3 Review Documentation for COTS	Not Covered
3.4 Supplier Audit Available on Request	Not Covered
4. Validation	11.10(a)- Validation
4.1 Cover Life Cycle	Not Covered
4.2 Change Control and Deviations	11.10(k)- Documentation Control

4.3 Systems Inventory	Not Covered
4.4 User Requirement Specifications	Not Covered
4.5 Quality Management System	Not Covered
4.6 Process for Customized Systems	Not Covered
4.7 Evidence of Appropriate Test Methods	Not Covered
4.8 Data Transfer Validation	11.10(h)- Device Checks
5. Data	11.10(f)- Operational System Checks 11.30- Controls for Open Systems
6. Accuracy Checks	11.10(f)- Operational System Checks
7. Data Storage	11.10(c)- Protection of Records
7.1 Secured and Accessible	11.10(d) Limiting System Access 11.10(e) - Secure Records 11.10(g) - Authority Checks
7.2 Back-Up	Not Covered
8. 1 Clear Printed Copies	11.10(b)- Generate Accurate and Complete Copies
8.2 Batch Release/Changed Since Original	Not Covered

ANNEX 11 SECTION	PART-11 SECTION
9. Audit Trails	11.10(e) - Electronic Audit Trail 11.10(k)(2)- Documentation Control
10. Change and Configuration Management	11.10(d)- Limiting System Access 11.10(e)- Electronic Audit Trail
11. Periodic Evaluation	11.300(b) and (e)- Periodically Checked 11.10(k)- Documentation Control
12. Security	11.10(c) - Protection of Records

13. 12.1 Physical/Logical	11.10(d) - Limiting System Access 11.10(g) - Authority Checks 11.200 (a) and (b) Biometrics 11.300(a) Unique 11.300(d) - Prevent Unauthorized Use
12.2 Criticality	Not Covered
12.3 Security - Record Events	11.300(b)and (c)-Controls for Identification Codes/Passwords
12.4 Data Management/Operators Entries	11.10(e)-Controls for Closed Systems
13 Incident Management	Not Covered
14 Electronic Signature	11.50 - Signature Manifestations
14(a) Same as Hand-Written	11.1(a) Scope 11.3(b)(7) Definitions 11.100(c) Certify Equivalent to Handwritten
14(b) Permanent Link	11.70- Signature/Record Linking
14(c) Time and Date	11.10(e)- Electronic Audit Trail
15 Batch Release	Not Covered
16 Business Continuity	Not Covered
17 Archiving	11.10(c)- Protection of Records for Accurate Retrieval

Table 3: Similarities and Difference between Part-11 vs Annex 11 Section

(Subpart B - Electronic Records and Subpart C - Electronic Signatures)

PART-11 SECTION	ANNEX 11 SECTION
11.10 Controls for Closed Systems	
11.10(a) Validation	4-Validation
11.10(b) Generate Accurate and Complete Copies	8.1-Printouts
11.10(c) Protection of Records for Accurate Retrieval	17-Archiving, 12-Security, 7-Data Storage

11.10(d) Limiting System Access to Authorized Individuals	7.1- Secured and Accessible 10- Change and Configuration Management 12.1-Security, Physical/Logical
11.10(e) Record of Operator Entries (Audit Trail)	7.1- Secured and Accessible 9-Audit Trails 10-Change and Configuration Management 12.4- Data Management/Operators Entries 14(c)-Electronic Signature
11.10(f) Operational System Checks	5-Data, 6- Accuracy Checks
11.10(g) Authority Checks	7.1- Secured and Accessible 12.1-Security, Physical/Logical
11.10(h) Device Checks	4.8-Validation
11.10(i) Personnel (who develop, users and maintain systems)	2-Personnel
11.10(j) User Accountability for Actions Initiated under e-signatures	Not Covered
11.10(k) Documentation Control	9-Audit Trails 4.2- change Control and Deviations 10-Change and Configuration Management 11- Periodic Evaluation
11.30 Controls for open systems	Principle (all systems) 5. Data
11.50 Signature Manifestations	14-Electronic Signature
11.70 Signature/Record Linking	14(b)-Electronic Signature
SUBPART C - ELECTRONIC SIGNATURES	
11.100 General requirements	
11.100(a) Unique/Not Reused	Not Covered
11.100(b) Verify Identity	Not Covered

11.100(c) Certify Equivalent to Handwritten	14(a) same as hand-written
11.200 Electronic signature components and controls	
11.200(a) Not Based on Biometrics	12.1-Security, Physical/Logical
11.200(b) Based on Biometrics	12.1-Security, Physical/Logical
11.300(a) Unique	12.1-Security, Physical/Logical
11.300(b) Periodically Checked	11. Periodic Evaluation 12.3-Security- Record Events
11.300(c) Procedures to deauthorize	12.3-Security, Record Events
11.300(d) Prevent Unauthorized Use	12.1-Security
11.300(e) Proper Function	11-Periodic Evaluation

Conclusion

Part 11 primarily pertains to the utilization of electronic records and signatures within computer systems, whereas Annex 11 concentrates on the quality management of computerized systems. Part 11 mandates that electronic records and signatures maintain the same level of trustworthiness and reliability as paper records and handwritten signatures. Conversely, Annex 11 mandates that computerized systems guarantee equivalent product quality and quality assurance as manual systems.

Annex 11 applies to the export or manufacture of products in the EU. However, Part 11 applies to e-submissions to the FDA. Part 11 and Annex 11 share similarities, yet diverge in aspects like authenticating the identity and accountability of authorized individuals and reporting to authorities. Annex 11 adopts a risk management perspective concerning criticality and ensures a system approach to periodic evaluations. Each guidance provides detail information to the life science companies to achieve regulatory compliance.