



7 October 2025

Submission of
comments on

Annex 11 Computerised Systems

Please note that these comments and the identity of the sender will be published unless a specific justified objection is received.
When completed, this form should be sent to the European Medicines Agency via the EU survey, in Excel format **(not PDF)**.
Columns A to E should mandatorily be filled in prior to completing the columns "Comment" and "Rationale" and/or "Proposed wording".
For more details on how to use this template please refer to the tab "Manual for commenter" below.

| Country | Organisation raising comment (if no organisation, name of individual) | Line from | Line to | Comment (only one topic per comment) (max 600 characters) | Rationale (must be included when proposing a change) (max 600 characters) | Proposed wording (must be included when proposing a change) (max 600 characters) |
|---------|---|-----------|---------|--|---|---|
| USA | ISPE | 0 | 0 | General Comment 1: The map of the document tries to cover all the chapters for the Eudralex volume 4 part 1. We suggest developing a GMP guidance dedicated to computerised systems. Annex 11 should consider all existing chapters of the GMP Eudralex Volume 4 Part I and Part III avoiding development or rewriting what is existing in other chapters. This document except for some specific requirements should not address PQS which is described in the Chapter 1 and QRM is a global requirement which does not need to be quoted in many clauses. | Attempting to repeat requirements of other Chapters or Annexes in Annex 11 has the strong potential over time to lead to inconsistencies between the documents. | n/a |
| USA | ISPE | 0 | 0 | General Comment 1 (cont.): ISPE suggests for PQS and QRM, as these concepts are described in Chapter 1, that PQS and QRM requirements should be summarised in the scope or principle of the document and not in other clauses as PQS and QRM are applicable to all Annex 11. | QRM and PQS applies to this document in its entirety and should not, normally, be referred to in specific paragraphs. | n/a |
| USA | ISPE | 0 | 0 | General Comment 2: We suggest having in this GMP guidance only WHAT regulators want to see and avoid describing in the GMP HOW industry should implement these requirements. HOW to implement is described in many pharmaceutical industry guidances. | Making HOW as requirement would have a negative impact as the annex would discourage the use of modern best practice and current and innovative technology. | If the HOW is included to assist inspectors with a current, more harmonised interpretation of requirements, we recommend that this interpretation is documented in other ways such as a Q&A document or a publicly available inspector's guide. |
| USA | ISPE | 0 | 0 | General Comment 3: On terminology, we suggest replacing the word "regulated users" which is not described in the various pharmaceutical texts, by "user" | "Regulated user" is a new phrase and considered unnecessary. "User" is considered appropriate. | n/a |
| USA | ISPE | 18 | 19 | The important Inventory Requirement from the current Annex 11 is missing... | Without the inventory, there is no clear mechanism to easily confirm all the GMP systems have been validated. | Suggest adding after the sentence at section 2.1 line 19: An up-to-date listing of all relevant systems and their GMP functionality (a system inventory) should be maintained. |
| USA | ISPE | 20 | 23 | We suggest that appropriate text relating to QRM in the principles section is sufficient. Please refer to the proposal for Principles in the General comments section. | Rationale is given in the General Comment 1 above. | QRM and PQS applies to this document in its entirety and should not, normally, be referred to in specific paragraphs. |
| USA | ISPE | 27 | 28 | The draft update to Chapter 4 references and defines ALCOA++ but in this Annex 11 draft it refers only to ALCOA+. This should be included in Chapter 4 nevertheless if repeat text is required it should be consistent between the 2 documents. | ALCOA++ is described in Chapter 4. We suggest there is consistency between Chapter 4 and Annex 11 with the wording. In our view, this appears to be an example of inconsistency between two documents and supports our General Comment 1 rationale. | Please update in Annex 11 to ALCOA++ |

| | | | | | | |
|-----|------|-----|-----|---|--|--|
| USA | ISPE | 32 | 33 | The text should focus on the business process being automated, not the functional requirements. | The most important part of putting in the right controls for a computerized system is assuring the business process that is being implemented is clearly defined. The regulated user should not be focusing on the functionality but the business process. | System requirements which describe the GMP business process the regulated user is automating, should be documented... |
| USA | ISPE | 36 | 38 | In the Annex 11 Principles, "Outsourced activities" could refer to Part I, Chapter 7, which addresses the requirements for outsourced activities. Computerised systems are considered not to be different from other GMP activities. | In very many quality-critical GxP outsourcing situations (not related to computerised systems) the regulated company remains accountable for meeting requirements but the third party maintains the detailed evidence within its own Quality System, where it is useful and effective. The regulated company maintains evidence of appropriate assessment, technical and quality agreements, monitoring, and other controls For example, clause 7.5, line 149 as written could negate many of the benefits of outsourcing. | We suggest in the Principles to mention that all Eudralex Volume 4, Part I including Chapter 7 on Outsourced Activities should apply to computerised systems. We suggest deletion of clause 7.5 in line 149ff relating to contracts. |
| USA | ISPE | 45 | 67 | PQS is already addressed in ICH Q10 and EU-GMP Chapter 1 and Part III (GMP Related Documents). It is unclear whether new expectations specific to computerised systems are introduced. We suggest removing this section from Annex 11 and include a short section referring to Eudralex Volume 4, Part I, Chapter 1 in the Scope or Principles sections as described in General Comment 1 above. | Clarification would help avoid duplication and ensure alignment with existing GMP guidance. | Clarification is required please on whether this section reinforces existing PQS principles for computerised systems or introduces new expectations. A reference to Chapter 1 and /or ICH Q10 should be sufficient. |
| USA | ISPE | 68 | 85 | ISPE suggests removing this section from the Annex 11 and referring to QRM, which is described in Chapter 1 of Eudralex Vol 4 Parts I and III, and ICH Q9 (R1). We suggest avoiding in Annex 11 rewording of existing documents in the GMP arena. | Rationale is described in General Comment 1 above. | n/a |
| USA | ISPE | 87 | 90 | We suggest removing Clause 5.1 as it is a HOW description for implementation of QRM. | Rationale is described in General Comment 2 above. | n/a |
| USA | ISPE | 91 | 93 | As Clause 5.2 applies to all activities using computerised systems in GMP activities we suggest having only one clause referring to Chapter 1 Eudralex Vol 4. | Rationale is described in General Comment 1 above. | n/a |
| USA | ISPE | 95 | 100 | The use of the term User Requirements Specification, and the wording that specifically "a regulated user must establish and approve" may result in unnecessary duplication of vendor documentation that adequately defines the system functionality. | There is no benefit to a regulated company duplicating information from the vendor if the vendor's information is fit for purpose. | Please replace the first sentence in 6.1 with the wording used in Section 2.5 " System requirements which describe the functionality the regulated user has automated and is relying on when performing GMP activities, should be documented and kept updated to fully reflect the implemented system and its intended use. " |
| USA | ISPE | 101 | 107 | We suggest for this clause referring to QRM and summarising what is required. Revised text is suggested. | There is too much HOW in this clause to allow flexibility; reference to the application of QRM should be sufficient. | ISPE suggests clause 6.2 is reworded: "The extent and detail of defined requirements should be commensurate with the risk, complexity and novelty of a system, and the description should be described using QRM principles as given in ICH Q9 R1." |
| USA | ISPE | 108 | 114 | The statement in 6.3 that "The regulated user should take ownership of the document [vendor requirements specification] covering the implemented version of the system and formally approve and control it after making any necessary changes." takes the information out of the vendor's control and their quality management system, and produces a difficult to control duplicate in the regulated company's system. | If there is no customisation to the system then the requirements specification may be fit for purpose as is. Duplicating it just increases the risk of errors and wastes effort. Taking it out of the vendor's / provider's QMS destroys its value. | Please delete the final sentence in 6.3 and replace it with " Where the vendor's system requirements adequately define the regulated company's intended use of system functionality in a GMP process, the regulated company may reference the vendor's requirements rather than duplicating them. The regulated company must review the currency and applicability of the requirements specification during any change to the system or its intended use, and at the system's periodic review, to assess ongoing that the specification remains valid and to update the reference to accommodate updates by the vendor. " |
| USA | ISPE | 119 | 121 | The text states that documented traceability between individual requirements, underlying design specifications and corresponding qualification and validation test cases should be established and maintained. Traceability through underlying design specifications is typically neither feasible nor helpful nor required for standard and configurable products. | Traceability through underlying design specifications developed and maintained by suppliers of standard and configurable products is not typically helpful nor possible. Traceability through design may be helpful for custom systems or custom components, and traceability through configuration may also be relevant in some cases. | Suggested rewording: Documented traceability between individual requirements, underlying design specifications and corresponding qualification and validation test cases and corresponding verification test cases should be established and maintained. Additionally traceability through underlying design and/or configuration specifications should be considered where relevant and helpful, e.g. for custom or complex configurable applications |
| USA | ISPE | 125 | 126 | The text states that the chosen configuration should be documented in a controlled configuration specification. This implies a traditional configuration specification document and may not reflect current approaches. Alternative text is suggested. | There may be cases where the chosen configuration may be more effectively captured using tools and automation in the system environment, and that this is the preferred method recommended by the product supplier. | Suggest adding: The chosen configuration should be documented in a controlled configuration specification, or defined and documented using a controlled technical method such as an appropriate software tool. |

| | | | | | | |
|-----|------|-----|-----|--|---|--|
| USA | ISPE | 127 | 166 | This section repeats the content of Chapter 7 in Eudralex Volume 4, Part I. All these clauses are not specific to computerised systems. We suggest deleting this section and having only one clause referring to Chapter 7 of Eudralex Volume 4, Part I "Outsourced activities". | Rationale is described in General Comment 1 above. | We suggest just providing a reference to Chapter 7 of Part I Eudralex Volume 4 "Outsourced activities" which covers all this section. |
| USA | ISPE | 167 | 199 | In General, Section 8 introduces a new section on Alarms, which is a topic not covered at all in the current Annex 11. Alarm management, however, is an activity that has been routinely and successfully performed by regulated companies and supplier companies for very many decades. We suggest replacing all the section with the proposed wording. | Comprehensive up-to-date and widely used standards for alarm management exist. The primary standards are IEC 62682 and ANSI/ISA-18.2. It is suggested that the section be replaced with a reference to international standards. We suggest to refer to these guidance as a foot note . | Please consider replacing the whole of Section 8 with this simple statement: The regulated company should establish policies, standards, and procedures for managing alarms throughout their lifecycle. Appropriate international standards on the topic, such as IEC 62682 and ANSI/ISA-18.2 should be consulted and followed. |
| USA | ISPE | 193 | 199 | 8.7 Review The term "periodic reviews" within line 193 is not clearly defined. It is unclear whether the review is expected to be operational (routine checks), retrospective (trend analysis), or both. Clarification would help ensure consistent and effective implementation. Without a clear expectation, companies may interpret the requirement differently, leading to inconsistent practices. A more precise description would help ensure harmonised application. | The expectation of "periodic reviews" is not defined. Section 8.7 is too prescriptive. | If Section 8 continues to exist, then consider clarifying Section 8.7 regarding the expectation for "periodic review" by specifying whether it should include operational checks, retrospective evaluations, or both. |
| USA | ISPE | 201 | 202 | The current text states that qualification and validation activities for computerised systems should follow the general principles outlined in GMP Annex 15. This is ambiguous, as it could be read to mean that the guidance in the "Principles" Section of Annex 15 should be applied (which is understandable and acceptable), but also could be read as implying that the detailed approach to facilities, equipment, utilities and processes described should be also applied to computerised systems, which would be harmful. Alternative text is suggested. | Annex 15 describes the principles of qualification and validation which are applicable to facilities, equipment, utilities and processes. Much of the detailed content of Annex 15 (as it is intended for facilities, equipment, utilities and processes) is not appropriate for application to many modern IT, automation and process systems, and are not aligned with current models, life cycles and techniques. Direct application of such detailed, prescriptive, and in many cases outmoded approaches to modern IT, automation and process systems is not an effective way of achieving effective and high quality systems that are fit for intended use. | Please remove the reference to Annex 15. Section 9.1 could be rephrased as: Qualification and validation activities for computerised systems should follow the general principles outlined in GMP Annex 15 collectively demonstrate and ensure the systems are fit for their intended use. The activities should address both standard and configured system functionality, as well as any functionality realised through customisation. |
| USA | ISPE | 211 | 213 | The text states that prior to commencing any test activity, it should be verified that a computerised system and its components have been correctly installed and configured according to specifications. Alternative text is suggested. | This does not take into account that a large proportion of valuable and relevant testing of computerised system takes place before installation. We suggest removing the last sentence to the clause as covered by other clauses. | We suggest rephrasing as: Prior to commencing any test activity acceptance and release , it should be verified that a computerised system and its components have been correctly installed and configured according to specifications. and where applicable, that relevant components have been properly calibrated. Operating systems and platforms should be updated to supported versions and relevant security patches should be deployed (see 15.10 Updated platforms and 15.13 Timely patching). |
| USA | ISPE | 220 | 223 | This section on traceability is too restrictive as some requirements, especially non-functional requirements, may not be verified by executing test cases but rather by other verification activities like review of the system design. As written this clause may not include much valuable testing that may have been done without or before traceability to specifications but such testing still contributes significantly to the quality of the implemented system. Alternative text is suggested. | A significant proportion of testing is aimed at identification of defects and errors and may also be aimed at identifying missing requirements or finding other error or omissions. These critical types of tests are typically not traceable to requirements or specifications but are essential in ensuring that systems are fit for intended use and reducing defects in the operational phase. Quality critical requirements should however be traceable to verification activities. | Suggest replacing 9.5 with all new text below: All verification activities aimed at demonstrating compliance with specific quality critical requirements should be traceable to those relevant requirements, e.g., by means of a requirements traceability process. |
| USA | ISPE | 224 | 226 | The need to focus on key functionality designed to ensure patient safety and product quality are not included in clause 9.6. Focus. Alternative text is suggested. | Focus needs to be given to key functionality implemented as a mitigating action with the intention of reducing risk to an acceptable level | Suggest amending to: 9.6. Focus. Increased focus should be on testing a system's handling of key functional requirements, on functionality intended to ensure that activities are conducted according to GMP, and on functionality designed to ensure data integrity. Focus should also be given to key functionality and controls implemented as an outcome of risk assessments to ensure that identified unacceptable levels of risk to patient safety, product quality and data integrity have been mitigated to an acceptable level. |

| | | | | | | |
|-----|------|-----|-----|---|---|---|
| USA | ISPE | 230 | 232 | At line 231, requiring test scripts to be pre-approved prevents the use of unscripted testing and also prevents use of automated testing. Also, the term "protocol" can be confusing when considering it can also relate to clinical trial protocols, network protocols, communication protocols, blockchain protocols etc. Alternative text is suggested. | Requirement for repeatability rules out many valuable test methods including exploratory testing, as described in IEC/IEEE/ISO 29119-1: Software and systems engineering – Software testing - Part 1: Concepts and definitions. Such methods have played an integral part in the testing of systems, including safety-critical systems, for over half-a-century. As long as the test scripts are produced by competent personnel in line with approved plans, there should be no requirement for the test scripts themselves to be approved. | Suggested Change: 9.7. Plan and approval. Qualification and validation activities should be conducted according to approved plans and specifications . protocols and test scripts. Test scripts should be described in sufficient 231 detail to ensure a correct and repeatable conduct of test steps and prerequisites. |
| USA | ISPE | 248 | 250 | We suggest removing this clause which is already addressed in the Chapter 4, Sections 4.12 iii and 4.81. | Rationale is described in General Comment 1 above. | n/a |
| USA | ISPE | 256 | 259 | There may not be a validated process available for data migration and as a one-off activity the effort to validate the process may not be justified. Alternative text is suggested. | The focus should be on the integrity of the data rather than having a validated process which may not be practical. | Suggested rewording: Where an ad hoc process requires that critical data or a whole database be migrated from one system to another (e.g., when moving data from a retired system to a new one), this should be based on a validated process. the integrity of the migrated data must be maintained. |
| USA | ISPE | 261 | 278 | System security remains an area with new concepts and technologies emerging frequently. This section enforces certain current authentication and security methods, describing how access management should be done rather than defining the quality objective. It would prohibit the adoption of current cutting-edge security concepts like Passwordless Authentication with FIDO2/WebAuthn keys or device-based or certificate-based authentication or Federated Identity concepts that adopt OAuth2, OpenID Connect, and SAML 2.0 for seamless identity across apps or any other future security enhancements. We suggest removing clauses 11.4 and 11.6. | Best practice in this area is dynamic and rapidly changing. The sub sections are too detailed and too focused on current concepts and specific scenarios e.g. brute force attack in auto locking. Suggest that detailed "how" be replaced by "What" by replacing and simplifying the following sections to 'future-proof' the regulation. | Suggestion modified text as follows: 11.3 Certain Identification The method of authentication should identify users with a high degree of certainty and provide an effective protection against unauthorised access. Typically, it may involve a unique username and a password, although other methods providing at least the same level of security may be employed (e.g. biometrics). Authentication only by means of a token or a smart card is not sufficient, if this could be used by another user. The method of authentication should identify users with a high degree of certainty and provide an effective protection against unauthorised access. 11.4 - Delete |
| USA | ISPE | 278 | 290 | Systems Security is a requirement, HOW to implement security should not be in a GMP guidance. Security accesses and data is mandatory not HOW to implement we suggest using the proposed wording. | This section enforces certain current authentication and security methods, describing how access management should be done rather than defining the quality objective | 11.5 Secure Passwords- Current text is too prescriptive Passwords should be secure and enforced by systems. Password rules should be commensurate with risks and consequences of unauthorised changes in systems and data. For critical systems, passwords should be of sufficient length to effectively prevent unauthorised access and contain a combination of uppercase, lowercase, numbers and symbols. A password should not contain e.g. words that can be found in a dictionary, the name of a person, a user id, product or organisation, and should be significantly different from a previous password. Change to: The regulated user must establish and enforce policies on secure passwords according to current good practice and standards. (Let the user decide HOW) 11.6 - Delete 11.7 Auto-locking. Accounts should be automatically locked after a pre-defined number of successive failed authentication attempts. Accounts should only be unlocked by the system administrator after it has been confirmed that this was not part of an unauthorised login attempt or after the risk for such attempt has been removed. Change to Auto-Locking Access Attempts. Accounts should be protected against automated attempts to gain unauthorised access. |
| USA | ISPE | 291 | 299 | System security remains an area with new concepts and technologies emerging frequently. This section enforces certain security methods rather than defining the quality objective. We suggest amending section 11.8 and removing the clause 11.9 which is more related to HOW to implement Security. | The proposed text is too detailed and prescriptive and would not allow the adoption of new technologies to guard against unauthorised manipulation e.g. monitoring of keystroke activity patterns rather than a simple inactivity timeout. Suggest that detailed "how" be replaced by "What" by replacing and simplifying the following sections to 'future-proof' the regulation. | Suggestions: 11.8 Inactivity Logout Unauthorised Manipulation Systems should include adequate physical and/or logical controls to prevent unauthorised data manipulations. 11.9 Access log. Systems should include an access log (separate, or as part of the audit trail) 295 which, for each login, automatically logs the username, user role (if possible, to choose 296 between several roles), the date and time for login, the date and time for logout (incl. 297 inactivity logout). The log should be sortable and searchable, or alternatively, it should be 298 possible to export the log to a tool which provides this functionality. |

| | | | | | | |
|-----|------|-----|-----|---|---|---|
| USA | ISPE | 306 | 312 | The text is too detailed and too focused on how access reviews should be performed. There may be scenarios in which it would not be efficient, possible, or sensible to have managers conduct the reviews. Alternative text is suggested. | Too detailed and too focused on HOW access reviews should be performed. | Suggestion: 11.11 Recurrent reviews. User accounts and roles should be subject to risk-based recurrent, documented reviews. where managers 306 confirm the continued access of their employees in order to detect accesses which should 307 have been changed or revoked during daily operation, but were accidentally forgotten. If 308 user accounts are managed by means of roles, these should be subject to the same kind of 309 reviews, where the accesses of roles are confirmed. The reviews should be documented, and 310 appropriate action taken. The frequency of these reviews should be commensurate with the 311 risks and consequences of changes in systems and data made by unauthorised individuals. |
| USA | ISPE | 313 | 313 | ISPE recommends that recommends data audit trails should be clearly distinguished from system technical logs, access logs, and other event logs. These concepts are currently mixed-up. Note that this would bring the text in alignment with the accurate glossary definition of Audit trail, which reads: "In computerised systems, an audit trail is a secure, computer generated, time-stamped electronic record that allows reconstruction of the events relating to the creation, modification, or deletion of an electronic record." | Various system events and other logs may record all kinds of general events such as logons and technical system aspects, including configurations and settings, and access levels, but these are not "about" a specific predicated GMP record in the same way as a data audit trail event. They do not log the creation, modification or deletion of a record as part of the history of that record, such that the GMP event can be reconstructed. This important distinction is made clearly in 21 CFR Part 11, which refers to the subject record when describing audit trail requirements. | See comments following for Section 12 |
| USA | ISPE | 314 | 317 | Section 12.1. Manual user interactions confuse data audit trails and other system activities and logs. This section should cover only cases where users can create, modify or delete GMP data during operation. The logging and management of settings or access privileges, and acknowledgement of alarms are completely separate processes. Processes should be established for the management of alarms including alarm acknowledgement. These are separate from, and different to, data audit trail functionality. | Access logs and other types of system logs should not be confused with data audit trails, which record operator action that create, modify or delete GMP records. Data audit trails refer to specific subject records and should be maintained for the same retention period as the subject record. There is and can be no such requirement where there is no subject record. We suggest adding into the glossary definition of different logs in systems. | Remove reference to system settings, access privileges, and acknowledgement of alarms when discussing data audit trails. Add requirement where appropriate in other sections of the Annex that processes should be established for the management of system settings and for the management of access privileges, and management of alarms. |
| USA | ISPE | 318 | 324 | The detailed guidance provided may not be suitable for all systems and situations. For example, data in a pharmacovigilance/drug safety system is continuously updated as new information becomes available. While the who, what, and when should be recorded in the audit trail, the why may not be necessary for each data point, as it is clear due to the nature of the supported process. We suggest including this description in the Audit trail definition in Glossary. Alternative text is suggested. | The detailed guidance provided may not be suitable for all systems and situations. | Suggested rewording: For GMP-relevant data , the audit trail should unambiguously capture the user who made a change (including the user's role, if users may have more than one role), what was changed (including the data that was changed and the old and the new value), and the date and time when the change was made (including the time zone if applicable)... Where data is modified from an old value to a new value, the reason for the change should be documented in the audit trail, unless a justified exception applies or the reason is clear by context. |
| USA | ISPE | 325 | 329 | GMP-relevant systems are under change control throughout their life cycle. It is sufficient to state that audit trail functionality should be enabled and locked at all times. Any changes to the audit trail functionality or its configuration would need to be covered by change management processes. | GMP-relevant systems are under change control throughout their life cycle. | Suggest a simplified requirement: 12.3 No edit or deactivation. Audit trail functionality should be enabled and secured locked at all times. 325 and it should not be possible for any user to edit audit trail data. If audit trail settings or 326 system time can be changed, or if the functionality can be deactivated, this should by itself 327 create an entry in the audit trail, and it should only be possible for a system administrator 328 not involved in any GMP activities (see 11.10 Guiding principles). |
| USA | ISPE | 340 | 341 | This wording could be misinterpreted and could, for example, be used to justify making it an IT responsibility to review audit trails in a laboratory system. | FDA Data Integrity and Compliance with Drug CGMP Questions and Answers states "Personnel responsible for record review under CGMP should review the audit trails that capture changes to data associated with the record as they review the rest of the record". Depending on what is meant by "directly involved in the activities" in 12.6, such audit trail review is very often performed by persons very much involved in product testing and release, such as Quality Assurance, Lab Supervisors, Qualified persons and rightly so. | Please consider deleting para 12.6 entirely and rewording the opening sentence of 12.5 to simply state: Audit trail reviews should be conducted according to a documented procedure for the specific system, or type of systems. Audit trail reviews should be conducted as part of the defined record review process under GMP. |
| USA | ISPE | 351 | 353 | This requirement should be limited to GMP data and associated metadata. | This requirement should be limited to GMP data and associated metadata. | Suggested rewording: It should be possible to obtain a complete and searchable electronic copy of system GMP relevant data including audit trail data. Flat and locked files are not acceptable, it should be possible to search and sort data. |

| | | | | | | |
|-----|------|-----|-----|---|--|---|
| USA | ISPE | 357 | 382 | This section contains detailed technical requirements that might be outdated in the future. 13.1-13.8 should be one high level clause no implement requirements detailed in many clauses. | There is too much technical detail that will be outdated soon - suggest replacing sections 13.1 to 13.8 with the simplified text proposed. | Suggested replacement text: Electronic signatures must be unique to each individual and indisputable, equivalent to handwritten signatures. Signatures must be securely linked to their corresponding electronic records and contain the signer's full name, the date and time of signing including time zone, and the meaning of the signature (such as review, approval, or authorship). The system must require an initial full authentication on the first signature, and re-authentication via password or biometrics for each subsequent signature in the same session. |
| USA | ISPE | 388 | 423 | While the need for periodic reviews is undisputed, the frequency and scope should be determined following a risk-based approach. The wording in this section implies that all items listed are mandatory for each system with GMP relevance and suggests a need for re-validation which has never been a requirement and should not be now. We suggest referring to Chapter 1 Eudralex vol 4 which consider PQS, QRM, ICH Q9, ICH Q10. We suggest replacing all the section with the proposed rewording. We suggest Annex 11 should not describe the HOW to implement the requirement but focus on WHAT are the requirements. | Section 14. Periodic Reviews is overly prescriptive and defines details relating to periodic review which are unnecessary in a regulation. We suggest removing all of 14.1 to 14.3 and replacing it with the simplified text proposed. | Suggested replacement text: Periodic reviews of GMP-relevant systems in operational use should be conducted against a defined procedure. The review should verify whether the system remains in 'a validated state' and, if not, identify any activities necessary to return it to a validated state. The frequency and scope of reviews should be established and justified based on the risk the system poses to product quality, patient safety, and data integrity. |
| USA | ISPE | 424 | 504 | 15 Security. As a detailed 'how to' this section misses crucial requirements and is overly based on current technology and practices. We strongly recommend the regulation focuses on "what" must be achieved not how. Please consider referring instead to ISO standards for IT security, specifically the ISO 27000 series, which provide an internationally accepted framework for establishing, implementing, and maintaining an information security management system (ISMS). We suggest removing all the clauses from this section and made just one clause (see proposal) and refer to ISO 27000 series which could be quoted in a foot note | The annex would be better simply requiring an effective ISMS aligned with international standards and current good practice. | Simplified text is proposed to replace all of section 15 Security: Regulated users should implement an Information Security Management System based on the ISO/IEC 27000 framework and/or NIST Cybersecurity Framework (CSF) to safeguard authorised access to GMP systems and data and to detect and prevent unauthorised access to those systems and data. The effectiveness of the framework should be monitored and tested ongoing following a risk-based approach. Operating systems, platforms and applications should be updated in a timely manner according to vendor recommendations. |
| USA | ISPE | 526 | 530 | This section suggests that an end-of-process activity is required and that data cannot remain in the system under the original controls. It also implies that archival must occur via system interface, not manual export/import. While the intent is likely to ensure data integrity throughout the lifecycle, this can also be achieved by retaining data in the live system with appropriate access controls and audit trails to capture any changes. | A simplified replacement text for 17.1 is proposed. | 17. Archiving 17.1. Read-only. After completion of a process, e.g. release of a product, GMP data and metadata (incl. audit trails) should be protected from deletion and changes throughout the retention period. This may be by changing its status to read-only in the system where the data was generated or captured, or by moving it to a dedicated archival system via a validated interface. Archived GMP-relevant data, including metadata, should be managed according to a defined process, stored securely, and access strictly controlled. |
| USA | ISPE | 531 | 536 | Section 17.2 Verification This section is not needed as there is already guidance on data migration in 10.3 | n/a | Please delete section 17.2. |
| USA | ISPE | 537 | 539 | Section 17.3 Backup This section is not needed as there is already guidance on backups detailed in Section 16 We suggest as well Archiving is covered in Chapter 4 | n/a | Please delete section 17.3. |
| USA | ISPE | 540 | 543 | Section 17.4 Durability This section is not needed as there is already guidance on backups detailed in Section 16 | n/a | Please delete section 17.4 |
| USA | ISPE | 548 | 551 | The glossary defines only "ALCOA+", while Chapter 4 refers to "ALCOA++". There is inconsistency between the two draft documents (Annex 11 and Chapter 4). | Harmonised terminology is important for clarity and consistent implementation across the GMP framework. Inconsistent use of terms like "ALCOA++" may lead to confusion about the expected data integrity principles. | The terminology should be harmonised across all chapters and annexes. |
| USA | ISPE | 614 | 616 | Validation would be better defined as fitness for intended use, rather than fitness for purpose, to align with other regulation and industry good practice. Alternative text is suggested. | This would also align with fit for intended use as used on line 391. | Suggested rewording: Validation of a computerised system requires ensuring and demonstrating the fitness for its - purpose intended use. |

| | | | | | | |
|-----|------|-----|-----|---|--|--|
| USA | ISPE | 547 | 547 | The glossary is a very important part of the document. It should bring clarity in the understanding of the wording we suggest adding two terms in the glossary "critical" and "regulated user". | Critical is used 20 times in the document not always with the same meaning. We suggest clarifying this term and back ground understanding. Sometimes it relates to simple ideas some time with more complex concepts. Regulated users is not defined in Pharmaceutical regulations. we suggest using other terms such as manufacturers or users with a definition including all activities carried out in the manufacturing activities. | Definitions are requested for "critical" and "regulated user", which would be better described using a more common word. |
| END | | | | | | |