Annex 11 Computerised Systems in Consultation

Reviewing the Changes in Annex 11

Author:Eleanor | Date: 11 July 2025

Contents

1. Annex 11 Update – Draft in Consultation

Annex 11 has undergone a rewrite and several consultations. It is in stakeholder consultation with the content below.

For a review of the impact of these changes, strategic considerations that organisation will need to make, read Transforming Computerised Systems in GMP Environments.

1.1. Scope and Principles

NEW SECTION

Annex 11 now applies to all types of computerised systems used in the manufacturing of medicinal products and active substances. Eight fundamental principles have been introduced:

1. Systems must be validated before use and kept in a validated state throughout their **lifecycle**.
2. **Risk assessment** is required at all stages, considering system complexity and impact on quality, safety, and data integrity.
3. Proven **alternatives** may be used if they offer equal or better control.
4. **Data must be reliable and secure**, following ALCOA+ principles (e.g. audit trails, access control, signatures).
5. **Functional requirements** must be documented, updated, and used for qualification and validation.
6. The regulated user remains responsible for compliance and must retain evidence for audits for **outsourced activities**.
7. Users must **assure security** by monitoring threats and applying timely protections.
8. Computerisation must **not raise risks** to product quality, safety, or data integrity

1.2. Pharmaceutical Quality System

NEW SECTION

The revised Annex 11 mandates that regulated users implement a comprehensive Pharmaceutical Quality System (PQS) covering all computerised systems and associated personnel.

Key requirements include:

- recording and investigating deviations,
- managing changes through controlled procedures,
- conducting internal audits,
- performing regular management reviews.

Senior management is expected to oversee system control, allocate resources, and foster a culture of data integrity and security.

1.3. Risk Management
FORMALISED

Manufacturers must now apply Quality Risk Management (QRM) principles throughout the entire lifecycle of computerised systems, requiring more rigorous planning, documentation, and ongoing oversight.

- **Apply QRM** across the system's lifecycle, focusing on quality, safety, and data integrity.
- **Identify and assess risks** using defined procedures (e.g. **ICH Q9**).
- **Tailor validation** to system use and associated risks.
- **Mitigate risks** through design or process changes, shaping system architecture.
- **Evaluate data** criticality, vulnerability, and detection likelihood.

1.4. Personnel and Training
MINOR CHANGE

The Annex 11 update now specifies the training requirements for personnel, aligning with general GMP requirements, whilst still highlighting the importance of collaboration among stakeholders

1.5. System Requirements
NEW SECTION

This entirely new content might increase the burden on documentation and validation teams, but will ensure better system control and audit readiness:

1. **GMP Functionality:** Users must define and approve system requirements (e.g. URS) for GMP-relevant functions, regardless of system type or development method.
2. **Extent and Detail:** Requirements should reflect system risk and complexity, supporting all development stages and covering key aspects like functionality, data integrity, and compliance.
3. **Ownership:** Users must review, approve, and own vendor-supplied requirements to ensure GMP alignment.
4. **Update:** Keep requirements current to reflect changes; they form the basis for qualification and validation.
5. **Traceability:** Maintain links between requirements, design, and validation tests using suitable tools.

6. **Configuration:** Clearly document any configured or modified functionality in a controlled specification.

1.6. Supplier and Service Management

RESCOPED

This requirement of the previous version has been reframed, providing greater clarity on key points:

1. **Regulated users** remain fully accountable for GMP compliance, even when relying on vendors or IT departments.
2. Conduct **risk-based audits** to assess vendor/service provider procedures and documentation.
3. **Maintain control** via SLAs and KPIs to ensure performance and compliance.
4. Ensure all required **documentation is accessible** and explainable from the user's facility.
5. **Agreements** must define:
    - Provided activities and documentation
    - Compliance requirements
    - Reporting and oversight terms
    - Audit and inspection support
    - Issue resolution
    - Quality/security communication
    - Data control exit strategy
    - New version release and testing

1.7. Alarms

NEW SECTION

This new section again carefully itemises specific requirements for alarms, which were previously unmentioned in Annex 11.

- **System Reliance**: Alarms are required when user action is critical to prevent harm to product quality, patient safety, or data integrity.
- **Settings:** Alarm parameters must be justified, validated, and only adjustable by authorised users under controlled procedures.
- **Signalling**: Alarms should trigger clear visual/audible alerts suitable for timely response in the work environment.
- **Acknowledgement:** Only authorised users may acknowledge critical alarms, with a comment explaining the reason.
- **Logging**: Alarms and acknowledgements must be auto-logged with full details. Logs must be secure and uneditable.

- **Searchability**: Logs should be searchable/sortable or exportable to tools that offer this functionality.
- **Review**: Logs must be periodically reviewed to ensure proper handling and identify trends. Review frequency depends on risk.

1.8. Qualification and Validation

SIGNIFICANT CHANGES

This section, whilst previously included, has made some changes particularly regards the responsibilities of the regulated user

1. **Follow GMP Annex 15** for all system functions—standard, configured, or customised.
2. Use documented **risk assessments** to define the scope and depth of qualification and validation.
3. Verify correct **installation, configuration**, calibration, and patching before testing.
4. Provide **evidence** (e.g. test scripts, screenshots) that system requirements are met.
5. Link test cases to specific requirements using **traceability** tools (e.g. RTM).
6. **Prioritise testing** of GMP-critical functions like access control, audit trails, alarms, and backups.
7. Conduct tests using **approved plans** and detailed, repeatable scripts.
8. **Complete validation before use**; conditional use requires documented justification and follow-up.
9. Even if documentation is provided by others, the **regulated user remains accountable** and must review, approve, and ensure it supports GMP.

1.9. Handling of Data

RESCOPED

To safeguard data integrity throughout data lifecycle events:

- Systems must verify **plausibility** of manually entered critical data and use validated interfaces for data transfer.
- Data transfer/migration must follow **validated** interfaces/processes, and encryption should be applied where applicable.
- Critical data should be **encrypted** on a system, where applicable

1.10. Identity and Access Management

NEW SECTION

This new section is a reflection of the data breaches we read about every day. Data must be kept secure by controlling access:

1. **Unique Accounts:** Each user must have a personal account; shared accounts (except read-only) violate data integrity.
2. **Access Management:** Grant, modify, and revoke access promptly as roles change.
3. **Secure Authentication:** Use strong methods (e.g. passwords, biometrics); tokens alone are insufficient.
4. **Password Protection:** Keep passwords confidential and change them at first login.
5. **Password Strength:** Enforce secure password rules based on system risk.
6. **Multifactor Authentication:** Required for remote access to critical systems.
7. **Account Locking & Logout:** Lock accounts after failed logins; enforce inactivity logout with re-authentication.
8. **Access Logging:** Log login/logout details; logs must be searchable or exportable.
9. **Access Control Principles:** Apply least privilege and segregation of duties; review access regularly and document actions.

1.11. Audit Trails

SIGNIFICANTLY EXTENDED

Significant expansion of this section provides better guidance for the specific nuances of handling electronic data that the previous version didn't offer.

1. Systems must **automatically log** all manual user actions that affect data or settings.
2. Audit trails must **capture** who made changes, what was changed, when, and why.
3. Audit trails must be always **active, uneditable**, and changes to settings must be logged.
4. Audit data must be **searchable, sortable**, or exportable for effective review.
5. Reviews must follow **documented procedures**, be investigated if issues arise, and actions recorded.
6. Reviews should be done by **personnel** not involved in the activity being reviewed.
7. **Focus reviews on critical changes** and potential GMP violations.
8. Conduct **reviews before batch release** unless justified otherwise.
9. Full electronic copies of audit trail data must be **available and usable** by the QP at batch release.

1.12. Electronic Signatures

SIGNIFICANTLY EXTENDED

Once again, expanded to reflect the changes in technology since the last version:

1. **Applicability:** Required for systems where GMP mandates a signature.
2. **Open Systems:** Must meet additional national/international standards if access isn't fully controlled.
3. **Re-authentication:** Full re-authentication is required for signing; smart cards or reused logins are not sufficient.

4. **Timestamping:** Systems must log date, time, and time zone of each signature.
5. **Signature Meaning:** Users must be prompted to specify the purpose of the signature (e.g. approval).
6. **Display Details:** Signature display must include full name, username, role, meaning, and timestamp.
7. **Legal Equivalence:** Electronic signatures must be indisputable and equal to handwritten ones.
8. **Record Linkage:** Signatures must be permanently linked to records; changes must invalidate or remove the signature.
9. **Hybrid Systems:** If paper signatures are used for electronic records, changes must invalidate the signature (e.g. via hash checks).

1.13. Periodic Reviews

NEW SECTION

Periodic reviews: Verify systems remain validated and fit for use. Document findings and assess impact on quality, safety, and data integrity.

Scope of review: Include changes to system components, documentation, and combined effects. Review audit findings, incidents, maintenance, contracts, backups, data integrity, and regulatory updates.

Frequency: Conduct reviews per a risk-based schedule. Final review required before system retirement.

1.14. Security

SIGNIFICANTLY EXTENDED

A massive rewrite for this section introducing comprehensive security requirements which includes:

- Security system which safeguards access
- Continuous improvement
- Ongoing training and tests
- Physical access restriction
- Disasters and disturbances design consideration
- Replication of critical data
- Disaster recovery
- Segmentation and firewalls
- Review of firewalls
- Up to date platforms
- Timely validation and migration
- Unsupported and unpatched platforms should be isolated
- Timely patching
- Strict control and scanning of bidirectional devices (e.g. USB)
- Unused ports deactivated
- Anti-virus software installed
- Regular penetration testing for internet-facing critical systems
- Encryption for remote connections

1.15. Backup

NEW SECTION

1. Data and metadata must be **backed up regularly** to prevent loss from errors, deletion, or cyberattacks.
2. Backup intervals and retention periods should be **risk-based** (e.g. hourly to yearly).
3. Backups must be **stored away** from the original system to avoid shared impact from incidents.
4. Backups should be on **separate networks** to prevent simultaneous compromise.
5. **Critical applications and configurations** may also need to be backed up.
6. Restore processes must be **tested and documented** during validation and after changes, ensuring data is accessible.

1.16. Archiving

SECTION EXPANDED

1. **Read-Only Protection:** After process completion, GMP data should be protected from changes—either by setting it to read-only or archiving via a validated interface.
2. **Verification:** Data integrity must be verified (e.g. checksums) before deletion or transfer; archival processes and systems must be validated.
3. **Backup:** Archived data must be backed up regularly, with physical and logical separation.
4. **Durability:** Long-term storage on volatile media (e.g. CDs) must follow validated processes and ensure secure transfer to new media if needed.
5. **Retrieval:** Archived data must be retrievable in a searchable and sortable format, or exportable to tools that support these functions.