DIGITAL QUALITY COMPLIANCE

COMPACT READINESS SUMMARY

EU GMP Annex 11
2025 Draft

What's changing - and what to review now

REGULATORY STATUS

The 2025 text is a consultation draft and is not yet the applicable Annex 11. The January 2011 Annex remains the current baseline.

A focused overview - not a replacement for the official draft or a system-specific gap assessment.

01 | BIG PICTURE

From validation project to lifecycle control

The draft expands Annex 11 into a detailed framework spanning the PQS, data integrity, supplier oversight and cybersecurity.

A PQS & oversight

Computerised systems enter internal audit and management review. Senior management is expected to provide resources and promote data integrity and security culture.

B Lifecycle & QRM

Validated state, requirements and traceability are maintained through change, periodic review and retirement - with risk decisions linked to controls and tests.

C Accountability

The regulated user remains accountable when work is outsourced to vendors, cloud providers, service providers or internal IT.

D Electronic evidence

The direction is toward metadata-complete, searchable electronic evidence that remains usable through backup, restore and archive.

Practical implication

Readiness cannot sit with validation alone. Quality, system owners, IT, security and providers need a joined-up control model.

02 | CONTROL FOUNDATION

Requirements, providers and validation

1 Current URS and end-to-end traceability

Approved requirements should cover GMP functionality, data integrity, interfaces, security, performance and regulatory needs. Traceability should connect requirements to design/configuration and qualification/validation tests.

2 Supplier, SaaS/cloud and internal IT oversight

Use risk- and criticality-based assessment, approved SLAs/KPIs, audit and inspection support, notification duties, version governance and an exit strategy that preserves data control.

3 Risk-based qualification and validation

Verify installation, configuration, calibration, supported platforms and relevant patches. Use detailed repeatable scripts, requirement-level evidence and strong challenge testing for critical functions.

DQC READINESS LENS

Review critical-system URS quality, traceability depth, provider agreements and objective test evidence as one connected control chain.

03 | OPERATIONAL CONTROLS

Identity, audit trails, alarms and security

1 Identity & access

Unique personal accounts; prompt joiner/mover/leaver controls; least privilege; segregation of duties; recurring access reviews; MFA for specified remote access to critical systems.

2 Audit trails

Capture who/role, what, old/new values, when/time zone and why. Keep trails enabled and protected, with searchable evidence and independent, risk-targeted review.

3 Alarm lifecycle

Justify and validate limits and delays, restrict configuration and acknowledgement, protect alarm logs and perform documented risk-based review and trending.

4 Cybersecurity baseline

Supported platforms, timely patching, segmentation, restrictive firewalls, controlled removable media, malware protection, secure remote access and testing for critical internet-facing systems.

Do not treat these as generic IT controls.

The draft connects them directly to GMP risk, validated state, data integrity and evidence available for review and inspection.

04 | WHERE TO START

A practical four-stage sequence

Prioritise by GMP impact and evidence weakness - not by attempting to remediate every system at once.

1

Immediate baseline

Confirm governance, regulatory watch and a complete GMP system/service inventory. Triage shared accounts, audit trails, critical providers, unsupported platforms and restore capability.

2

Control design

Approve target standards for URS/traceability, IAM, audit-trail review, alarms, supplier/cloud oversight, cybersecurity, backup and archive.

3

Risk-based remediation

Prioritise batch-release systems, critical data/calculations, internet exposure, weak audit trails, unsupported technology and unproven restores.

4

Sustainable operation

Embed metrics, management review, internal audit, access and audit-trail review, provider KPIs, threat monitoring, periodic review and resilience exercises.

FROM SUMMARY TO EVIDENCE

Ready for Annex 11 - system by system?

A corporate standard is only the starting point. Actual readiness depends on each system's intended use, configuration, data flows, providers, controls and available evidence.

Digital Quality Compliance supports organisations with:

- system-specific Annex 11 gap assessments
- eQMS, CSV and digital quality systems
- data integrity and inspection readiness

25+ Years of Pharma and GxP Expertise

Exactly When You Need It.

digitalqualitycompliance.com

Based on the European Commission Revised Annex 11 consultation draft (published 7 July 2025).

The January 2011 Annex 11 remains applicable until a final revision and effective date are published.