Reprinted from PHARMACEUTICAL ENGINEERING®
The Official Magazine of ISPE
July/August 2011, Vol. 31 No. 4
www.ISPE.org

ISPE GAMP COP Annex 11 Interpretation

The ISPE GAMP Community of Practice (COP) provides its interpretation of the revised EU GMP Annex 11 *Computerised Systems* and consequential amendment of EU GMP Chapter 4 Documentation.

by Winnie Cappucci, Chris Clark, Tim Goossens, and Sion Wyn

Introduction

This interpretation of the revised Annex 11 requirements has been produced by a core GAMP COP Task Team, and reviewed by the GAMP COP Council and members of GAMP Regional Steering Committees.

The GAMP COP believes that there is nothing in the revised Annex 11 – if interpreted in a pragmatic and reasonable way – that should cause major concern or problems to any regulated company that was complying with the previous Annex 11, and generally following good practice as defined in GAMP 5 and associated key Good Practice Guides. The revised Annex 11 adopts a risk based approach, and is aligned with current industry good practice.

There is a risk of regulated companies and their suppliers over-analysing detailed wording (either new or changed) in extreme detail, looking for nuances and distinctions not intended by the authors of the regulation.

The GAMP COP advocates a sense of perspective and balance, and avoiding any unnecessary over-reaction to a sensible and reasonable piece of regulation.

Overview

The European Commission (EC) has announced a new revision of EU GMP Annex 11 *Computerised Systems*, and consequential amendment of EU GMP Chapter 4 *Documentation*. These will come into operation by 30th June 2011.

Annex 11 has been revised in response to the increased use of computerised systems and the increased complexity of these systems. The Annex defines EU requirements for computerised systems, and applies to all forms of computerised systems used as part of GMP regulated activities.

EU GMP Chapter 4 requirements on generation, control, and retention of documents have been revised in the light of the increasing use of electronic documents within the GMP environment, and in the light of the Annex 11 revision.

Initial draft revisions had been released for public consultation in April 2008. There was significant industry feedback, including substantive and detailed comments from the ISPE GAMP Community of Practice. Most of the issues raised by the GAMP COP have been addressed in the final revisions. The most significant aspects of the revisions are:

- Risk based approach to validation and operational controls
- Harmonization with current industry good practice
- Clarification of the acceptability of electronic records and signatures

Quality Risk Management

A significant addition to the revised Annex is a new clause on quality risk management, which states:

> *Risk management should be 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, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.*

This risk management based thinking, focused on patient safety and product quality, and based on good product and process understanding, is the key to a correct interpretation and understanding of the requirements in this regulation, and how appropriate controls to meet the requirements should be applied by the regulated companies.The revised Annex also states that regulated companies should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.

The risk management approach adopted is very much in line with ICH Q9 *Quality Risk Management* and the ISPE GAMP 5 Guide: *A Risk Based Approach to Compliant GxP Computerized Systems*.

Current Good Practice

The revised requirements are closely aligned with current industry good practice.The Annex is harmonised with GAMP 5 life cycle terminology such as the use of Project Phase and Operational Phase, and uses GAMP 5 terminology for roles and responsibilities such as System Owner and Process Owner. There is also good match between the operational requirements and the topics covered in the GAMP Good Practice Guide: *A Risk Based Approach to Operation of GxP Computerized Systems*.

Enhanced and clarified requirements covering suppliers and service providers have been included, reflecting the increasing role of IT service providers, and the increased dependence on supplier activities and documentation.

One aspect requiring clear interpretation is the requirement that quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request. Other interesting aspects include the need for:

- An up-to-date inventory of GMP systems and their functionality

- Documented adequacy assessments for automated testing tools and test environments

- Periodic evaluation of systems to confirm that they remain in a validated state and are compliant with GMP.

These are, however, already established industry good practice.

Electronic Records and Signatures

Annex 11 and Chapter 4 revisions together clarify the acceptability of the use of electronic records and signatures for GMP purposes. Some definitions, terms, and requirements for electronic records have been moved to Chapter 4.

Chapter 4 states that documentation may exist in a variety of forms, including paper-based, electronic or photographic media. Many documents (instructions and/or records) may exist in hybrid forms, i.e. some elements as electronic and others as paper based.

Records include the raw data which is used to generate other records. For electronic records regulated users should define which data are to be used as raw data. At least, all data on which quality decisions are based should be defined as raw data.The requirements of Chapter 4 include:

- Complex systems need to be understood, well documented, validated, and adequate controls should be in place

- Appropriate controls for electronic documents such as templates, forms, and master documents should be implemented.

- Appropriate controls should be in place to ensure the integrity of the record throughout the retention period.

The requirements covering electronic records and signatures are broadly in line with current US FDA expectations and interpretation of 21 CFR Part 11, but are less detailed and prescriptive.

Detailed Interpretation

Disclaimer: ISPE cannot ensure and does not warrant that computerized systems managed in accordance with this interpretation will be acceptable to regulatory authorities.

This interpretation is subject to update and change without notice.

Limitation of Liability: In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

Section	Interpretation
Principle	
This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfil certain functionalities.	This is similar in intent but not identical to the *PIC/S Good Practices for Computerised Systems in Regulated "GXP" Environments' (PI 011)*, which also includes controlled functions and associated documentation in the definition of computerised system. The definition is interpreted as being consistent with GAMP 5 terminology and usage, where the computerised system consists of the hardware, software, and network components, together with the controlled functions and associated documentation.

Section	Interpretation
Principle (continued)	
The application should be validated; IT infrastructure should be qualified.	This is consistent with the GAMP 5 approach to validate GxP regulated applications and to ensure control and compliance of the infrastructure (following GAMP 5 guidance regarding Category 1 components, and the *GAMP Good Practice Guide: IT Infrastructure Control and Compliance*). GAMP 5 defines Computerized System Validation as: *Achieving and maintaining compliance with applicable GxP regulations and fitness for intended use by:* • *the adoption of principles, approaches, and life cycle activities within the framework of validation plans and reports* • *the application of appropriate operational controls throughout the life of the system* The compliant and validated status of GxP applications are dependent upon an underlying IT Infrastructure being in a demonstrable state of control and regulatory compliance. The infrastructure should be brought into initial conformance with the regulated company's established standards through a planned verification process building upon acknowledged good IT practices. Once in conformance, this state should be maintained by established processes and quality assurance activities, the effectiveness of which should be periodically verified.
Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.	This is largely equivalent to a similar clause in the previous version. It underlines the focus on risk. This is consistent with the overall risk-based approach taken in GAMP 5 and ICH Q9.
General	
1. ***Risk Management*** Risk management should be 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, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	This is a significant, and welcome, new clause. This is consistent with the overall risk-based approach taken in GAMP 5 and ICH Q9.
2. ***Personnel*** There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	This is largely equivalent to similar clauses in the previous version. The GAMP 5 terms Process Owner and System Owner are used. Training should ensure that persons who develop, maintain, or use computerized systems have the education, training, and experience to perform their assigned tasks.
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, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.	The revision has expanded the requirements to clarify what is required, but has not introduced new concepts beyond current good practice. ICH Q10 Pharmaceutical Quality System, specifically the guidance on Management of Outsourced Activities and Purchased Materials is relevant and should be considered. This clause reflects the trend to centralize or outsource computerized system related services throughout the system lifecycle. Where this introduces additional GxP risk, such risk should be controlled by clear definition of delegated responsibilities and quality standards, supported by an assessment and periodic evaluation process. For internal providers such as IT departments, an established QMS including formal policies, procedures and supporting audits, are an effective way of meeting this requirements, and in such cases formal contracts – such as would be typical with external service providers –would not be required. For internal service providers agreements such as Service Level Agreements (SLA) and Operational Level Agreements (OLA) as described in Information Technology Infrastructure Library (ITIL) may be useful good practice, but are not mandatory.
3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	This is largely equivalent to similar clauses in the previous version, and consistent with GAMP 5 and ICH Q10 approach to supplier assessment. The regulated company should verify, prior to contract placement, that the supplier has adequate expertise and resources to support user requirements and expectations. The most common mechanism for this is the supplier assessment, which may include an audit depending on risk, complexity, and novelty.
3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	This is largely equivalent to similar clauses in the previous version, and consistent with GAMP 5 approach to supplier assessment, traceability, and design review. Commercial off-the-shelf products should be assessed and verified as being able to meet user and GxP requirements. This requires clearly defined requirements based on product and process understanding, and appropriately traced to verification.

Section	Interpretation
General (continued)	
3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	This is a significant new clause. This, like Clause 3.2 above, is related to the regulated company's responsibility to verify that supplier has adequate expertise and resources to support user requirements and expectations. Evidence of an appropriate assessment process and subsequent judgement of supplier suitability, including significant GMP related findings and outcomes should be made available to regulators on request. Some detailed aspects of assessment finding, especially those related to supplier intellectual property and technology may be covered by confidentiality agreements between the regulated company and the supplier. If a regulator requests supplier information, a request may be passed on to the supplier – and when necessary further confidentiality agreements discussed. For service suppliers of high risk processes, contracts should notify them of the possibility for direct inspection and request timely access to their QMS if needed during regulatory inspection. Note also that general life cycle and validation documentation – including validation plans, validation reports, and verification documents – will also demonstrate that the system is fit for intended use. For IT service suppliers, the regulated company is responsible for assessing the supplier's QMS as fit for purpose and monitoring its effectiveness.
Project Phase	
4. ***Validation*** 4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	This is consistent with the overall risk-based approach taken in GAMP 5 and ICH Q9. It emphasises the risk based approach and the need for documented justification of the life cycle approach.
4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	This is current good practice, and consistent with GAMP 5. Project change control and configuration management should be applied. A computerized system validation report should be produced summarizing the activities performed, any deviations from the plan, any outstanding and corrective actions, and providing a statement of fitness for intended use of the system. See GAMP 5 Appendix M7 for further details.
4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the arrangements, data flows and interfaces with other systems or processes, software pre-requisites, and security measures should be available.	A system list or inventory is current good practice, and is consistent with Annex 15, Clause 4c. See also GAMP 5 Section 6.1.5 Maintaining the System Inventory The need for system descriptions is largely equivalent to similar clauses in the previous version. Current industry good practice is to have a system description (or equivalent – see below) for all GxP regulated systems. This may be covered by the User Requirements specification (URS) or Functional Specification (FS), or a separate document may be produced. A detailed system description may not be necessary for systems with a low risk to product quality or patient safety. The level of detail should be commensurate with risk and complexity of the system. See GAMP 5, Appendix D6 System Descriptions.
4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.	This is largely equivalent to similar clauses in the previous version, but with increased emphasis on the documented assessment of risk and GMP impact. It also underlines the interrelationship of requirements definition and risk assessment activities. Requirements should be based on product and process understanding, and relevant regulatory requirements. Specification of requirements should be focused on aspects with highest risk to product quality and patient safety. Traceability is a process for ensuring that: • requirements are addressed and traceable to the appropriate functional and design elements in the specifications • requirements can be traced to the appropriate verification Traceability should be focused on requirements with highest risk to product quality and patient safety. See GAMP 5 Appendix M5 for further guidance on traceability.
4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.	This is largely equivalent to similar clauses in the previous version. See also comments on other supplier assessment and management requirements above.
4.6 For the validation of bespoke or customised computerised systems there should be 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.	This reflects the added life cycle activities required for a bespoke or customized application, and the use of a controlled life cycle with clearly defined phases or stages. Such life cycle activities should be scaled based on risk, complexity, and novelty. At the conclusion of the project, a computerized system validation report should be produced summarizing the activities performed, any deviations from the plan, any outstanding and corrective actions, and providing a statement of fitness for intended use of the system.

Section	Interpretation
Project Phase (continued)	
4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered.	This shows a welcome increased focus on careful choice of test strategy, including negative or challenge testing, intended to identify defects. Verification confirms that specifications have been met. This may involve multiple stages of reviews and testing depending on the type of system, the development method applied, and its use. Testing computerized systems is a fundamental verification activity. Regulated companies should be prepared to justify the adequacy of their verification approach. Testing is concerned with identifying defects so that they can be corrected, as well as demonstrating that the system meets requirements.
Automated testing tools and test environments should have documented assessments for their adequacy.	Testing often is performed at several levels depending on the risk, complexity, and novelty. One level of testing may be appropriate for simple and low risk systems This clause reflects the increased use of, and acceptability of automated testing methods. The use of the phrase documented assessment for adequacy is consistent with a GAMP Category 1 approach. The type and level of assessment should be commensurate with potential risk. Testing tools and test environments do not typically need to be validated. Specific controls and verification may be appropriate, based on risk, if such tools are used to maintain regulated records.
4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	This is a new clause aimed primarily at data migration and archiving. It is consistent with statements in US FDA Part 11 SCOPe and Application Guidance on the preservation of content and meaning of GxP records during COPying or migration. It is also consistent with the approach described in the GAMP Good Practice Guide: *A Risk-Based Approach to Compliant Electronic Records and Signatures*. Data migration may be required when an existing system is replaced by a new system, when an operational system experiences a significant change, or when the sCOPe of use of a system changes. The migration process should be accurate, complete, and verified. Appropriate guidance is given in GAMP 5 Appendix D7 Data Migration, and the GAMP Good Practice Guide on *Electronic Data Archiving*.
Operational Phase	
5. ***Data*** Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	This is a new clause aimed at system interface design, reflecting the increasing inter-connectedness of systems and increasing number of system-interfaces, and the corresponding need to focus on appropriate risk control during system specification, design, and verification.
6. ***Accuracy Checks*** For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	This is largely equivalent to similar clauses in the previous version. The term "critical data" in this context is interpreted as meaning data with high risk to product quality or patient safety.
7. ***Data Storage*** 7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.	This is largely equivalent to similar clauses in the previous version. It is consistent with statements in US FDA Part 11 SCOPe and Application Guidance on record retention requirements. GAMP 5 gives guidance on data security, specifically in Appendix O11 Security Management.
7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	This is largely equivalent to similar clauses in the previous version, but with added emphasis on the verification of the backup and restore process, and periodic monitoring of that process (e.g. to cover media aging) Backup is the process of COPying records, data and software to protect against loss of integrity or availability of the original. Restore is the subsequent restoration of records, data or software when required. Applicable GAMP 5 guidance on the topic includes Appendix O9 on Backup and Restore. In many cases backup and restore capability will be provided by elements of the IT infrastructure, which as discussed above (See discussion of "Principle") should be in a state of control and compliance. In such cases the individual system backup and restore needs should be specified, configured, and verified.
8. ***Printouts*** 8.1 It should be possible to obtain clear printed COPies of electronically stored data.	This is largely equivalent to similar clauses in the previous version. Regulated companies must provide reasonable and useful access to GMP records to regulators. This is consistent with statements in US FDA Part 11 SCOPe and Application Guidance regarding the availability of human readable COPies in order to provide such reasonable and useful access to records during an inspection. See also GAMP Good Practice Guide: *A Risk Based Approach to Compliant Electronic Records and Signatures*.

Section	Interpretation
Operational Phase (continued)	
8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	This is similar to clauses in the previous version, but with significant additions. Additions indicate the importance of a high level of control over, and transparency of changes to, records supporting batch release. Suitable methods should be selected based on a justified and documented risk assessment, and an analysis of the process. The term printout is interpreted as indicating a suitable human-readable form.
9. ***Audit Trails*** Consideration should be 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 the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	This is largely equivalent to similar clauses in the previous version. The need for, and the type and extent of, any audit trail should be based on a documented and justified risk assessment. This is consistent with statements on audit trails in US FDA Part 11 SCOPe and Application Guidance. See also GAMP Good Practice Guide: *A Risk Based Approach to Compliant Electronic Records and Signatures*. The need for audit trail review should be based on a documented and justified risk assessment, taking into account: • Initial verification of audit trail functionality, and subsequent verification (as appropriate) during change management • Effective segregation of duties and related role-based security • Established and effective procedures for system use, administration, and change management Any review of audit trails deemed necessary should focus on checking that they are enabled and effective. Suitable records security controls should be in place for high risk records, and appropriate segregation of duties enforced (e.g. such that nobody with a conflict of interest has privileges that would allow alteration of data or audit trail configuration). Audit trails should be regarded as only one element in a wider framework of controls, processes, and procedures aimed at an acceptable level of record and data integrity. Audit trails should be regarded primarily as a tool to be used for investigation, as and when required, rather than for continuous routine review. Routine review of all audit trail content is not required, and is not consistent with a risk-based approach. The cost and effort is not justified by any likely benefit.
10. ***Change and Configuration Management*** Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	This is largely equivalent to similar clauses in the previous version. Change management is the process of controlling the life cycle of changes, enabling beneficial changes to be made without compromising regulated processes or records. Configuration management comprises those activities necessary to be able to precisely define a computerized system at any point during its life cycle, from the initial steps of development through to retirement. All changes should be reviewed, risk assessed, authorized, documented, tested, and approved before implementation. These activities should be documented. See GAMP 5 Appendix O6 Operational Change and Configuration Management for more details.
11. ***Periodic Evaluation*** Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	This is a new clause, but consistent with current industry good practice as described in GAMP 5. (See Appendix O8 Periodic Review). It is consistent with Annex 15 clauses 23 and 45. Periodic reviews are used throughout the operational life of a computerized system to verify that it remains compliant with regulatory requirements, fit for intended use, and satisfies company policies and procedures. The review should confirm that, for all components of a system, the required support and maintenance processes are established and that the expected regulatory controls (plans, procedures and records) are established and in use.
12. ***Security*** 12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	This is largely equivalent to similar clauses in the previous version. Measures should be implemented to ensure that GxP regulated computerized systems and data are adequately and securely protected against wilful or accidental loss, damage, or unauthorized change. Such measures should ensure the continuous control, integrity, availability, and (where appropriate) the confidentiality of regulated data. This process should include: • Establishing and maintaining security roles and responsibilities, policies, standards, and procedures • Performing security monitoring and periodic testing, e.g., manual check of system access log, automated notification of lockouts, testing of tokens • Implementing corrective actions for identified security weaknesses or incidents.

Section	Interpretation
Operational Phase (continued)	
12. ***Security (continued)*** 12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. ***(continued)***	• Ensuring a list of those authorized to access the system is established and maintained The design of the system's physical and technical security mechanisms should be assessed and (if necessary) tested. GAMP 5 gives guidance on security, specifically in Appendix O11 Security Management.
12.2 The extent of security controls depends on the criticality of the computerised system.	See above. This is consistent with GAMP 5 risk-based approach to operational controls.
12.3 Creation, change, and cancellation of access authorisations should be recorded.	See above. This is consistent with current industry good practice.
12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	This is a new clause, but the intent is already covered in Clause 9 and Clause 12.1. The approach should be commensurate with the risk associated with the data in question.
13. ***Incident Management*** All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	This is largely equivalent to similar clauses in the previous version. This is current industry good practice. Further guidance is available in GAMP 5 Appendix O4 Incident Management The primary objective of Incident Management is to ensure that any unplanned issues that could impact patient safety, product quality, and data integrity are addressed before any harm occurs. The incident management process should ensure that operational events which are not part of the standard operation (i.e., issues, problems, and errors) are identified, evaluated, resolved, and closed in a timely manner.
14. ***Electronic Signature*** Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.	This clarifies that electronic signatures are allowed, but are not mandatory. It reflects current industry good practice. The phrase "within the boundaries of the company" clarifies that such signatures applied to records maintained by the regulated company are not subject to Directive 1999/93/EC on a Community framework for electronic signatures, nor the 2000/31/EC Directive on electronic commerce, nor any associated national regulations of EU member states on such topics. The approach is consistent to that described in in the US FDA Part 11 SCOPe and Application Guidance See also GAMP Good Practice Guide: *A Risk Based Approach to Compliant Electronic Records and Signatures*, which describes an approach that is consistent with the revised Annex 11 and Chapter 4, as well as the current FDA interpretation of Part 11.
15. ***Batch Release*** When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	This is largely equivalent to a similar clause in the previous version, with additional discussion of electronic signatures This additional discussion is interpreted not as making the use of electronic signatures mandatory for batch release, but rather requiring that if the release is performed electronically that the requirements of Clause 14 above are met. The possibility of repudiation or lack of integrity of such high risk signatures should be managed by suitable controls, based on a justified and documented risk assessment.
16. ***Business Continuity*** For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	This is largely equivalent to similar clauses in the previous version. This is current industry good practice, and consistent with GAMP 5, e.g. Appendix O10 Business Continuity Management. Patient safety, product quality, and data integrity should not be compromised by system failure or breakdown. The regulated company should perform business continuity planning to actively protect its ability to continue to supply the public, and to comply with the regulatory requirements. Business continuity processes should be documented, communicated, and verified as effective.
17. ***Archiving*** Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	This is largely equivalent to similar clauses in the previous version, and is consistent with Section 7 and 10 above. It underlines that checks and controls are required to ensure the preservation of data and record content and meaning throughout the required retention period. Computerised systems change management should take into account potential risks to data and record retention capability.