Changes to PIC/s Annex 11 and GAMP

- Presented by Seamus Orr, 6th August 2018

Hosted by PharmOut

GMP, Engineering & Cannabis Forum 2018

PharmOut

Session Agenda

- Review Key Changes to Annex 11 of PIC/S PE-009-13
- How will this affect you?
- EU Annex 11 Updates
- Guidelines on Annex 11 Compliance

PIC/s PE 009-13

Annex 11 on Computerised systems:

(0 major/12 minor)

- Rewrite of the entire Annex
- Introduction of QRM principles
- Contains a lot of new clauses - Minor?
- Change to Management of Suppliers & Service Providers
- Inventory of IT systems + GxP risk
- Introduction of a requirement to **periodically review** computerised systems for their validated state

Annex 11

Risk Management

Required throughout the lifecycle

Roles and Responsibilities

Process Owner: Responsible for the Business Process

System Owner: (Typically)

Responsible for Availability of system
Maintenance of system
Security of the data on the system

EU GMP – PIC/S Guide Annex 15 "Qualification & Validation"

Main Changes:

- Cross-reference made to Annex 11 Computerised systems
- Planning and documentation for Qualification and Validation
- Added information on the qualification stages for equipment, facilities and utilities
- No disconnect between process & automation

Annex 11

Principle

The application should be validated; IT infrastructure should be qualified.

Principle

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.**

Annex 11

Clause §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.

Annex 11

Clause §2 Personnel

- There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Authorised Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

Suppliers and Service Providers

§3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that **user requirements are fulfilled**.

Clause 3: Suppliers & Service Providers

Clause §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.

Clause §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.

Clause 3: Suppliers & Service Providers

Clause §3.3

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.

Clause §3.4

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.

GAMP Software Categories

CATEGORY	DESCRIPTION		RANGE OF APPLICATIONS	TYPICAL EXAMPLES
5 Custom Software	Software custom designed and coded to suit the business process.	↑	Complex application, coding language requires consideration of program level decisions/timing/looping as well as process level decisions/timing/looping.	VB or C++ Application DCS or SCADA scripting IEC61131-3 IL or ST application IEC61131-3 LD or SFC application
4 Configured Software	Software (often very complex) which can be configured by the user to meet the specific needs of the user's business process. Software code is not altered.	↑	Library functions selected, parameterized and connected with branches and decisions. Increasing complexity of configuration. Library functions selected, parameterized, and connected in linear fashion.	IEC61131-3 FBD application Vision system software DCS/SCADA Databases **Smart camera software**
3 Non-Configured Software	Runtime parameters may be entered and stored but the software cannot be configured to suit the business process.	↑	Standard item needs a large parameter file loading before it will work. Increasing complexity of parameterization (works 'out of the box').	Electronic Chart Recorder PID Controller Smart Transmitter
1 Infratructure Software	Software used to manage the operating environment. Layered software upon which applications are built.		Refer to GAMP 5 and the GAMP Good Practice Guide: IT infrastructure Control and Compliance for further details.	Version Control Tools Programming Languages Underlying Operating System

Source: GAMP® Good Practice Guide: A Risk-Based approach to GxP Process Control Systems Figure 4.8.: illustrative examples of software categories.

Potential Outcomes from Supplier Risk Assessment

Summary of approach as a result of Risk Classification categorisation

Risk Classification	Compliance Expectations: Business, Regulatory & IT Standards , e.g. security	Computer Testing Package	Computer Validation Test Execution
Low Risk	Not specified to supplier	Supplier standard accepted	Performed by supplier
Medium Risk	Specified to supplier and where applicable, applied to system	Supplier standard accepted where compliance expectations covered (or additional testing scripts created)	Performed by supplier, or with support for additional testing
High Risk	Specified to supplier and applicable to entire system	Specific package developed , based on detailed risk based testing approach for compliance expectations	Performed by supplier with sign-off, or performed by site

Annex 11

Clause §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.**

Clause §4.2

Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

Annex 11

Clause §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 physical and logical arrangements, data flows and interfaces with other systems or processes, any

Annex 11

Clause §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**

Clause §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. Automated testing tools and test environments should have documented assessments for their adequacy.

User Requirements Specifications

- A document that specifies the requirements for a computerised system – what it should do
- Should be commensurate with level of risk, complexity and novelty of system
- Should be detailed enough to allow for subsequent verification of system requirements
- May include operational requirements , functional requirements , data requirements, technical requirements, interface requirements, performance requirements, security requirements, maintenance requirements, retirement requirements
- For commercially available systems - may be part of purchasing document

Software Validation

Category	Validation Approach
1 Infrastructure Software	●Record version (include service pack). ●Verify Correct Installation
3 Non - Configured	●URS ●Record version and verify installation ●Risk based tests against requirements ●Procedures put in place for maintaining compliance ●Consider auditing supplier for critical and complex applications
4 Configured	●As above, plus… ●Life cycle approach ●Supplier questionnaire – Adequate QMS ●Risk based tests against requirements in a test environment ●Risk based tests against requirements within the business process
5 Custom	●As above, plus… ●Full life cycle documentation ●Design and source code review *GAMP 5 Appendix M4*

Annex 11 – Data Storage Changes

Clause §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.

Clause §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.

Annex 11 – Audit Trail

Clause §9

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.

Annex 11 – Periodic Re-evaluation

Clause §11

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.

Annex 11 – Security

Clause §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.

Clause §12.2

The extent of security controls depends on the criticality of the computerised system.

Clause §12.3

- Creation, change, cancellation of access authorisations to be recorded.

Clause 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.

Annex 11 – Incident Management

Clause §13

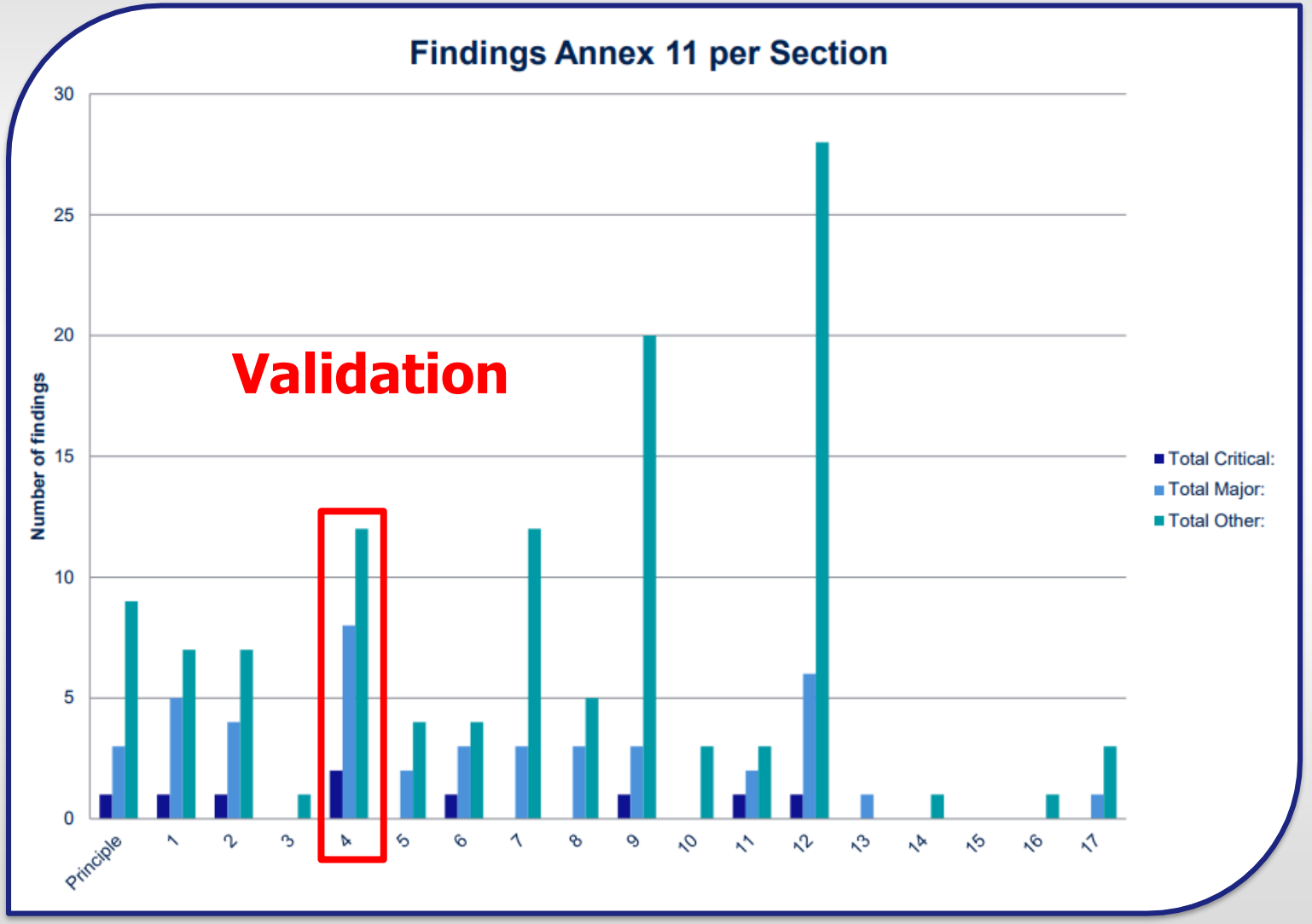
All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

Annex 11 – Business Continuity

Clause §16

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.

Annex 11 – Computerised Systems



Data integrity implicit in PIC/S

6.16. The results obtained should be recorded and checked to make sure that they are consistent with each other. Any calculations should be critically examined.

6.17. The tests performed should be recorded and the records should include at least the following data:

a) name of the material or product and, where applicable, dosage form;

b) batch number and, where appropriate, the manufacturer and/or supplier;

c) references to the relevant specifications and testing procedures;

d) test results, including observations and calculations, and reference to any certificates of analysis;

e) dates of testing;

f) initials of the persons who performed the testing;

g) initials of the persons who verified the testing and the calculations, where appropriate;

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.

What does the TGA expect?

Between 1 January and 30 June 2018

- Documented assessment of Annex 11 changes and impact upon existing operations
- Change controls and/or Continual Improvement activities initiated within QMS, This assessment should lead to corrective and preventative actions being taken as necessary.
- Implement changes, demonstrate effectiveness and audit readiness by 1 Jan 2019

Examples Deficiencies – Annex 11

- The [business continuity process] was not available for use as documented in [a deviation]. The associated investigation did not assess why the contingency procedure and process had failed.
- The clock used for determining time/date for the HPLC software could be adjusted therefore allowing the option to alter the true time and date in the printed paper records
- There were no audits to address the **data integrity controls** within the laboratory, data integrity was not included within the scope of audits of **contact laboratories**
- There were no overall risk assessments of electronic systems within the company in order to define **data integrity control strategies**

Examples Deficiencies – Annex 11

- The qualification of the ERP system was considered deficient in that:
  i. The independent code review was not available for review during the inspection.
  ii. The actual observed results were not always documented within the qualification records
  iii. The procedure for electronic signatures data transfer to the ERP system was not described in a procedure and was not qualified.
  iv. There was no assessment of ERP database integrity.

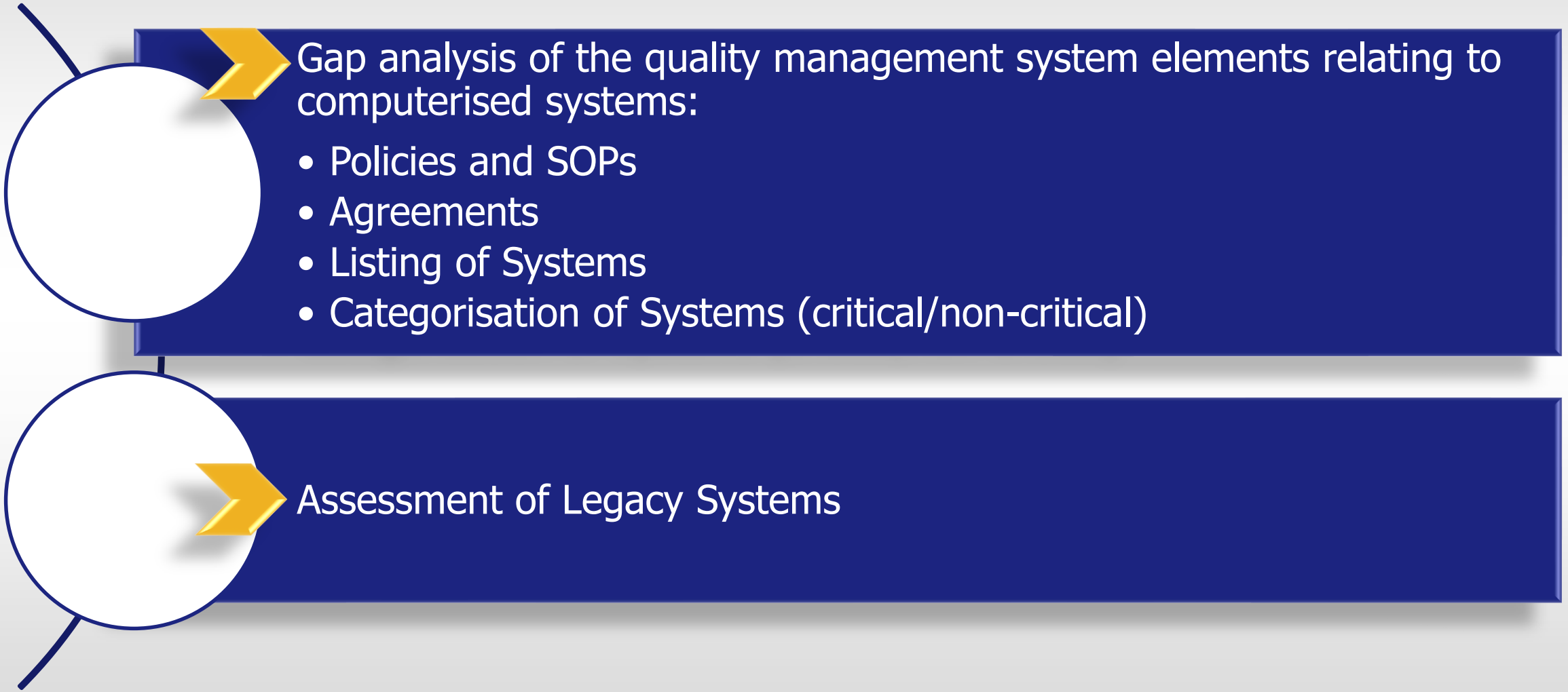
EU Annex 1 - changes

- **Section 2.0 Principle – Manufacture of Sterile Products:**

a) *Facility, equipment and process design must be optimized qualified and validated according to Annex 11 and Annex 15 of EU GMP. The use of appropriate **current** technologies should be implemented to **ensure protection and control of the product** from potential extraneous sources of particulate and microbial contamination such as personnel, materials and the surrounding environment.*

b) *Personnel must have appropriate **skills**, **training** and **attitudes** with a specific focus on the principles involved in the **protection of sterile product** during the manufacturing, packaging and distribution processes.*

Assessment



Legacy Systems

- For each Legacy System:
  1. Define the user requirements
  2. Perform a gap analysis to determine the validation effort for retrospective validation.
  3. Verify user requirements

Recap?

- Software should be validated and maintained
- Infrastructure should be qualified and maintained
- Issues should be appropriately investigated and resolved

Recap?

- Understand your system and it's interfaces
- Risk Assess each system
- There should be no resultant decrease in product quality, process control or quality assurance

Thank you for your time.
Questions?

Seamus Orr
Lead Consultant

seamus.orr@pharmout.net
www.pharmout.net