

Computerised Systems: Current and Future Considerations

Neale Baldwin & Alyce Maksoud
Manufacturing Quality Branch
Department of Health and Aged Care, TGA



GMP FORUM 2024



Australian Government
Department of Health and Aged Care
Therapeutic Goods Administration

tga.gov.au

Agenda

- Current Requirements
- Expectation of the current PIC/S and Section 10 of the Australian Code of GMP (The Code)
- Common Issues/ Deficiencies
 - Current issues observed at Inspection
 - Specific system management issues
 - Technical issues

Agenda

- Future Considerations
 - Cloud-based systems/applications
 - 3rd Party Providers
 - Artificial Intelligence
- Regulatory Developments
 - Developments with the EMA/PIC/s Concept Paper
 - Annex 11 Update proposed timelines


Current Annex 11 and the Code Requirements





PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PE 009-16 (Annexes)
1 February 2022

A magnifying glass with a black handle and a silver rim is positioned over the title text, enlarging it. The title text is enclosed in a black rectangular border.

**GUIDE TO GOOD MANUFACTURING
PRACTICE FOR MEDICINAL PRODUCTS
ANNEXES**

Current PIC/s GMP Annex 11

Updated last in 2011

- Widened scope to consider networking and wider system applications
- Key principles focussed
- Risk-based approach
- Clarification of ownership/responsibilities
- Clarity of validation expectations and System lifecycle management
- Electronic Signatures
- Incident management and Business continuity

Annex 11 Version PE009-16 & the Code

Topics not fully addressed include:

- Complex networks
- Cloud-based data management & applications
- AI/Machine Learning
- Alarm management
- 3rd Party system/infrastructure management
- Virtual security management
- Digital Transformation
- Validation and qualification



However, current key principles can still be applied! (but often aren't)

Common Computer System Issues

Annex 11 and Section 10 of the Code key principles:

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.

The application should be **VALIDATED**; IT infrastructure should be **QUALIFIED**.

There should be **CLOSE COOPERATION** between all relevant personnel such as Process Owner, System Owner, Authorised Persons and IT.

General problem categories:

- System selection, validation and implementation
- System maintenance, including operating systems and infrastructure
- Control of System use and system ownership
- In other words, issues identified at inspections relate to all stages of 'SOFTWARE LIFE CYCLE' management

Common computer inspection deficiencies/ issues



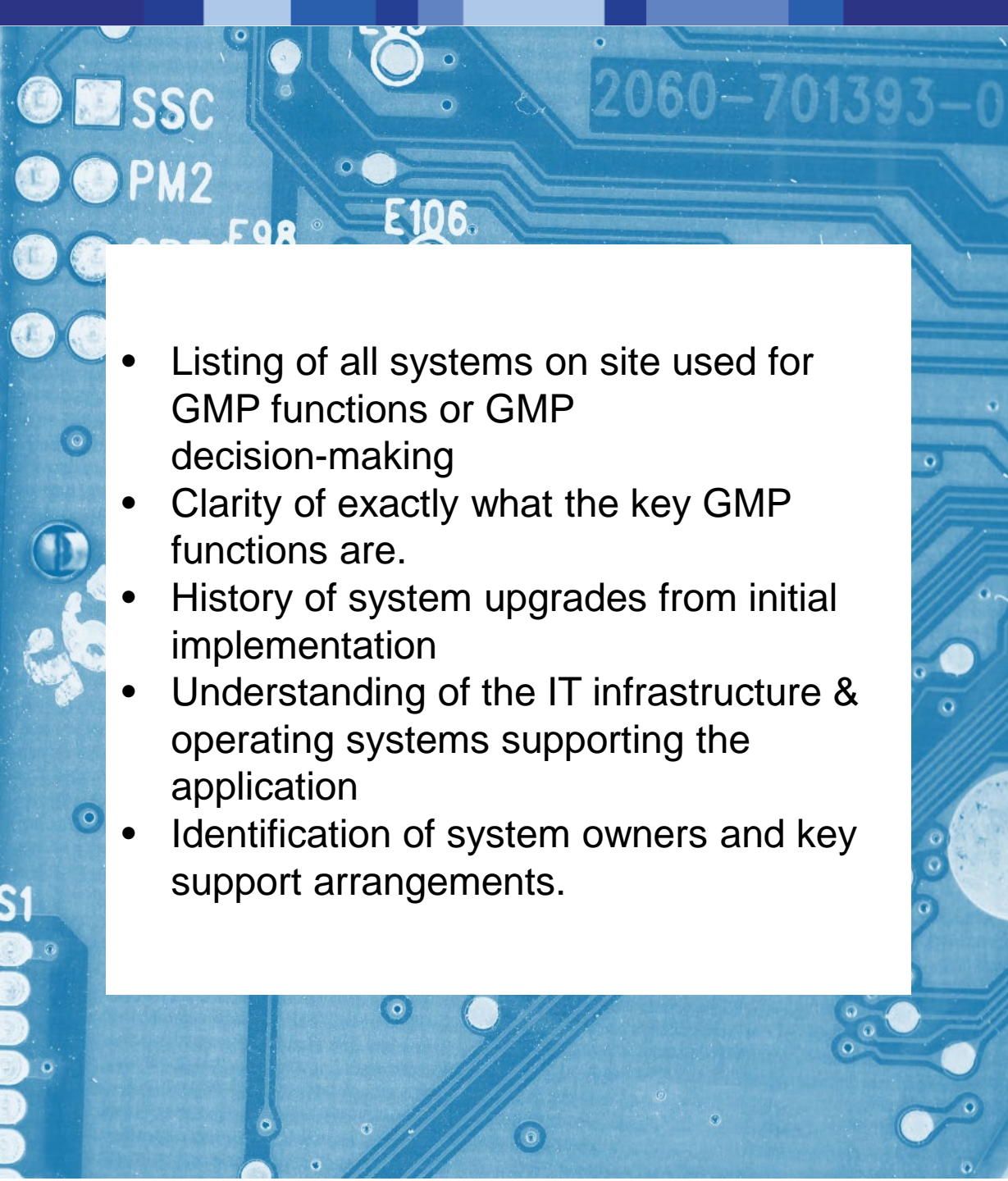
Computer System Identification

Annex 11§4.3 & The Code (Clause 1006)

- 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 hardware and software pre-requisites, and security measures should be available.

Common Issues

- No current listing available or an incomplete/outdated list available.
- No process to ensure systems are assessed for GMP functionality.
- No identification of current and history of application software versions.
- No identification of the validation status.
- No identification of security measures employed i.e.. Procedures, access control mechanisms, etc.

- 
- Listing of all systems on site used for GMP functions or GMP decision-making
 - Clarity of exactly what the key GMP functions are.
 - History of system upgrades from initial implementation
 - Understanding of the IT infrastructure & operating systems supporting the application
 - Identification of system owners and key support arrangements.

Listings/Registries need to:

- Identify all systems including information systems, monitoring & control systems, PLC's, measurement systems, calculation applications (e.g. spreadsheets, stats software, etc.), firmware, etc.
- Identify infrastructure and operating software supporting applications, including network/integration configuration
- Identify the implemented software versions and control of updates
- Identify validation state and any supporting documentation



Information
Databases &
Data analysis
systems

Monitoring &
Control
systems

Manufacturing
Equipment
Systems

QC
Laboratory
Systems

Networks/
Infrastructure
/ Operating
Software

Maintenance
systems

Inventory
Management
systems

Computer System Validation

Annex 11§4.1 & the Code (Clause 1008)

- *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.*

Common Issues

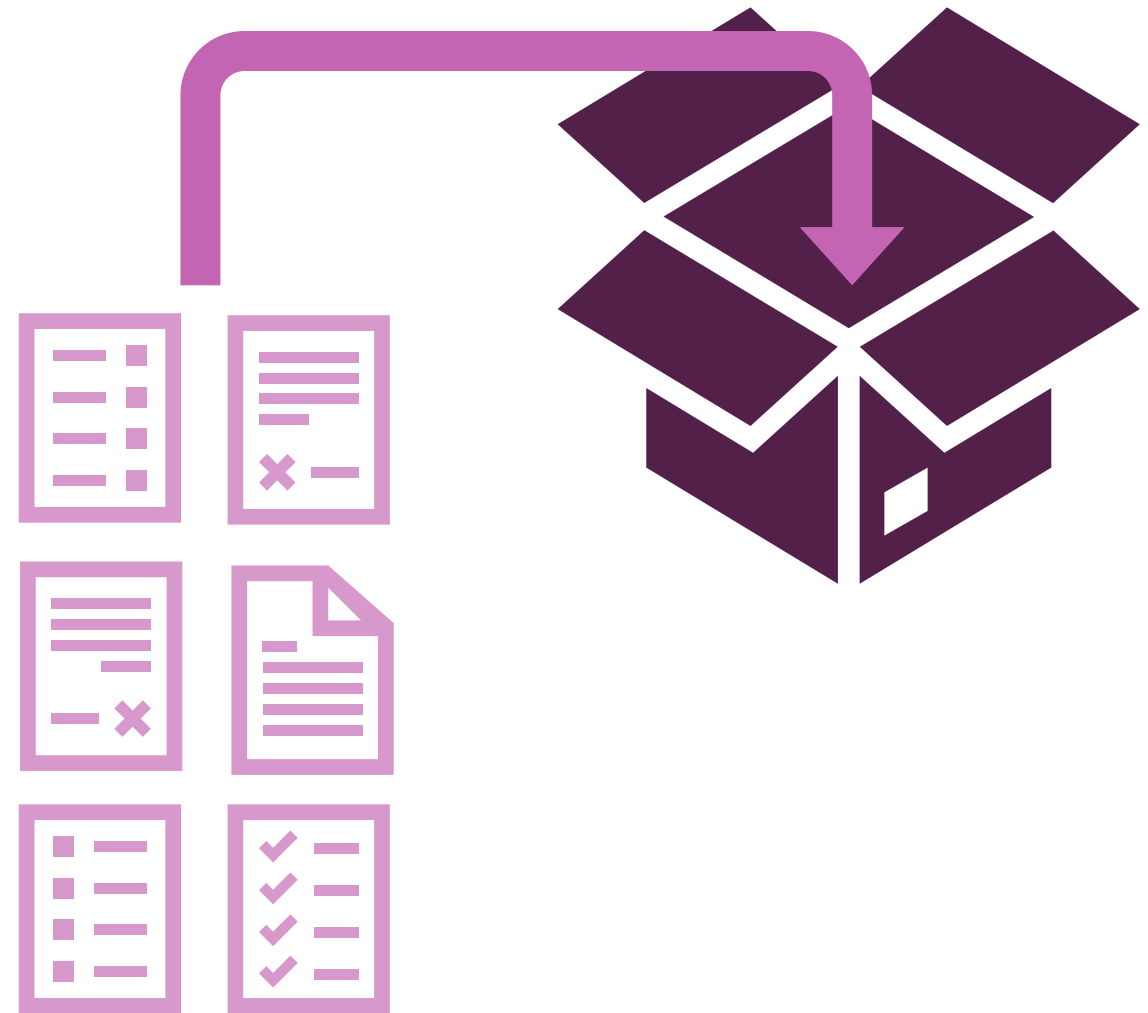
(Excluding issues where systems are not even identified)

- **No validation or no available/complete Validation documentation**
- No Val plan, no RA or justification of approach employed, no URS, no validation summary and release approval
- Often missing or incomplete testing documentation (particularly where supplier Val packages are used)
- No periodic review of validation
- No validation of software/system updates

Validation

Examples

- Company failed to provide complete validation documents
- No record of verification of successful validation before implementation
- No documented release of system to operational environment
- No justification of approach to validation or deliverables
- No change control for initial implementation or for system updates/upgrades
- No periodic review of validation



Inspection Feedback on Vendor Validation Packages

Pros	Cons
Provide general comprehensive approach to system validation including selection of added/optional functionality	Expensive (but probably cheaper than self-developing documentation)
Tried and tested documented testing	Doesn't always cover integration with other systems
Technically comprehensive	Doesn't always cover supporting infrastructure or OS details
Cheaper than self-developing validation documentation	Not all planned functionality is tested/recorded
Have good stage-gate checks	Need to be completed to the satisfaction of the system Owner

Companies appear to spend NO time to understand what is in the documents and assurance that they are satisfactorily completed.

***Ask the vendor to explain!
(You paid good money for it!)***

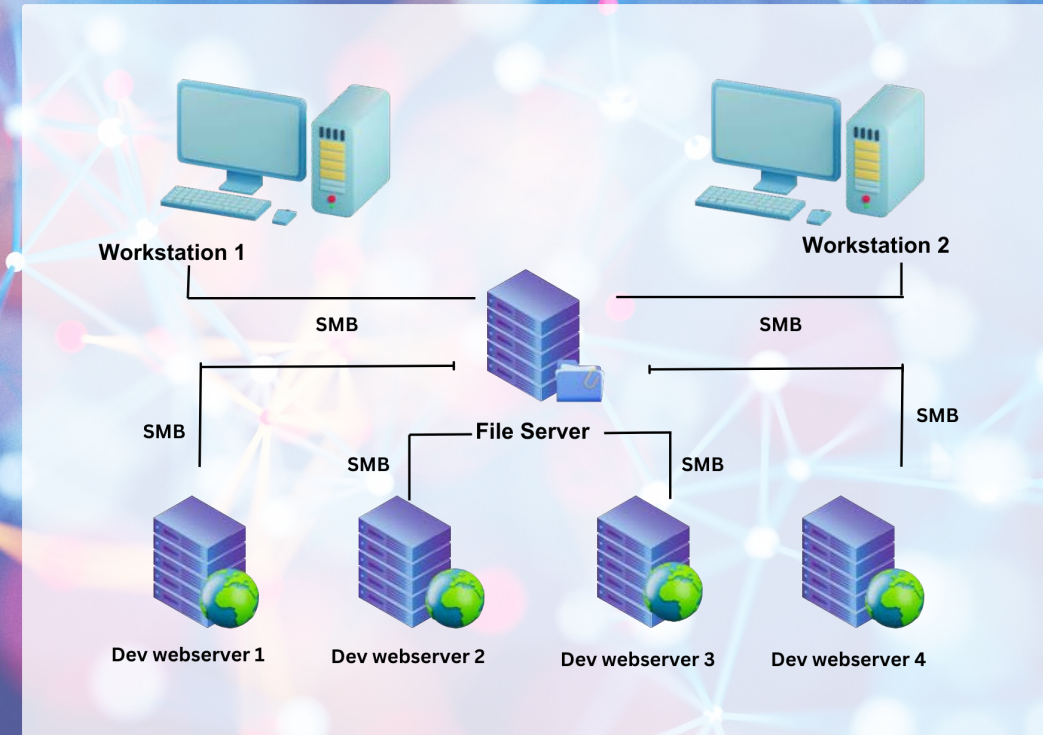
Networks

Annex 11 Principle & the Code (Clause 1000 Principle)

- ... IT infrastructure should be qualified.
- *Definition: IT Infrastructure - The hardware and software such as networking software and operation systems, which makes it possible for the application to function.*

Issues

- Lack of distinction of GMP and non-GMP functionality/security of networks
- Lack of understanding/definition of networks
- Lack of control of changes to networks
- Lack of clarity of ownership of networks and cooperation with system owners
- Lack of control of changes to networks
- Lack of documentation to support qualification



Network



IT

System
Owner

User

IT versus System Owners

- System owners have no understanding of the controls applied to the network
- IT often have no understanding of the criticality/functionality of systems in GMP

What hope does the User have?

Network Definition

- What is the network and how does it interact with GMP functions?
 - Consider both infrastructure and logical/virtual configuration.
 - Consider risks associated with the network and its operation
 - Ensure all understand the network layout and inherent risks (at least in Laymen's terms)
 - Consider business and GMP components and their integrated or separated operation, including network load
 - Ensure all operating in the network understand GMP principles/procedures (particularly administrators/superusers)
- What applications and functions operate on the network?
 - What operations occur within the scope of the network?
 - How are they controlled?
 - What are all GMP applicable functions the network is used for?
- Who are allocated what responsibilities?
 - Who is the network owner and who are the system owners?
 - What are their respective responsibilities?
 - Ensure all understand what their responsibility entails & **ensure they understand** what this means.
 - How do service providers/application support operate in the network? Who supervises them and understands what they do?

Remember:

Annex 11§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.

**How are changes to the network managed?
(Usually not all that well!)**

System/Application Access

Annex 11§12.1 & 12.3 and the Code (Clause 1011)

- *Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons*
- *Creation, change, and cancellation of access authorisations should be recorded.*

Issues

- No appropriate or documented process/procedure User access control & understanding/ application of User access levels.
- Unclear authority/application of User access control.
- Lack of control of User access/ access level changes
- No process for User access removal/expiry
- No regular review to ensure appropriate User access assignment

It is commonly found at inspection that unauthorised, inappropriate or departed users have access to critical GMP systems.



Some (poor) Examples

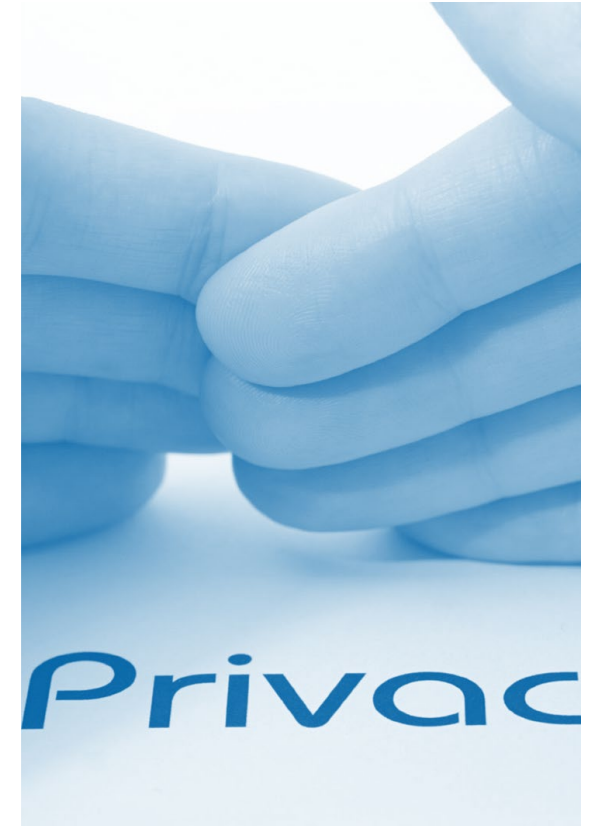
Global manufacturer potential product release disaster

- Global manufacturer decided to provide product release user access to identified Authorised Person delegates.
- Rather than adding the individual delegates, they added the delegates access level profile to the product release access profile.
- By doing so, they inadvertently opened access to product release functionality to all operators, including manufacturing operators, that had the same general access rights as the two delegates.

Change Management issue

- Company failed to maintain integrity of system access by using annual review as the key mechanism to update User access authority.
- QA employee promoted to Manufacturing management yet maintained access to restricted QA functions for 9 months.
- The company's annual user access review wasn't effective as they still had staff with access to systems despite leaving the organisation up to 5 years earlier.

In reality, there was NO User access control process.





Some (Poor) Examples cont.

Admin rights to Supplier

- Despite having robust internal access authorisation processes, software supplier was given general admin access to propriety application.
- The supplier was given remote user access (i.e.. Online access).
- Could make changes and updates without awareness of the system owner or users.
- The supplier had a generic user Id. So there was no record of who had made administrative changes.

Supplier Change Management issues

- Company failed to maintain integrity of system by allowing changes/installing updates without oversight.
- Supplier service arrangements allowed the supplier to routinely service the equipment, including updating software.
- The company had comprehensive initial validation package for the installed software version.
- However, they had no link, validation or associated records to current software version in operation.

This is a commonly observed issue at inspection

Key issues observed

- No assessment of where audit trails are/should be applied.
- No procedures or assignment of Audit trail review.
- No functionality enabled to perform Audit trail review.
- No records of Audit trail review, particularly for critical actions.
- Limited assurance that the data integrity was maintained.
- Inappropriate use of paper-based data translation in place of audit trail review.

*"If it isn't written down,
then it didn't happen"*

Audit Trails

PIC/s Annex 11§9 & the Code (Clause 1007):

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").

[FDA 21 CFR Part 11 regulation](#) requires the system used to manage electronic records to provide a secure, computer-generated, and time-stamped audit trail

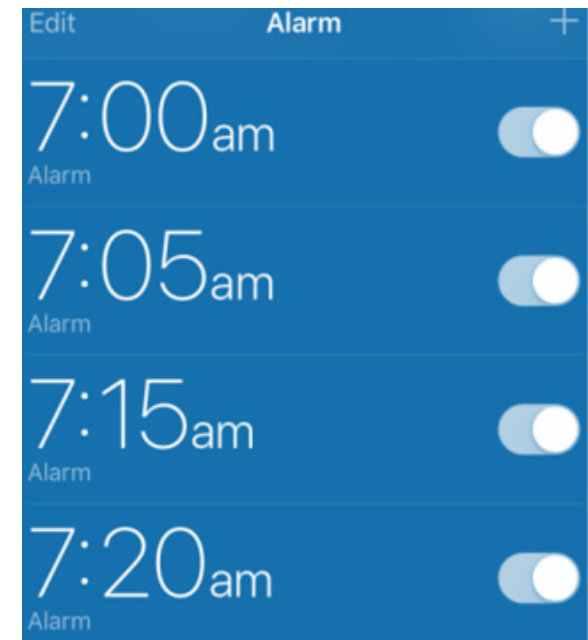
OECD ENV/JM/MONO(2016)13 – Principles of GLP:
Audit trail for a computerised system should be enabled, appropriately configured and reflect the roles and responsibilities of study personnel.

Computerised alarms

Overuse of Alarms

Most systems have numerous alarms, but how do users know which are important alarms, which are just warnings and which are not relevant?

Which Alarm is the important one?



Key Issues with Alarm Management

Critical alarms

Critical Alarms – notify conditions that may impact product quality/performance.

- No definition, criteria or categorisation of critical alarms that require appropriate actions should they be activated.
- Incomplete records and review of these alarms and assurance that appropriate, timely actions were undertaken
- No assessment of impact on the product

Notifications/ Warnings /Alerts

Notifications – notify conditions that may alert the operator to consider more diligent monitoring or to take action to avoid departure from acceptable operating parameters.

- No clarity of which warnings require awareness and what interim actions to take
- Lack of clarity of actions required
- Poor oversight/understanding of notification alarms

Irrelevant or false alarms

False/undefined Alarms – not understood, not assessed or lack of clarity on the actions required.

- No understanding of significant number of false/irrelevant alarms (i.e. usually >90% of all alarms)
- No assessment of impact/relevance for manufacturing processes.

Develop a documented Alarm Strategy

Alarm basics

*What are critical alarms, what are notifications and what are irrelevant alarms?
Categorise Alarms!*

Turn-off unwanted/unused alarms!

*Clarify the time frame that alarms are relevant
i.e. During batch manufacture but not during
down time, over weekends, etc*

*Provide clarity of actions required for critical
alarms and notifications.*

- Provide listing of relevant alarms and when they apply for systems, applications, equipment, etc.
- Make sure it is clear what actions are required and when required
- Ensure mechanism for reporting/acknowledging and assessing impact of relevant alarms.
- Review alarm parameters initially and periodically to ensure they are appropriately notifying of conditions that need to be acknowledged

Be careful of equipment/process automated alarms. These still need to be addressed as the process has been halted/stopped.

Computer System 3rd Party Support

[Annex 11 Section 3 & the Code \(Clause 1016\)](#)

Clause 3.1 - When third parties (e.g. suppliers, service providers) are used e.g. to **provide, install, configure, integrate, validate, maintain, 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 3.3 - Documentation supplied with commercial off-the-shelf products should be **reviewed by regulated users** to check that user requirements are fulfilled.

Clause 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.

Common Issues

- No agreement in place with vendors, suppliers or service providers (SP's) for applications, hardware and software.
- No documented assessment of suppliers.
- No understanding of the technical services they provide and the impact on their operations.
- Unclear/lack of internal control of suppliers/service providers.
- Lack of understanding of remote system operation & support.
- No periodic review of arrangements with Suppliers/SP's.

3rd Party System Support

Supplier Assessment

- Assess your Supplier (and Record this!)
- Understand their response time.
- Periodically review arrangements and ensure they are appropriate (**and that you still understand them!**).

3rd party agreements

- Work with the Supplier/service provider (and internal IT!) to be clear what is required.
- Understand what the supplier/SP is providing.
- Understand what your IT can/can't perform.
- **Understand/define what you are required to do.**
- Ensure users (and you!) understand how the agreement operates in the operational world.

You paid good money for IT systems.

Understand what you get for that outlay!

3rd Party System Support

Supplier Assessment

- Assess your Supplier (and Record this!)
- Understand their response time.
- Periodically review arrangements and ensure they are appropriate (**and that you still understand them!**).

3rd party agreements

- Work with the Supplier/service provider (and internal IT!) to be clear what is required.
- Understand what the supplier/SP is providing.
- Understand what your IT can/can't perform.
- **Understand/define what you are required to do.**
- Ensure users (and you!) understand how the agreement operates in the operational world.


You paid good money for IT systems.

Understand what you get for that outlay!

Some key questions



- Does your IT Dept understand/have training in GMP? (can they distinguish GMP systems from general systems/applications?)
- Does your IT Dept. understand that changes to infrastructure or operating systems potentially impact GMP applications?
- Does your supplier/service provider understand your requirements, particularly GMP expectations?
- Will your IT Dept. and Supplier/SP notify you of any changes prior to implementation?
- Will providers of remote applications or on-line applications where remote support can be provided, contact you (and get agreement) before any changes are implemented?
- Where general network locations are used to house application data, does your IT Dept. recognise these locations

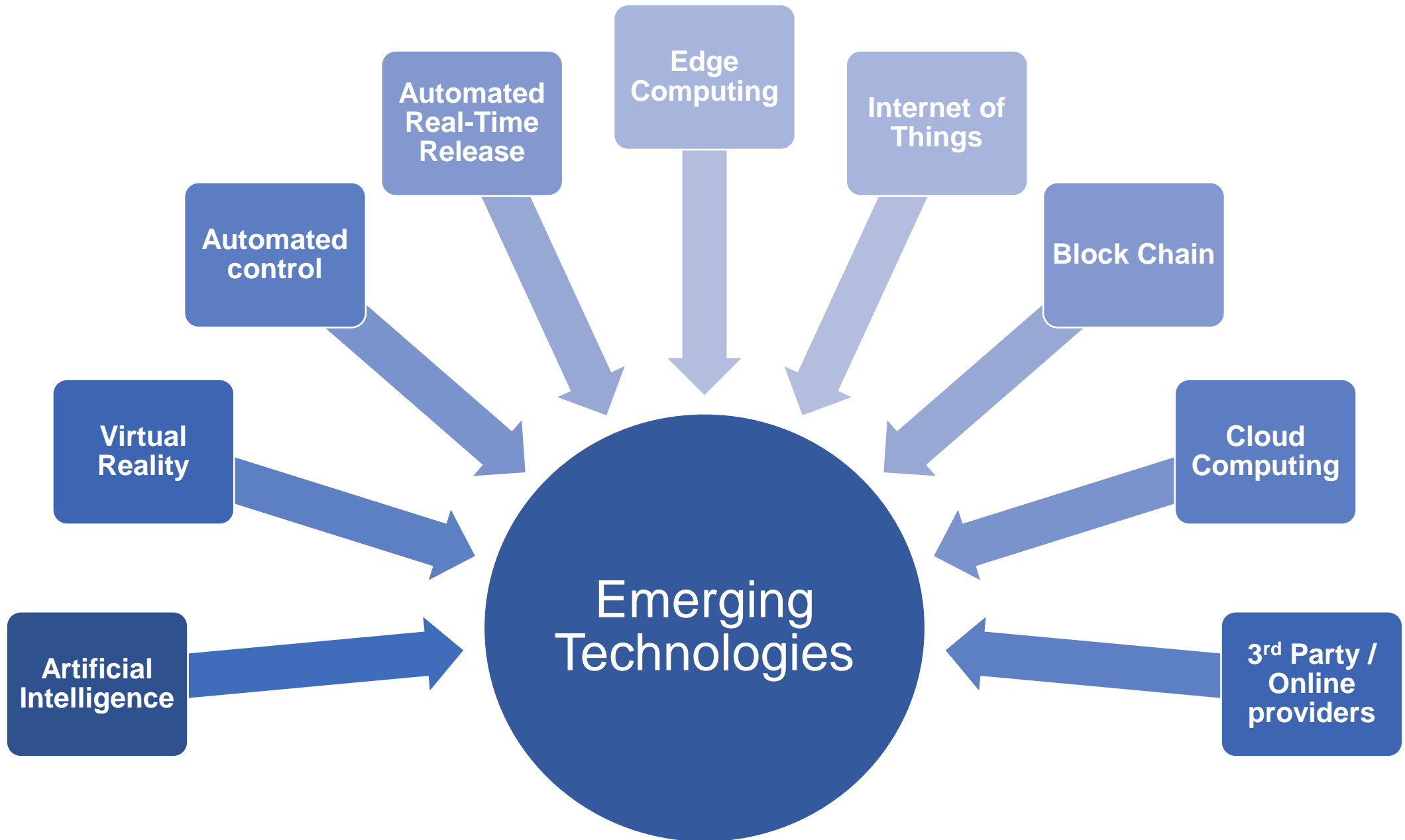


It is important that the manufacturer and the local IT Support, **FULLY** understand the operation of systems, applications and their control, whether the system is a locally installed application, or an on-line cloud based commercial system.

If you don't understand, ask!

Emerging Computerised Technologies





Inspector Observed Developments

Some key observations made:

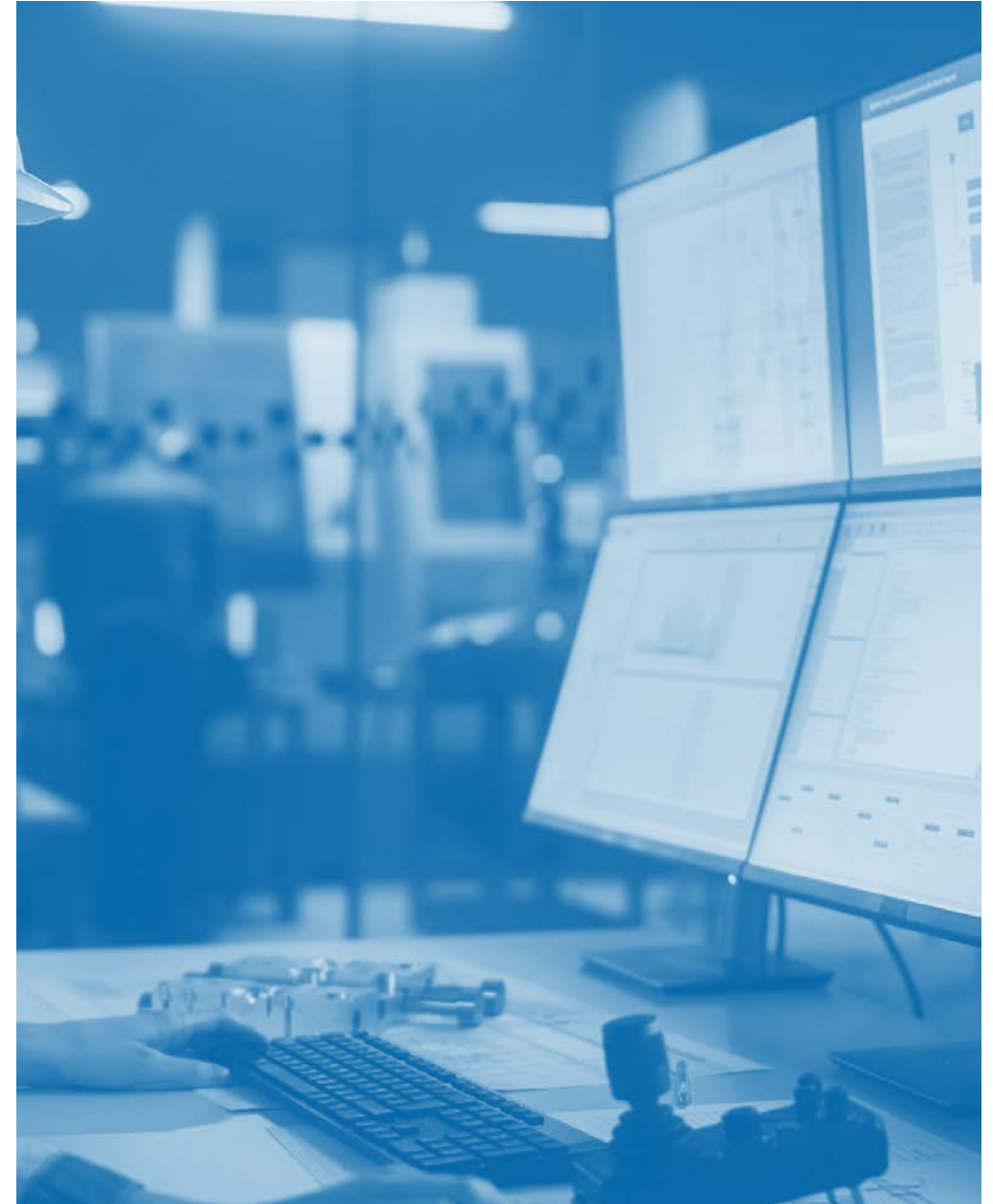
- Pharma industry slow to adopt/implement new technologies
- Nervousness over compliance of new technologies
- Concern with potential impact on product quality/patient
- Concern over robustness, repeatability, control, security, etc.
- Appropriate application of new technologies/downsides
- Training/expertise to support use of new technologies
- How are new technologies validated/implemented in line with existing paradigms
- What are the risks of new technologies and how are they identified and mitigated
- Cost!!!



Existing/grandfathered approaches seem tried and tested!

GxP AI/ML applications seen (or heard of) so far

- Interrogation of deviation/OOS/customer complaint databases for similar issues
- Powder homogeneity using multiple visual sensors
- Microbial colony identification
- Writing concise issue summaries
- Pharmacovigilance monitoring/assessment
- Real-time product release (limited application)
- Data analysis
- Process monitoring using live video
- Automated visual inspection analysis/categorisation



Emerging Technology



Scan the QR code with your device to participate in this activity

Q1. What are manufacturer biggest concerns with application of new technologies?

A. cost | B. regulatory acceptance | C. complexity of systems in regulated environment | D. validation of applications | E. control of systems

Q2. What systems are manufacturers considering/developing?

A. AI for QMS/data analysis | B. automating manufacturing processes | C. Improve system control | D. use virtual reality – training/process monitoring | E. Integrating systems/data

Q.3 What is inhibiting/hindering adoption of emerging technologies?

A. Cost | B. Acceptance | C. IP Security | D. confidence in AI/ML outcomes

Q.4 What technologies do manufacturers expect to be the most widely implemented?

A. Data Analysis | B. real-time process monitoring/release | C. Virtual reality applications | D. non-GMP applications ie. Safety | E. R&D/PAT

So, what is industry considering?

The Inspectorate are keen to understand, discuss, learn what new IT applications are being considered.



EMA | PIC/s Annex 11 – Concept Paper



EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

EMA/PIC/s Concept Paper

Background

- Initiated due to growing disparity and development of new computerised systems and their application
- Follow-on from recent work regarding Data Integrity updates
- Aimed at providing greater guidance
- Intended to include greater clarity on networks, 'Cloud' services and AI/ML
- Also to address increase in 3rd party systems/support, including manufacturers distance from development/control
- Also concurrent with update of Chapter 4 - Documentation



Concept Paper on the revision of Annex 11 of the guidelines on Good Manufacturing Practice for medicinal products – Computerised Systems

Working Group includes members from: Netherlands, Italy, Austria, Switzerland, Germany, Finland, Canada, US, Australia, France

Guidance on Key Questions

	Questions
Software development and system control evolving dramatically i.e.. Agile development	How do you validate and control a diverse and evolving system?
Digital transformation exploding	Can I improve my processes and control by computerisation?
Growing use of online applications	How do you control a system outside your 4 walls?
Global networking the norm with business and manufacturing process support blurred	What are you responsible for at your site and what is corporate/3 rd party IT support responsible for?
Use of the 'Cloud' systems and cloud data management	Where is my applications and data? How do I control them when I don't know where they are?
AI/ML being used in manufacturing at all levels	How do I validate a system that is continually learning?

Have companies kept pace with control of systems, data and management of their use?

No, not from what we see at Inspection!

Instead of this...



Do this!



Current/Future Developments in Annex 11 Update



Questions?



Scan this QR code with your device to submit a question



GMP FORUM 2024



Australian Government

Department of Health and Aged Care
Therapeutic Goods Administration