Annex 11: Computerised Systems

Reasons for changes: The GMP/GDP Inspectors Working Group and the PIC/S Committee jointly recommended that the current version of Annex 11 on Computerised Systems, be revised to reflect changes in regulatory and manufacturing environments. The revised guideline should clarify requirements and expectations from regulatory authorities, and remove ambiguity and inconsistencies.

Document map

Introduction

With an ever-evolving IT landscape, increased use of cloud services, and introduction of new technologies in computerised systems used in GMP activities, there is a growing need for updated guidance on regulatory requirements, and for adopting a common approach between member states of the European Union (EU) and the Pharmaceutical Inspection Co-operation Scheme (PIC/S). The updated Annex 11 outlines the requirements for the use of computerised systems in GMP-regulated activities, thereby ensuring product quality, patient safety and data integrity.

1. Scope

This annex applies to all types of computerised systems used in the manufacturing of medicinal products and active substances.

2. Principles

2.1. *Lifecycle management*. Computerised systems should be validated before use and maintained in a validated state throughout their lifecycle.

2.2. *Quality Risk Management*. Quality Risk Management (QRM) should be applied throughout all lifecycle phases of a computerised system used in GMP activities. The approach should consider the complexity of processes, the level and novelty of automation, and the impact on product quality, patient safety and data integrity.

2.3. *Alternative practices*. Practices which constitute alternatives to the activities required in this document may be used, if they have been proven and documented to provide the same or higher level of control.

2.4. *Data integrity*. It is critically important that data captured, analysed and reported by systems used in GMP activities are trustworthy. As defined by the ALCOA+ principles, data integrity covers many topics including but not limited to requirements defined in the sections Handling of Data, Identity and Access Management, Audit Trails, Electronic Signatures, and Security.

2.5. *System requirements*. System requirements which describe the functionality the regulated user has automated and is relying on when performing GMP activities, should be documented and kept updated to fully reflect the implemented system and its intended use. The requirements should serve as the very basis for system qualification and validation.

2.6. *Outsourced activities*. When using outsourced activities, the regulated user remains fully responsible for adherence to the requirements included in this document, for maintaining the evidence for it, and for providing it for regulatory review.

2.7. *Security*. Regulated users should keep updated about new security threats to GMP systems, and measures to protect these should be implemented and improved in a timely manner, where needed.

2.8. *No risk increase*. Where a computerised system replaces another system or a manual operation, there should be no resultant decrease in product quality, patient safety or data integrity. There should be no increase in the overall risk of the process.

3. Pharmaceutical Quality System

3.1. *Pharmaceutical quality system*. A regulated user should implement a pharmaceutical quality system (PQS), which covers all computerised systems used in GMP activities and personnel involved with these. It should include all activities required in this document and in addition, it should be ensured that:

i. All deviations occurring during validation or operation of computerised systems are recorded and any significant deviations investigated with the objective of determining the root cause and any impact on product quality, patient safety or data integrity. Suitable corrective and preventive actions (CAPA) should be identified and implemented, and the effectiveness of these should be verified.

ii. Any change to a computerised system including but not limited to its configuration, its hardware and software components, and its platform and operating system, are made in a controlled manner and in accordance with defined procedures. Any significant change which may impact product quality, patient safety or data integrity, should be subject to re-qualification and validation.

iii. Internal audits are planned, conducted, reported and followed up on to detect procedural deviations and ensure product quality, patient safety and data integrity.

iv. Regular management reviews cover relevant performance indicators for the computerised system and the process it is used in (quality metrics) and ensure that adequate action is taken.

v. Senior management effectively oversee the state of control throughout the system lifecycle, allocate appropriate resources, and implement a culture that promotes data integrity, security and a timely and effective handling of deviations.

4. Risk Management

4.1. *Lifecycle*. Quality Risk Management (QRM) should be applied throughout the lifecycle of a computerised system considering any possible impact on product quality, patient safety or data integrity.

4.2. *Identification and analysis*. Risks associated with the use of computerised systems in GMP activities should be identified and analysed according to an established procedure. Examples of risk management methods and tools can be found in ICH Q9 (R1).

4.3. *Appropriate validation*. The validation strategy and effort should be determined based on the intended use of the system and potential risks to product quality, patient safety and data integrity.

4.4. *Mitigation*. Where applicable, risks associated with the use of computerised systems in GMP activities should be mitigated and brought down to an acceptable level, if possible, by modifying processes or system design. The outcome of the risk management process should result in the choice of an appropriate computerised system architecture and functionality.

4.5. *Data integrity*. Quality risk management principles should be used to assess the criticality of data to product quality, patient safety and data integrity, the vulnerability of data to deliberate or indeliberate alteration, deletion or loss, and the likelihood of detection of such actions.

5. Personnel and Training

5.1. *Cooperation*. When conducting the activities required in this document, there should be, where applicable, close cooperation between all relevant parties. This includes process owner, system owner, users, subject matter experts (SME), QA, QP, the internal IT department, vendors, and service providers.

5.2. *Training*. All parties involved with computerised systems used in GMP activities should have adequate system specific training, and appropriate qualifications and experience, corresponding to their assigned responsibilities, duties and access privileges.

6. System Requirements

6.1. *GMP functionality*. A regulated user should establish and approve a set of system requirements (e.g. a User Requirements Specification, URS), which accurately describe the functionality the regulated user has automated and is relying on when performing GMP activities. This principle should be applied regardless of whether a system is developed in-house, is a commercial off-the-shelf product, or is provided as-a-service, and independently on whether it is developed following a linear or iterative software development process.

6.2. *Extent and detail*. The extent and detail of defined requirements should be commensurate with the risk, complexity and novelty of a system, and the description should be sufficient to support subsequent risk analysis, specification, design, purchase, configuration, qualification and validation. It should include, but may not be limited to, operational, functional, data integrity, technical, interface, performance, availability, security, and regulatory requirements. Where relevant, requirements should include process maps and data flow diagrams, and use cases may be applied.

6.3. *Ownership*. If a system is purchased or consists of software-as-a-service, a requirements specification may be provided by the vendor. However, the regulated user should carefully review and approve the document and consider whether the system fulfils GMP requirements and company processes as is, or whether it should be configured or customised. The regulated user should take ownership of the document covering the implemented version of the system and formally approve and control it after making any necessary changes.

6.4. *Update*. Requirements should be updated and maintained throughout the lifecycle of a system to ensure that they continue to give a complete and accurate description of system functionality as the system undergoes subsequent changes and customisations. Updated requirements should form the very basis for qualification and validation of a system.

6.5. *Traceability*. Documented traceability between individual requirements, underlaying design specifications and corresponding qualification and validation test cases should be established and maintained. The use of effective tools to capture and hold requirements and facilitate the traceability is encouraged.

6.6. *Configuration*. It should be clear what functionality, if any, is modified or added by configuration of a system. Options allowing configuration of system functionality should be described in the requirements specification and the chosen configuration should be documented in a controlled configuration specification.

7. Supplier and Service Management

7.1. *Responsibility*. When a regulated user is relying on a vendor's qualification of a system used in GMP activities, a service provider, or an internal IT department's qualification and/or operation of such system, this does not change the requirements put forth in this document. The regulated user remains fully responsible for these activities based on the risk they constitute on product quality, patient safety and data integrity.

7.2. *Audit*. When a regulated user is relying on a vendor's or a service provider's qualification and/or operation of a system used in GMP activities, the regulated user should, according to risk and system criticality, conduct an audit or a thorough assessment to determine the adequacy of the vendor or service provider's implemented procedures, the documentation associated with the deliverables, and the potential to leverage these rather than repeating the activities.

7.3. *Oversight*. When a regulated user is relying on a service provider's or an internal IT department's operation of a system used in GMP activities, the regulated user should exercise effective oversight of this according to defined service level agreements (SLA) and key performance indicators (KPI) agreed with the service provider or the internal IT department.

7.4. *Documentation availability*. When a regulated user relies on a vendor's, a service provider's or an internal IT department's qualification and/or operation of a system used in GMP activities, the regulated user should ensure that documentation for activities required in this document is accessible and can be explained from their facility. In this, the regulated user may be supported by the vendor, the service provider or the internal IT department.

7.5. *Contracts*. When a regulated user is relying on a service provider's or an internal IT department's qualification and/or operation of a system used in GMP activities, the regulated user should have a contract with a service provider or have approved procedures with an internal IT department which:

i. Describes the activities and documentation to be provided

ii. Establishes the company procedures and regulatory requirements to be met

iii. Agrees on regular, ad hoc and incident reporting and oversight (incl. SLAs and KPIs), answer times, resolution times, etc.

iv. Agrees on conditions for supplier audits

v. Agrees on support during regulatory inspections, if so requested

vi. Agrees on resolution of issues brought up during normal operation, audits and regulatory inspections etc.

vii. Defines requirements and processes for communication of quality and security related issues

viii. Defines an exit strategy by which the regulated user may retain control of system data

ix. Agrees on the process for release of new system versions and on the regulated user's possibility to test these prior to release.

8. Alarms

8.1. *Reliance on system*. Alarms should be implemented in computerised systems where a regulated user is relying on the system to notify about an event. This is required when the user must take a specific action, without which product quality, patient safety or data integrity might otherwise be compromised.

8.2. *Settings*. Alarm limits, delays, and any early warnings or alerts, should be appropriately justified, and set within approved and validated process and product specifications. Setting, changing or deactivation should only be available to users with appropriate access privileges and should be managed by an approved procedure.

8.3. *Signalling*. Alarms should set off visible and/or audible signals when set alarm limits are exceeded and after any defined delay. The signalling should accommodate a timely reaction and should be appropriate to the work environment.

8.4. *Acknowledgement*. Critical alarms potentially impacting product quality, patient safety or data integrity should only be acknowledged by users with appropriate access privileges. As part of the acknowledgement, i.e. a confirmation that the alarm has been seen and appropriate action will be taken, a comment should be added about why the alarm was acknowledged (see 12 Audit Trails).

8.5. *Log*. All alarms and acknowledgements should be automatically added to an alarm log. This should contain the name of the alarm, date and time of the alarm, date and time of the acknowledgement, username and role of the user acknowledging the alarm and any comment about why the alarm was acknowledged. It should not be possible for users working according to GMP to deactivate or edit alarm logs.

8.6. *Searchability and sortability*. Alarm logs should be searchable and sortable in the originating system, or it should be possible to export logs to a tool which provides this functionality. Other methods of reviewing alarms may also be used, if they provide the same effectiveness.

8.7. *Review*. Alarm logs should be subject to appropriate periodic reviews based on approved procedures, in which it should be evaluated whether they have been timely acknowledged by authorised users and whether appropriate action has been taken. Reviews should be documented, and results should be evaluated to identify any trends that could indicate negative performance of a system or process, or impact on the product. The frequency and detail of reviews should be based on the risk to product quality, patient safety and data integrity.

9. Qualification and Validation

9.1. *Principles*. Qualification and validation activities for computerised systems should follow the general principles outlined in GMP Annex 15. The activities should address both standard and configured system functionality, as well as any functionality realised through customisation.

9.2. *Quality risk management*. Computerised systems should be qualified and validated in accordance with the principles of quality risk management. Decisions on the scope and extent of qualification and validation of specific functionality and entire systems should be based on a justified and documented risk assessment of individual requirements and, where relevant, functional specifications, considering the risk for product quality, patient safety and data integrity.

9.3. *Installation and configuration*. Prior to commencing any test activity, it should be verified that a computerised system and its components have been correctly installed and configured according to specifications, and where applicable, that relevant components have been properly calibrated. Operating systems and platforms should be updated to supported versions and relevant security patches should be deployed (see 15.10 Updated platforms and 15.13 Timely patching).

9.4. *Evidence*. System qualification and validation should provide evidence in the form of executed test scripts, and where relevant, screen dumps, that requirements, and where applicable, derived functional specifications, are met by the system.

9.5. *Traceability*. Test cases should be traceable to individual requirements or specifications, e.g. by means of a requirements traceability matrix. Test cases not referring (traceable) to requirements or applicable specifications do not meet the requirements to qualification and validation.

9.6. *Focus*. Increased focus should be on testing a system's handling of key functional requirements, on functionality intended to ensure that activities are conducted according to GMP, and on functionality designed to ensure data integrity. This includes but is not limited to access privileges, release of products and results, calculations, audit trails, error handling, handling of alarms and warnings, boundary and negative testing, reports and interfaces, and restore from backup.

9.7. *Plan and approval*. Qualification and validation activities should be conducted according to approved plans, protocols and test scripts. Test scripts should be described in sufficient detail to ensure a correct and repeatable conduct of test steps and prerequisites.

9.8. *Completion prior to use*. Qualification and validation activities should be successfully completed and reported prior to approval and taking a system into use. Conditional approval to proceed to taking a system into use may be granted where certain acceptance criteria have not been met, or deviations have not been fully addressed. A condition for this is, that there is a documented assessment, that any deficiencies in the affected system functionality or

GMP processes, will not impact product quality, patient safety or data integrity. Where a conditional approval is issued, it should be explicitly stated in the validation report and there should be close follow-up on approval of outstanding actions according to plan.

9.9. *Authorisation*. Qualification and validation documentation may be provided by a service provider, a vendor or an internal IT department in parts or in whole. However, the regulated user is fully accountable and should carefully review and authorise the use of the documentation. They should carefully consider whether it covers the implemented version and supports GMP, and company processes as is, or whether it should be repeated in parts or completely by the regulated user.

10. Handling of Data

10.1. *Input verification*. Where critical data is entered manually, systems should, were applicable, have functionality to verify the plausibility of the inputs (e.g. within expected ranges), and alert the user when the input is not plausible.

10.2. *Data transfer*. Where a routine work process requires that critical data be transferred from one system to another (e.g. from a laboratory instrument to a LIMS system), this should, where possible, be based on validated interfaces rather than on manual transcriptions. If critical data is transcribed manually, effective measures should be in place to ensure that this does not introduce any risk to data integrity.

10.3. *Data migration*. Where an ad hoc process requires that critical data or a whole database be migrated from one system to another (e.g. when moving data from a retired to a new system), this should be based on a validated process. Among other things, it should consider the constraints on the sending and receiving side.

10.4. *Encryption*. Where applicable, critical data should be encrypted on a system.

11. Identity and Access Management

11.1. *Unique accounts*. All users should have unique and personal accounts. The use of shared accounts except for those limited to read-only access (no data or settings can be changed), constitute a violation of data integrity.

11.2. *Continuous management*. User accesses and roles should be granted, modified and revoked as relevant and in a timely manner as users join, change, and end their involvement in GMP activities.

11.3. *Certain identification*. The method of authentication should identify users with a high degree of certainty and provide an effective protection against unauthorised access. Typically, it may involve a unique username and a password, although other methods providing at least the same level of security may be employed (e.g. biometrics). Authentication only by means of a token or a smart card is not sufficient, if this could be used by another user.

11.4. *Confidential passwords*. Passwords and other means of authentication should be kept confidential and protected from all other users, both at system and at a personal level. Passwords received from e.g. a manager, or a system administrator should be changed at the first login, preferably required by the system.

11.5. *Secure passwords*. Passwords should be secure and enforced by systems. Password rules should be commensurate with risks and consequences of unauthorised changes in systems and data. For critical systems, passwords should be of sufficient length to effectively prevent unauthorised access and contain a combination of uppercase, lowercase, numbers and symbols. A password should not contain e.g. words that can be found in a dictionary, the name of a person, a user id, product or organisation, and should be significantly different from a previous password.

11.6. *Strong authentication*. Remote authentication on critical systems from outside controlled perimeters, should include multifactor authentication (MFA).

11.7. *Auto locking*. Accounts should be automatically locked after a pre-defined number of successive failed authentication attempts. Accounts should only be unlocked by the system administrator after it has been confirmed that this was not part of an unauthorised login attempt or after the risk for such attempt has been removed.

11.8. *Inactivity logout*. Systems should include an automatic inactivity logout, which logs out a user after a defined period of inactivity. The user should not be able to change the inactivity logout time (outside defined and acceptable limits) or deactivate the functionality. Upon inactivity logout, a re-authentication should be required (e.g. password entry).

11.9. *Access log*. Systems should include an access log (separate, or as part of the audit trail) which, for each login, automatically logs the username, user role (if possible, to choose between several roles), the date and time for login, the date and time for logout (incl. inactivity logout). The log should be sortable and searchable, or alternatively, it should be possible to export the log to a tool which provides this functionality.

11.10. *Guiding principles*. Access privileges for users of computerised systems used in GMP activities should be managed according to the following two guiding principles:

- Segregation of duties, i.e. that users who are involved in GMP activities do not have administrative privileges.

- Least privilege principle, i.e. that users do not have higher access privileges than what is necessary for their job function.

11.11. *Recurrent reviews*. User accounts should be subject to recurrent reviews where managers confirm the continued access of their employees in order to detect accesses which should have been changed or revoked during daily operation, but were accidentally forgotten. If user accounts are managed by means of roles, these should be subject to the same kind of reviews, where the accesses of roles are confirmed. The reviews should be documented, and appropriate action taken. The frequency of these reviews should be commensurate with the risks and consequences of changes in systems and data made by unauthorised individuals.

12. Audit Trails

12.1. *Manual user interactions*. Systems which are used to control processes, capture, hold or report data, and where users can create, modify or delete data, settings or access privileges, acknowledge alarms or execute electronic signatures etc., should have an audit trail functionality which automatically logs all manual user interactions.

12.2. *Who, what, when, why*. The audit trail should unambiguously capture the user who made a change (including the user's role, if users may have more than one role), what was changed (including the data that was changed and the old and the new value), and the date and time when the change was made (including the time zone if applicable). Audit trail data should be recorded at the time of events, not at the end of a process. Where data is changed from an old value to a new value, systems should automatically prompt the user for, and register the reason, why the change was made.

12.3. *No edit or deactivation*. Audit trail functionality should be enabled and locked at all times, and it should not be possible for any user to edit audit trail data. If audit trail settings or system time can be changed, or if the functionality can be deactivated, this should by itself create an entry in the audit trail, and it should only be possible for a system administrator not involved in any GMP activities (see 11.10 Guiding principles).

12.4. *Accommodate review*. Systems should accommodate effective and efficient reviews of audit trail data. It should be possible for all users to sort and search audit trail data (who, what, when and why) in the system, or alternatively, to allow export of the data to a tool where this is possible.

12.5. *Reviews*. Audit trail reviews should be conducted according to a documented procedure for the specific system, or type of systems. The procedure should outline who should make the review, what should be reviewed, and when should the review be made. The use of tools to help conduct audit trail reviews is encouraged and appropriate action should be taken and documented following the reviews. Any significant variation from the expected outcome found during the audit trail review should be fully investigated and recorded.

12.6. *Independent review*. Audit trail reviews should be conducted by personnel not directly involved in the activities covered by the review (a peer review).

12.7. *Scope of review*. Reviewing all entries in an audit trail record may not be effective. Reviews should be targeted, based on risk and adapted to local manufacturing processes. Procedures for audit trail reviews should focus on detecting any deliberate or indeliberate changes to critical processes or data that indicate a violation of GMP principles, including, but not limited to, repetition of activities, errors, omissions, unauthorised process deviations and loss of data integrity. A key element should be to verify the reason why a change is made.

12.8. *Timeliness of review*. Audit trail reviews should be conducted in a timely manner according to the risk of the process reviewed. The audit trail review should be conducted prior to batch release, unless the risk of a later detection of any unwarranted changes can be justified.

12.9. *Electronic copy*. It should be possible to obtain a complete electronic copy of system data including audit trail data. Flat and locked files are not acceptable, it should be possible to search and sort data.

12.10. *Availability to QP*. Audit trail reviews with direct impact on the release of a product should be available to the QP at the time of batch release.

13. Electronic Signatures

13.1. *Scope*. Requirements for electronic signatures in this document apply to systems and tools used in processes where GMP require a signature.

13.2. *Open systems*. Where the system owner does not have full control of system accesses (open systems), or where required by other legislation, electronic signatures should, in addition, meet applicable national and international requirements, such as trusted services.

13.3. *Re-authentication*. When executing an electronic signature, a system should enforce users to perform a full re-authentication providing at least the same level of security as during system login (see 11.3 Certain identification). When executing subsequent electronic signatures in immediate sequence, authentication may be by means of a password or biometrics only. Authentication only by means of a smart card, a pin code, or relying on the previous system authentication is not acceptable.

13.4. *Date and time*. Systems should automatically log the date and time and, where applicable, the time zone when an electronic signature was applied.

13.5. *Meaning*. It should be clear when a user is executing an electronic signature and where applicable, systems should prompt the user for the meaning of the signature (e.g. reviewer or approver).

13.6. *Manifestation*. When an electronic signature is displayed (on screen or print), the manifestation should include the full name of the user, the username, where applicable the role of the signer and the meaning of the signature, the date and time, and where needed the time zone, when the signature was applied.

13.7. *Indisputability*. Electronic signatures should be indisputable and equivalent to hand-written signatures.

13.8. *Unbreakable link*. Electronic signatures should be permanently linked to their respective records. Controls should be in place to ensure that a signed record cannot be modified or alternatively, that if a later change is made to a signed record, it will clearly appear as unsigned.

13.9. *Hybrid solution*. If a wet-ink signature (on paper) is used to sign electronic records held in a computerised system (a hybrid solution), measures should be implemented to provide a high degree of certainty that any change to the electronic record will invalidate the signature. This may be implemented by calculating a hash code (check sum) of the electronic record and printing that on the signature page.

14. Periodic Reviews

14.1. *Periodic reviews*. After a system has been initially validated and is put into operation, periodic reviews should be conducted. This review should verify whether the system remains 'fit for intended use' and in 'a validated state', or whether changes should be made and re-validation (complete or in parts) is required. The reviews should be documented and findings analysed to identify any consequences on product quality, patient safety and data integrity, and to prevent recurrence.

14.2. *Scope of review*. Where applicable, periodic reviews should include, but may not be limited to:

Changes made since the previous review:

i. To the system's hardware and software components, configuration, platform, infrastructure and interfaces.

ii. To the system documentation, e.g. requirements specifications, user guides and SOPs. This includes a verification that system changes are fully reflected in the system documentation

iii. The combined effect of multiple changes in this, and in other systems, should be assessed. Undocumented (unapproved) changes should be effectively identified, e.g. by means of configuration auditing.

Follow-up on supporting processes:

iv. Actions from previous periodic reviews, audits and inspections, and corrective and preventive actions.

v. Conduct of, and actions from, audit trail reviews, access reviews, and risks assessments.

vi. Actions from incidents, problems and deviations, security incidents and new security threats.

vii. Maintenance, calibration, support contracts and service level agreements (SLA).

viii. Contracts and key performance indicators (KPI) with vendors and service providers.

ix. Adequacy of backup procedures, restore tests and disaster recovery plans.

x. Adequacy and timeliness of archival.

xi. Conduct and actions from data integrity assessments.

xii. Changes to regulatory requirements.

14.3. *Frequency*. Periodic reviews should be conducted, approved and closed according to plan. The frequency of reviews should be established and justified based on the risk the system poses to product quality, patient safety and data integrity. A final review should be conducted when the system is taken out of use.

15. Security

15.1. *Security system*. Regulated users should ensure an effective information security management system is implemented and maintained, which safeguards authorised access to, and detects and prevents unauthorised access to GMP, systems and data.

15.2. *Continuous improvement*. Regulated users should keep updated about new security threats, and measures to protect GMP systems and data should be continuously improved as applicable to counter this development.

15.3. *Training and tests*. Regulated users should undergo recurrent security awareness training, as relevant, to raise and maintain their understanding of cyber threats and safe behaviour. The effectiveness of the training should be evaluated, e.g. by means of simulated tests.

15.4. *Physical access*. Servers, computers, devices, infrastructure and storage media used in GMP activities should be physically protected against unauthorised access, damage and loss. Physical access to server rooms and data centres should be limited to the necessary minimum and these should be securely locked, e.g. by means of multi-factor authentication. If unauthorised access is possible (e.g. `co-location´), access to individual servers should be protected.

15.5. *Disasters and disturbances*. Data centres should be constructed to minimise the risk and impact of natural and manmade disasters and disturbances. This includes, but may not be limited to, storms, flooding, water leaks, earthquakes, fires, power outages, and network failures etc.

15.6. *Replication*. Where relevant, critical data should be replicated from a primary to a secondary data centre. The replication should take place automatically with a delay which is short enough to minimise the risk of loss of data. The secondary (failover) data centre should be located at a safe distance from the primary site to minimise the risk that the same incident destroys both data centres.

15.7. *Disaster recovery*. A disaster recovery plan should be in place, tested and available during and after a disaster has affected a data centre, server, computer, infrastructure, or data. Where applicable, the plan should ensure the continuity of operation within a defined Recovery Time Objective (RTO).

15.8. *Segmentation and firewalls*. Networks should be segmented, and effective firewalls implemented to provide barriers between networks, and control incoming and outgoing network traffic. Firewall rules (e.g. based on IP addresses, destinations, protocols, applications, or ports) should be defined as strict as practically feasible, only allowing necessary and permissible traffic.

15.9. *Review of firewalls*. Firewall rules should be periodically reviewed as the rules tend to be changed or become insufficient over time (e.g. as ports are opened but never closed, or as new cyber threats evolve). This review should ensure that firewalls continue to be set as tight as possible.

15.10. *Updated platforms*. Operating systems and platforms for applications should be updated in a timely manner according to vendor recommendations, to prevent their use in an unsupported state.

15.11. *Validation and migration*. Validation of applications on updated operating systems and platforms and migration of data should be planned and completed in due time prior to the expiry of the vendor’s support.

15.12. *Unsupported platforms*. Applications on operating systems and platforms, which are no longer supported by vendors, and for which threats are no longer monitored and applicable security patches released, are highly vulnerable and should be isolated from computer networks and the internet.

15.13. *Timely patching*. While operating systems and platforms are under support, vendors typically release security patches to counter identified vulnerabilities, some of which (critical vulnerabilities) could otherwise be exploited to give unauthorised individuals privileged access to systems and allow code execution (e.g. ransomware attacks). Hence, relevant security patches released by vendors of operating systems and platforms should be deployed in a timely manner according to vendor recommendations. For critical vulnerabilities, this might be immediately.

15.14. *Unpatched platforms*. Applications on operating systems and platforms, which are not security patched in a timely manner (critical patches) according to vendor recommendations are highly vulnerable and constitute a major risk for loss of data integrity. Where relevant, such systems should be isolated from computer networks and the internet.

15.15. *Strict control*. The use of bidirectional devices (e.g. USB) in servers and computers used in GMP activities should be strictly controlled within the organisation.

15.16. *Effective scan*. If bidirectional devices (e.g. USB) may have been used outside the organisation (e.g. privately), they may intentionally or unintentionally introduce malware and cause code execution. Hence, they should not be used unless they have been effectively scanned and found to be harmless, and not compromise system and data integrity.

15.17. *Deactivated ports*. Ports for bidirectional devices (e.g. USB) in critical servers and computers should be deactivated by default, blocked or even removed, unless they are used for devices necessary to operate the system (e.g. keyboard or mouse).

15.18. *Anti-virus software*. Anti-virus software should be installed and activated on systems used in GMP activities, especially those interfacing the internet. The anti-virus software should be continuously updated with the most recent virus definitions to identify, quarantine, and remove known computer viruses. The effectiveness of the process should be monitored.

15.19. *Penetration testing*. For critical systems facing the internet, penetration testing (ethical hacking) should be performed at regular intervals to evaluate the adequacy of security measures taken, and to identify vulnerabilities in system security. This should include the potential for unauthorised parties to gain access to and control the system and its data. The effectiveness of the process should be verified and monitored. Vulnerabilities identified, especially those related to a potential loss of data integrity, should be addressed and mitigated in a timely manner.

15.20. *Encryption*. When remotely connecting to systems over the internet, a secure and encrypted protocol should be used.

16. Backup

16.1. *Regular backup*. Data and metadata should be regularly backed up following established procedures to prevent the loss of data in case of accidental or deliberate change or deletion, loss as the result of a malfunction or corruption, e.g. as the result of a cyber-attack.

16.2. *Frequency and retention*. The frequency, retention period and storage of backups is critically important to the effectiveness of the process to mitigate the loss of data. Backups should be made at suitable intervals (e.g. hourly, daily, weekly and monthly) and their retention determined through a risk-based approach (e.g. correspondingly a week, a month, a quarter, and years).

16.3. *Physical separation*. Backups should be physically separated from the server or computer holding the original data and stored at a safe distance from this, to prevent that both would be impacted by the same incident.

16.4. *Logical separation*. Backups should not be stored at the same logical network as the original data to avoid simultaneous destruction or alteration.

16.5. *Scope*. Depending on the criticality and urgency for recovery after an incident, applications and system configurations may also need to be backed up.

16.6. *Restore test*. Restore of data from backup should be tested and documented based on risk during system validation and after changes are made to the backup or restore processes and tools. Restore tests should be documented and include a verification that data is accessible on the system.

17. Archiving

17.1. *Read only*. After completion of a process, e.g. release of a product, GMP data and metadata (incl. audit trails) should be protected from deletion and changes throughout the retention period. This may be by changing its status to read-only in the system where the data was generated or captured, or by moving it to a dedicated archival system via a validated interface.

17.2. *Verification*. When moving GMP data and metadata from one location to another in a system, or to a dedicated archival system, the integrity of the data should be verified by a high degree of certainty before any data is deleted, e.g. by means of a checksum. Where this is not possible, the completeness and integrity of the data should be verified manually. However, this verification does not alter the need for a validation of the archival and retrieval process, and of the systems and interfaces involved.

17.3. *Backup*. If data is archived on a server (disk), it should be regularly backed up following the same procedures as for live data (see 16 Backup). As for other backups, these should be physically and logically separated from the archived data.

17.4. *Durability*. If data is archived long-term on volatile storage media with limited durability (e.g. CD), this should follow a validated process. It should ensure that data is stored only for a verified duration according to vendor recommendations, and if necessary, transferred to new media in secure manner (see 16 Backup).

17.5. *Retrieval*. It should be possible to retrieve archived data and metadata in a format which allows searching and sorting of the data, or alternatively, to allow export of the data to a tool where this is possible.

Glossary

ALCOA+

An acronym for "attributable, legible, contemporaneous, original and accurate", which puts additional emphasis on the attributes of being complete, consistent, enduring and available – implicit basic ALCOA principles.

Application

Software installed on a defined platform/hardware providing specific functionality.

Audit trail

In computerised systems, an audit trail is a secure, computer generated, time-stamped electronic record that allows reconstruction of the events relating to the creation, modification, or deletion of an electronic record.

Backup

Provisions made for the recovery of data files or software, for the restart of processing, or for the use of alternative computer equipment after a system failure or disaster.

Change control

Ongoing evaluation and documentation of system operations and changes to determine whether the actual changes might affect a validated status of the computerised system. The intent is to determine the need for action that would ensure that the system is maintained in a validated state.

Commercial off-the-shelf

Software or hardware is a commercial off-the-shelf (COTS) product if provided by a vendor to the general public, if available in multiple and identical copies, and if implemented by the test facility management without or with some customization.

Computerised System

A computerised system is a function (process or operation) integrated with a computer system and performed by trained personnel. The function is controlled by the computer system. The controlling computer system is comprised of hardware and software. The controlled function is comprised of equipment to be controlled and operating procedures performed by personnel.

Configuration

A configuration is an arrangement of functional units and pertains to the choice of hardware, software and documentation. It affects function and performance of the system.

Customisation

A computerised system individually designed to suit a specific business process.

Electronic record

Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Infrastructure

The hardware and software such as networking software and operation systems, which makes it possible for the application to function.

Migration

Data migration is the activity of e.g. transporting electronic data from one computer system to another, transferring data between storage media or simply the transition of data from one state to another [e.g. conversion of data to a different format]. The term “data” refers to “raw data” as well as “metadata”.

Multifactor authentication (MFA)

A combination of two of the three factors: something you know (e.g. a password), something you have (e.g. a phone or smartcard) or something you are (biometrics).

Operating system

A program or collection of programs, routines and sub-routines that controls the operation of a computer. An operating system may provide services such as resource allocation, scheduling, input/output control, and data management.

Qualification

Action of verifying that the system (including hardware and software) is effectively designed, installed, commissioned, and operates correctly. Refer to Computer system Validation

Regulated user

A company regulated under GMP.

Specification

A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behaviour, or other characteristics of a system or component, and often, the procedures for determining whether these provisions have been satisfied.

Test case

A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement.

User

An individual user at a company regulated under GMP.

User requirement specifications (URS)

User requirement specifications define in writing what the user expects the computerised system to be able to do.

Validation

Action of proving that a process leads to the expected results. Validation of a computerised system requires ensuring and demonstrating the fitness for its purpose.

Verification

Confirmation, through the provision of objective evidence that specified requirements have been fulfilled.