Afternoon Meeting for ITQA
Validation and operation of IT systems in GxP
30 November 2023 at 14.30-17.00
Ib Alstrup, Medicines Inspector GxP IT, DKMA

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

Program

- Introduction
- Audit trail and audit trail review
- Example from Novo Nordisk
- User review
- Pause
- Backup
- Example from Novo Nordisk
- Cloud computing
- IT security
- Networking (until 17:00)

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

Why a meeting with ITQA?

- Approve
- Responsibility
- Relationship
- Ambassadors?
- Not a discussion of the Annex 11 Concept Paper

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

Regulatory Requirements within the different GxPs

To qualification and safe operation of IT systems

Design, validation and safe operation of IT systems is described in very different detail:

GLP: OECD#17 (CS) 32p | OECD#22 (DI) 30p | OECD#17[1] (Cloud) 31p | IT Sec (draft)
GCP: EMA GCP eGuidance 52p | ICH GCP E6 R2 1p (in revision)
GMP: GMP Annex 11 4.5 p (in revision)
GVP: EU GVP ~0.5p

- No objective reasons why expectations and level of guidance should be so different.
- The more detailed regulatory requirements are, the less we have to interpret.
- The opposite is also true.

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

OECD GLP no. 17 on Computerised Systems

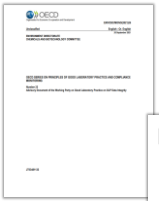
Published April 2016

https://one.oecd.org/document/env/jm/mono(2016)13/en/pdf

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

OECD GLP no. 22: GLP Data Integrity

Published September 2021

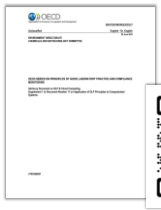


https://one.oecd.org/document/env/cbc/mono(2021)26/en/pdf

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

OECD GLP no. 17 supplement 1: Cloud Computing

Published June 2023



https://one.oecd.org/document/ENV/CBC/MONO(2023)27/en/pdf

EU and PIC/S GMP Annex 11 Concept Paper

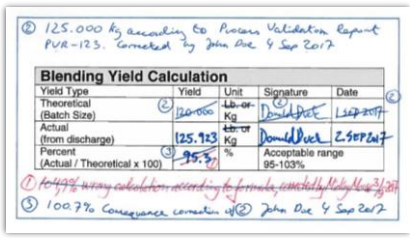
Published November 2022

- Drafted by GMP inspectors from EU and PIC/S countries
- Contains 33 proposed specific changes and new additions
- Approved by the EMA GMP IWG and PIC/S
- Constitutes an outline for the revision of Annex 11
- Public consultation from November 2022 to January 2023
- Approx. 567 comments received (now under review)

https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/concept-paper-revision-annex-11-guidelines-good-manufacturing-practice-medicinal-products_en.pdf

Audit Trail

A Batch Record (example)



① 125.000 kg according to Process Validation Report PVR-123. Corrected by John Doe 4 Sep 2017

Blending Yield Calculation

Yield Type	Yield	Unit	Signature	Date
Theoretical (Batch Size) ②	120.000	~~Lb. or~~ Kg	Donald Duck	1 SEP 2017
Actual (from discharge)	125.923	~~Lb. or~~ Kg	Donald Duck	2 SEP 2017
Percent (Actual / Theoretical x 100) ③	95.5	%	Acceptable range 95-103%	

④ 104.9% wrong calculation according to formula, corrected by John Doe 3/9 2017

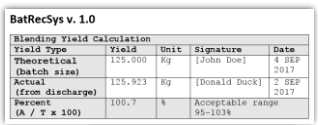
⑤ 100.7% Consequence correction of ② John Doe 4 Sep 2017

- Good old paper
- GxP corrections
- Good Documentation Practice

A Batch Record

Three representations

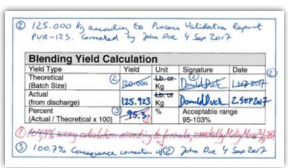
Which one do you prefer?



BatRecSys v. 1.0

Blending Yield Calculation

Yield Type	Yield	Unit	Signature	Date
Theoretical (batch size)	125.000	Kg	[John Doe]	4 SEP 2017
Actual (from discharge)	125.923	Kg	[Donald Duck]	2 SEP 2017
Percent (A / T x 100)	100.7	%	Acceptable range 95-103%	



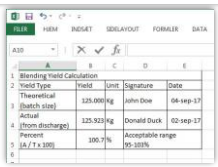
① 125.000 kg according to Process Validation Report PVR-123. Corrected by John Doe 4 Sep 2017

Blending Yield Calculation

Yield Type	Yield	Unit	Signature	Date
Theoretical (Batch Size) ②	120.000	~~Lb. or~~ Kg	Donald Duck	1 SEP 2017
Actual (from discharge)	125.923	~~Lb. or~~ Kg	Donald Duck	2 SEP 2017
Percent (Actual / Theoretical x 100) ③	95.5	%	Acceptable range 95-103%	

④ 104.9% wrong calculation according to formula, corrected by John Doe 3/9 2017

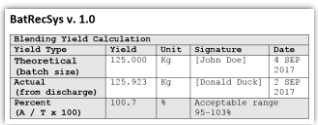
⑤ 100.7% Consequence correction of ② John Doe 4 Sep 2017



	A	B	C	D	E
1	Blending Yield Calculation				
2	Yield Type	Yield	Unit	Signature	Date
3	Theoretical (batch size)	125.000	Kg	John Doe	04-sep-17
4	Actual (from discharge)	125.923	Kg	Donald Duck	02-sep-17
5	Percent (A / T x 100)	100.7 %		Acceptable range 95-103%	

A Batch Record

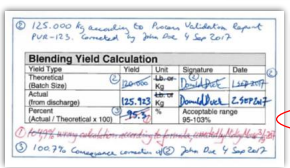
Why should we accept the electronic version?



BatRecSys v. 1.0

Blending Yield Calculation

Yield Type	Yield	Unit	Signature	Date
Theoretical (batch size)	125.000	Kg	[John Doe]	4 SEP 2017
Actual (from discharge)	125.923	Kg	[Donald Duck]	2 SEP 2017
Percent (A / T x 100)	100.7	%	Acceptable range 95-103%	



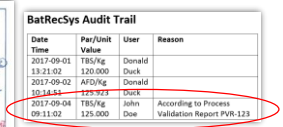
① 125.000 kg according to Process Validation Report PVR-123. Corrected by John Doe 4 Sep 2017

Blending Yield Calculation

Yield Type	Yield	Unit	Signature	Date
Theoretical (Batch Size) ②	120.000	~~Lb. or~~ Kg	Donald Duck	1 SEP 2017
Actual (from discharge)	125.923	~~Lb. or~~ Kg	Donald Duck	2 SEP 2017
Percent (Actual / Theoretical x 100) ③	95.5	%	Acceptable range 95-103%	

④ 104.9% wrong calculation according to formula, corrected by John Doe 3/9 2017

⑤ 100.7% Consequence correction of ② John Doe 4 Sep 2017

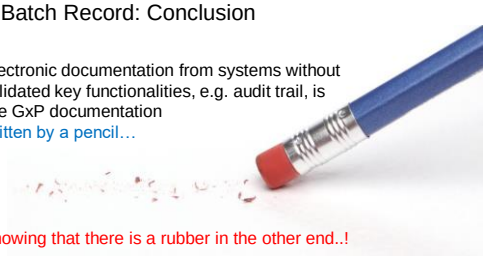


BatRecSys Audit Trail

Date Time	Par/Unit Value	User	Reason
2017-09-01 13:21:02	TBS/Kg 120.000	Donald Duck	
2017-09-02 10:14:51	AFD/Kg 125.923	Donald Duck	
2017-09-04 09:11:02	TBS/Kg 125.000	John Doe	According to Process Validation Report PVR-123

A Batch Record: Conclusion

Electronic documentation from systems without validated key functionalities, e.g. audit trail, is like GxP documentation
written by a pencil…



knowing that that there is a rubber in the other end..!

Audit trail (19)

GLP: OECD GLP doc. no. 17 on Computerised Systems (2016)

"80. An audit trail provides documentary evidence of activities that have affected the content or meaning of a record at a specific time point. Audit trails need to be available and convertible to a human readable form. […] Any change to electronic records must not obscure the original entry and be time and date stamped and traceable to the person who made the change."

"81. Audit trail for a computerised system should be enabled, appropriately configured and reflect the roles and responsibilities of study personnel. The ability to make modifications to the audit trail settings should be restricted to authorised personnel. Any personnel involved in a study (e.g. study directors, heads of analytical departments, analysts, etc.) should not be authorised to change audit trail settings."

"83. The system should be able to highlight alterations made to previously entered data both on the screen and in any printed copies. The original and modified entries should be retained by the system. […]"

Audit trail (42)

GLP: OECD GLP doc. no. 22 on Data Integrity (2021)

"The audit trail is a form of metadata that contains information associated with actions that relate to the creation, modification or deletion of electronic data. An audit trail provides an automated secure way of recording life cycle details such as creation, additions, deletions or alterations of information in an electronic record without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record, including the 'who, what, when and why' of the action."

"Computerised system design should always provide for the retention of full audit trails to show all changes to the data without obscuring the original record. It should be possible to associate all changes to data with the person having made those changes and the date they were made, for example, by use of a data audit trail or equivalent mechanisms, or timed and dated (electronic) signatures. Reason for changes must be given."

Audit trail (42)

GLP: OECD GLP doc. no. 22 on Data Integrity (2021)

Where computerised systems are used to capture, process, modify, report, store or archive data electronically, system design should always provide for the retention of audit trails to show all changes to, or deletion of the data while retaining previous data. It should be possible to associate all data and changes to data with the persons making those changes, and changes should be dated and time stamped (time and including, where applicable, the time zone). The reason for the change should also be recorded. The items included in the audit trail should be those of relevance to permit reconstruction of the process or activity.

Audit trails should always be switched on during GLP activities. Any personnel with a direct interest in the data (study directors, heads of analytical departments, study personnel etc.) should not have the ability to amend or switch off the audit trail functionality. Where a system administrator amends or switches off the audit trail functionality, the audit trail should record this automatically and it should also be recorded automatically when the audit trail functionality is switched on again.

Audit trail (62)

GCP: Guideline on Computerised System and Electronic Data (2023)

"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."

"Electronic source data, including the audit trail should be directly accessible by investigators, monitors, auditors, and inspectors […]"

"An audit trail is essential to ensure that changes to the data are traceable. Audit trails should be robust, and it should not be possible for 'normal' users to deactivate them. If possible, for an audit trail to be deactivated by 'admin users', this should automatically create an entry into a log file (e.g. audit trail). Entries in the audit trail should be protected against change, deletion, and access modification (e.g. edit rights, visibility rights). The audit trail should be stored within the system itself. The responsible investigator, sponsor, and inspector should be able to review and comprehend the audit trail and therefore audit trails should be in a human-readable format."

Audit trail (62)

GCP: Guideline on Computerised system and electronic data (2023)

Audit trails should be visible at data-point level in the live system, and it should be possible to export the entire audit trail as a dynamic data file to allow for the identification of systematic patterns or concerns in data across trial participants, sites, etc. The audit trail should show the initial entry and the changes (value - previous and current) specifying what was changed (field, data identifiers) by whom (username, role, organisation), when (date/timestamp) and, where applicable, why (reason for change).

[…]

Audit trails should capture any changes in data entry per field and not per page (e.g. eCRF page).

[…]

Audit trail

EU & PIC/S GMP Annex 11 (2011)

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.

Audit trail

EU & PIC/S GMP Annex 11 Concept Paper (2022)

17. [8] The section should include an expectation to be able to obtain data in electronic format including the complete audit trail. The requirement to be able to print data may be reconsidered.

18. [9] An audit trail functionality which automatically logs all manual interactions on GMP critical systems, where users, data or settings can be manually changed, should be regarded as mandatory; not just 'considered based on a risk assessment'. Controlling processes or capturing, holding or transferring electronic data in such systems without audit trail functionality is not acceptable; any grace period within this area has long expired.

19. [9] The audit trail should positively identify the user who made a change, it should give a full account of what was changed, i.e. both the new and all old values should be clearly visible, it should include the full time and date when the change was made, and for all other changes except where a value is entered in an empty field or where this is completely obvious, the user should be prompted for the reason or rationale for why the change was made.

Audit trail

EU & PIC/S GMP Annex 11 Concept Paper (2022)

20. [9] It should not be possible to edit audit trail data or to deactivate the audit trail functionality for normal or privileged users working on the system. If these functionalities are available, they should only be accessible for system administrators who should not be involved in GMP production or in day-to-day work on the system (see 'segregation of duties').

23. [9] Audit trail functionalities should capture data entries with sufficient detail and in true time, in order to give a full and accurate picture of events. If e.g. a system notifies a regulated user of inconsistencies in a data input, by writing an error message, and the user subsequently changes the input, which makes the notification disappear; the full set of events should be captured.

24. [9] It should be addressed that many systems generate a vast amount of alarms and event data and that these are often mixed up with audit trail entries. While alarms and events may require their own logs, acknowledgements and reviews, this should not be confused with an audit trail review of manual system interactions. Hence, as a minimum, it should be possible to be able to sort these.

Audit Trail Review

Audit trail review

GLP: OECD GLP doc. no. 17 on Computerised Systems (2016)

A system should be in place that can ensures a risk based review of the audit trail functions, its settings and the recorded information. The test facility management may consider, but should not be limited to, individual events (e.g. user behavior, suspected data integrity issues) to review the audit trail records. Completeness and suitability of the audit trail functions and settings may be considered. GLP quality assurance personnel should be involved. A review of the audit trail functions should be based upon an understanding of the use of the system, the ability to modify the record and the controls preventing malicious alterations of the records.

Audit trail review (2)

GLP: OECD GLP doc. no. 22 on Data Integrity (2021)

It is not necessary for audit trail review to include every system activity.

The relevant data among all the retained data in audit trails should be identified to permit robust data review/verification. The review should be conducted according to a documented risk-based process identifying the criticality of the data subject to the review and the criticality of transactions identified through the data flow. The review may be achieved by direct access to the system audit trail or by use of appropriately designed and validated system reports.

Reviewers should have sufficient knowledge and system access to review relevant audit trails, raw data and metadata.

Audit trail review (7)

GCP: Guideline on Computerised system and electronic data (2023)

Procedures for risk-based trial specific audit trail reviews should be in place and performance of data review should be generally documented.

Audit trail review can also be used to detect situations where direct data capture has been defined in the protocol but where this is not taking place as described.

In addition to audit trail review, metadata review could also include (among others) review of access logs, event logs, queries, etc.

The investigator should receive an introduction on how to navigate the audit trail of their own data in order to be able to review changes.

Audit trail review

GMP: EU & PIC/S GMP Annex 11 (2011)

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.

Audit trail review

GMP: EU & PIC/S GMP Annex 11 Concept Paper (2022)

21. [9] The concept and purpose of audit trail review is inadequately described. The process should focus on a review of the integrity of manual changes made on a system, e.g. a verification of the reason for changes and whether changes have been made on unusual dates, hours and by unusual users.

22. [9] Guidelines for acceptable frequency of audit trail review should be provided. For audit trails on critical parameters, e.g. setting of alarms in a BMS systems giving alarms on differential pressure in connection with aseptic filling, audit trail reviews should be part of batch release, following a risk-based approach.

Summary on AT and ATR

Audit Trail and Audit Trail Review - Expectations

- Automatically records who (incl. role), what, when, for manual entries, changes and deletions
- Prompts and records why a change was made, except where the reason is obvious
- Recorded in true time, not at end of process; change after critical info is aggravating factor
- Non-editable for normal users, and preferably, for privileged users
- Not possible to deactivate, at least for normal users; deactivation should create entry
- Possible to create electronic dynamic copy, e.g. during regulatory inspection
- Searchable, e.g. user, activity, parameter, value, date and time interval, reason
- Sortable, e.g. to block out alarms, events and other non-audit trail information
- Exportable to spreadsheet, in lack of proper built-in search and sort functionality
- Readable and understandable for normal users, auditors and inspectors
- New and all previous values must be clearly visible
- Reviewable, accommodating an efficient audit trail review
- A procedure for audit trail reviews should exist, incl. what to review, when and by whom
- Reviewed according to the procedure and appropriate actions taken
- Included in backup, restore and archival procedures

Audit Trail Review

In GMP

Who should review:

- An independent (second) person

What to look for (only examples):

- Changes in status from on-hold or quarantined to approved (think like a detective)
- Changes made after user obtained critical information, e.g. OOS
- Changes made after normal working hours or by unexpected users
- Changes handled by only one person, if two or more would be expected

When to review:

- No later than batch release for systems with direct product impact

Qualifying the Audit Trail Functionality
Often seen mistakes

A test case typically includes a set of preceding activities and ends with producing a screen shot of the Audit Trail, but very often, test cases are not proving the required functionality because

- The AT data* in the screen shot cannot be verified by previous test steps
- The screen shot is not readable, or in lack of a screen shot (not recommended), the tester has not verified that AT data* seen in previous test steps, have correctly been recorded

*) AT data: who, what, when and why

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

Audit trail & Audit trail review

The Novo Nordisk approach

Kristian Alkjærsig
KAL@NOVONORDISK.COM

Audit trail and review – selected QA focus areas

When/what/how
The basics:
Does the audit trail capture what it should and when it should?

Coverage
Does the audit trail capture changes for all relevant data/situations?

Review
Is the relevant review of the audit trail performed?

Audit trail and review – selected QA focus areas

When/what/how
The basics:
Does the audit trail capture what it should and when it should?

Coverage
Does the audit trail capture changes for all relevant data/situations?

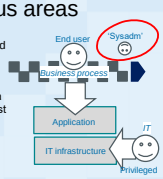
Review
Is the relevant review of the audit trail performed?

Audit trail and review – selected QA focus areas

When/what/how
The basics:
Does the audit trail capture what it should and when it should?

- **When**: Audit trail to capture change whenever end users are able to create, modify or delete GxP data via the user/application interface.

For 'privileged users': Changes to data managed via change control, training, 'segregation of duties', 'least privilege' principle and low # of users.



- **What**: Contents of audit trail entries:
  - *who* performed the entry or action,
  - *when* it took place,
  - *what* was created/modified/deleted,
  - *why* (reason for change), where
    - required by GxP regulations, or
    - important to the process, but not obvious from the context
- **How:** Verify correct contents, readability, availability and useability in business process

Audit trail and review – selected QA focus areas

When/what/how
The basics:
Does the audit trail capture what it should and when it should?

Coverage
Does the audit trail capture changes for all relevant data/situations?

Review
Is the relevant review of the audit trail performed?

Audit trail and review – selected QA focus areas

Coverage

Does the audit trail capture changes for all relevant data/situations?

What are the relevant data?

Data used for GxP regulated processes includes data required by relevant regulations, data that supports GxP decisions, and data necessary to reconstruct GxP activities.

And what are the relevant situations?

Business process

GxP related events (data audit trail):

- *Changed data (including deletions)*
- *Signs of abnormal data/activities*
- *Omitted data ('orphan' data)*

Collaboration and agreement

Segregation of duties

IT

System related events (event/system logs):

- *Audit trail configuration changes (incl. deactivation)*
- *IT security events*
- *System failure states potentially impacting data*

Audit trail and review – selected QA focus areas

When/what/how

The basics: Does the audit trail capture what it should and when it should?

Coverage

Does the audit trail capture changes for all relevant data/situations?

Review

Is the relevant review of the audit trail performed?

Audit trail and review – selected QA focus areas

Review approach

Is the relevant review of the audit trail performed?

1. Routine review

A routine review within the approval process. **This is the regular way of handling ATR**

2. Periodic review

Review with a defined frequency, e.g. every week or every 3 months

3. 'As-needed'

A review process on an as-needed basis, e.g. in connection with a deviation, CAPA

Not performing ATR at all is not an option! Review on an 'as-needed basis' for data of low criticality

*This could be a combination of 1) and 2), i.e. **BOTH** an ATR as part of batch release or approval of analysis **AND** a periodic review of data generated between batches/analytical runs*

Main principle: Review the audit trails together with the rest of the data/records. The decision on review frequencies must be risk-based and compliant with external requirements.

SOP

novo nordisk®

User review

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

User review

Guideline on GVP: Module I – PV Systems and Quality Systems (2012)

"As part of a record management system, specific measures should therefore be taken at each stage in the storage and processing of pharmacovigilance data to ensure data security and confidentiality. This should involve strict limitation of access to documents and to databases to authorised personnel respecting the medical and administrative confidentiality of the data."

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

User review

GCP: Guideline on Computerised system and electronic data (2023)

"Checks should be used to ensure that only authorised individuals have access to the system and that they are granted appropriate permissions (e.g. ability to enter or make changes to data). Records of authorisation of access to the systems, with the respective levels of access clearly documented, should be maintained."

"The responsible party should maintain a security system that prevents unauthorised access to the data."

"At any given time, an overview of current and previous access, roles and permissions should be available from the system. This information concerning actual users and their privileges to systems should be verified at suitable intervals to ensure that only necessary and approved users have access and that their roles and permissions are appropriate. There should be timely removal of access no longer required, or no longer permitted."

User review (2)

GMP: EU & PIC/S GMP Annex 11 (2011)

"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."

"Creation, change, and cancellation of access authorisations should be recorded."

User review

GMP: EU & PIC/S GMP Annex 11 Concept Paper (2022)

30. [12.3] The current version says that "Creation, change, and cancellation of access authorisations should be recorded". However, it is necessary to go further than just recording who has access to a system. Systems accesses and roles should be continually managed as people assume and leave positions. System accesses and roles should be subject to recurrent reviews in order to ensure that forgotten and undesired accesses are removed.

User review

Typical findings

- This is one of the activities which most often is misunderstood (like e.g. reviewing that users who have been authorised by managers also have access)
- Review does not cover all users
- Review does not verify correct setup of roles

Backup

Backup

Guideline on GVP: Module I – PV Systems and Quality Systems (2012)

"During the retention period, retrievability of the documents should be ensured. Documents can be retained in electronic format, provided that the electronic system has been appropriately validated and appropriate arrangements exist for system security, access and back-up of data."

Backup

GCP: Guideline on Computerised system and electronic data (2023)

"Data and configurations should be regularly backed up."

"Backups should be stored in separate physical locations and logical networks and not behind the same firewall as the original data to avoid simultaneous destruction or alteration."

"Frequency of backups (e.g. hourly, daily, weekly) and their retention (e.g. a day, a week, a month) should be determined through a risk-based approach."

"Checks of accessibility to data, irrespective of format, including relevant metadata, should be undertaken to confirm that the data are enduring, continue to be available, readable and understandable by a human being. There should be procedures in place for risk-based (e.g. in connection with major updates) restore tests from the backup of the complete database(s) and configurations and the performed restore tests should be documented."

"Disaster mitigation and recovery plans should be in place to deal with events that endanger data security. Such plans should be regularly reviewed. Disaster mitigation and recovery plans should be part of the contractual agreement, if applicable."

Backup (2)

GMP: EU & PIC/S GMP Annex 11 (2011)

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.

Backup

GMP: EU & PIC/S GMP Annex 11 Concept Paper (2022)

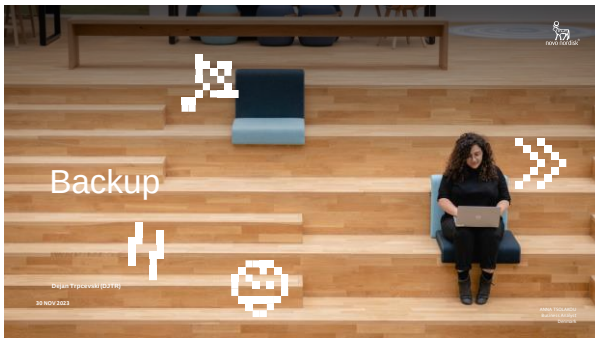
15. [7.2] Testing of the ability to restore system data (and if not otherwise easily recreated, the system itself) from backup is critically important, but the required periodic check of this ability, even if no changes have been made to the backup or restore processes, is not regarded necessary. Long-term backup (or archival) to volatile media should be based on a validated procedure (e.g. through 'accelerated testing'). In this case, testing should not focus on whether a backup is still readable, but rather, validating that it will be readable for a given period.

16. [7.2] Important expectations to backup processes are missing, e.g. to what is covered by a backup (e.g. data only or data and application), what types of backups are made (e.g. incremental or complete), how often backups are made (all types), how long backups are retained, which media is used for backups, and where backups are kept (e.g. physical separation).

Backup

Typical findings

- In majority of cases, organisation are not able to prove that they ever tested to restore complete system data from backup
- Retention of backups seen as low a 7 days
- Backups not physically or logically separated from system
- As a result, data have been seen to have been lost



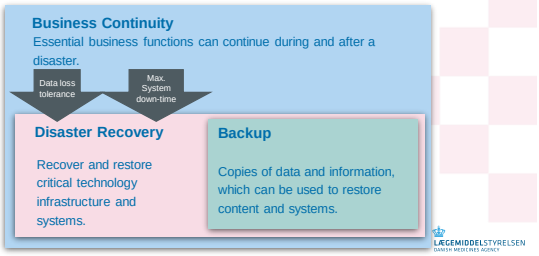
Annex 11

Backup

Good IT Practices

ITIL, NIST, PCI DSS, HIPAA, COBIT, ISO/IEC 20000, ISO/IEC 27001, 27002, …

Novo Nordisk IT Process



Common Vulnerabilities

Un-defined retention of backup	Lack of recovery plan	Not testing the backup	Not protecting The backup	Confusing Archiving and Backup
How long are you keeping the backups before they are recycled? Why?	Do you know how to use the backups in case a disaster strikes? When did you last rehearse your plan?	Have you checked that the backup data is usable? Does it contain the expected records?	Where are the backups located? Who has access to them? Are they encrypted?	How can we archive and preserve data from this system?

Take aways

- Apply Good IT Practices, then compliance with Annex 11 will follow.
- Requirements to backup should follow from business requirements.
- Don't underestimate the complexity of the backup process.

novo nordisk®

Cloud computing

LÆGEMIDDELSTYRELSEN
DANISH MEDICINES AGENCY

Cloud computing

GCP: Guideline on Computerised system and electronic data (2023)

"Irrespective whether a computerised system is installed at the premises of the sponsor, investigator, another party involved in the trial or whether it is made available by a service provider as a cloud solution, the requirements in this guideline are applicable."

Cloud computing

GMP: EU & PIC/S GMP Annex 11 (2011)

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.

Cloud Computing

GMP: EU & PIC/S GMP Annex 11 Concept Paper (2022)

6. [3.1] The list of services should include to 'operate' a computerised system, e.g. 'cloud' services.

7. [3.1] For critical systems validated and/or operated by service providers (e.g. 'cloud' services), expectations should go beyond that "formal agreements must exist". Regulated users should have access to the complete documentation for validation and safe operation of a system and be able to present this during regulatory inspections, e.g. with the help of the service provider. See also Notice to sponsors and Q&A #9 on the EMA GCP website and Q&A on the EMA GVP website)

IT Security

IT Security (spec. Vulnerability Management)

Guideline on GVP: Module I – PV Systems and Quality Systems (2012)

"During the retention period, retrievability of the documents should be ensured. Documents can be retained in electronic format, provided that the electronic system has been appropriately validated and appropriate arrangements exist for system security, access and back-up of data."

IT Security (spec. Vulnerability Management)

GCP: Guideline on Computerised system and electronic data (2023)

Vulnerabilities in computer systems can be exploited to perform unauthorised actions, such as modifying data or making data inaccessible to legitimate users. Such exploitations could occur in operating systems for servers, computer clients, tablets and mobile phones, routers and platforms (e.g. databases). Consequently, relevant security patches for platforms and operating systems should be applied in a timely manner, according to vendor recommendations.

Systems, which are not security patched in a timely manner according to vendor recommendations, should be effectively isolated from computer networks and the internet, where relevant.

IT Security (spec. Vulnerability Management)

GMP: EU & PIC/S GMP Annex 11 (2011)

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.

IT Security (spec. Vulnerability Management)

GMP: EU & PIC/S GMP Annex 11 Concept Paper (2022)

27. [12.1] The current version says that "Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons". However, it is necessary to be more specific and to name some of the expected controls, e.g. multi-factor authentication, firewalls, platform management, security patching, virus scanning and intrusion detection/prevention

IT Security (spec. Vulnerability Management)

Typical findings

- Very often, companies and even big pharma and tech giants (cloud providers) are seen to deploy critical security patches in 6-9 months, while vendor recommendation is "immediately"
- No rationale for not deploying patches in a timely manner

Thanks for your attention

For questions:

Ib Alstrup, Medicines Inspector GxP IT, Danish Medicines Agency
ibal@dkma.dk, www.linkedin.com/in/ib-alstrup-baa2542