fimea

Lääkealan turvallisuus- ja kehittämiskeskus | Säkerhets- och utvecklingscentret för läkemedelsområdet | Finnish Medicines Agency

IT Systems in the Test Facility

Mirka Laavola
11 December 2019
GLP Seminar

Outline

- GLP requirements
- Project phase
  - Validation
- Operational phase
  - Change control
  - Incident management
  - Periodic reviews
  - Security
  - Business continuity and disaster recovery
- Retirement phase

IT requirements in GLP

Number 1:
OECD Principles on Good Laboratory Practice

Number 17: Advisory Document
Application of GLP Principles to Computerised Systems

1. Test Facility Organisation and Personnel

1.1 Test Facility Management’s Responsibilities

- establish procedures to ensure that computerised systems are suitable for their intended purpose, and are validated, operated and maintained in accordance with these Principles of Good Laboratory Practice.

1.2 Study Director’s Responsibilities

- ensure that computerised systems used in the study have been validated

4. Apparatus, Material, and Reagents

1. Apparatus, including validated computerised systems, used for the generation, storage and retrieval of data, and for controlling environmental factors relevant to the study should be suitably located and of appropriate design and adequate capacity.

7. Standard Operating Procedures

7.4. Standard Operating Procedures should be available for, but not be limited to, the following categories of test facility activities. The details given under each heading are to be considered as illustrative examples.

2. Apparatus, Materials and Reagents

b) Computerised Systems

- Validation, operation, maintenance, security, change control and back-up.

3. Record Keeping, Reporting, Storage, and Retrieval

- Coding of studies, data collection, preparation of reports, indexing systems, handling of data, including the use of computerised systems.

8. Performance of the Study

8.3 Conduct of the Study

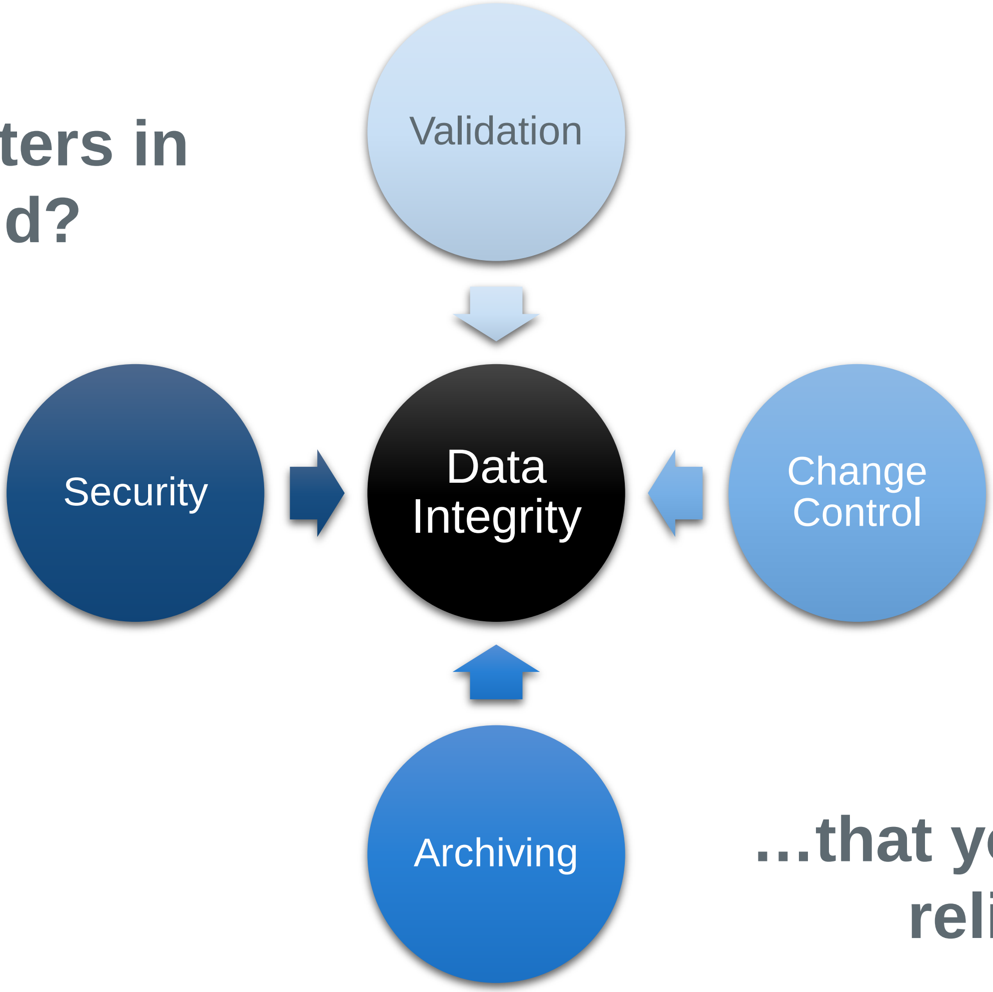
5. Data generated as a direct computer input should be identified at the time of data input by the individual(s) responsible for direct data entries. Computerised system design should always provide for the retention of full audit trails to show all changes to the data without obscuring the original data. It should be possible to associate all changes to data with the persons having made those changes, for example, by use of timed and dated (electronic) signatures. Reason for changes should be given.

10. Storage and Retention of Records and Materials

10.1 The following should be retained in the archives for the period specified by the appropriate authorities:

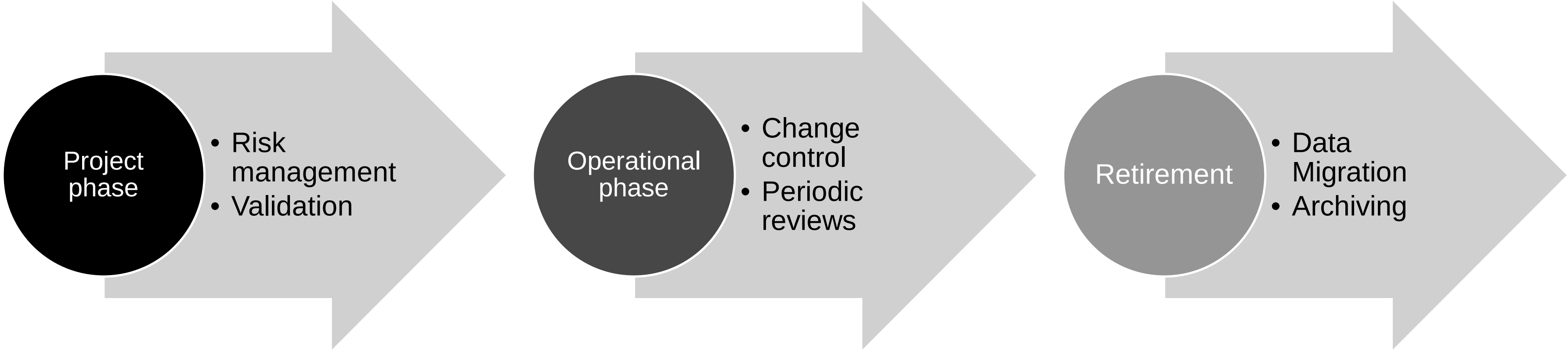
e) Validation documentation for computerised systems

What matters in the end?



…that your data is reliable!

Lifecycle management of Computerised systems



- Risk management should be applied throughout the life cycle
- Taking into account the need to ensure data integrity and the quality of the study results.
- Decisions on the extent of validation and data integrity controls should be based on a documented rationale and documented risk assessment.

Categorize the systems

E.g. using GAMP5 categories (Good automated manufacturing practice)

- Category 1 – Infrastructure software including operating systems, Database Managers, etc.
- Category 3 – Non configurable software including, commercial off the shelf software (COTS), Laboratory Instruments / Software.
- Category 4 – Configured software including, LIMS, SCADA, CDS, eArchiving, etc.
- Category 5 – Bespoke software

Validation

- Validation is required, if systems or data are:
  - directly relevant for regulatory submission or indirectly support GLP-relevant data
- Validation should be done **prospectively**

Excemptions: scope changed or an existing system becomes GLP relevant; (otherwise **no retrospective validation**)

Validation approach

- **Qualification**
  - Simple systems like commercial off the shelf software (COTS) e.g. pipettes, balances, photometers, refrigerators, freezers, data loggers

- **Validation**
  - Based on the complexity e.g. MS Excel Sheets, Temperature monitoring systems,
    - Validation Plan, Simple Testing, Validation Report
  - Configured and bespoken softwares
    - More validation deliverables are needed

Validation deliverables

- Vendor evaluation (basic evaluation, postal audit, on site audit)
- User requirement specification
- System description (data flows, interfaces, security controls etc.)
- Risk assessment
- Validation plan
  - IQ/OQ/PQ plan
  - Migration plan
- Validation testing
  - Test scripts (full testing or risk based approach)
- Data migration and migration verification
- Validation report
  - IQ/OQ/PQ reports
  - Migration report
  - Training report

Implementation

- Confirm that all necessary validation activities have been completed
- Deviations have been handled
- Changes during project phase have been handled and documented
- Procedures are in place
- Training has been done
- Take care of traceability of your specifications and testing (e.g.traceability matrix)

- Formal approval by responsible personnel before implementation

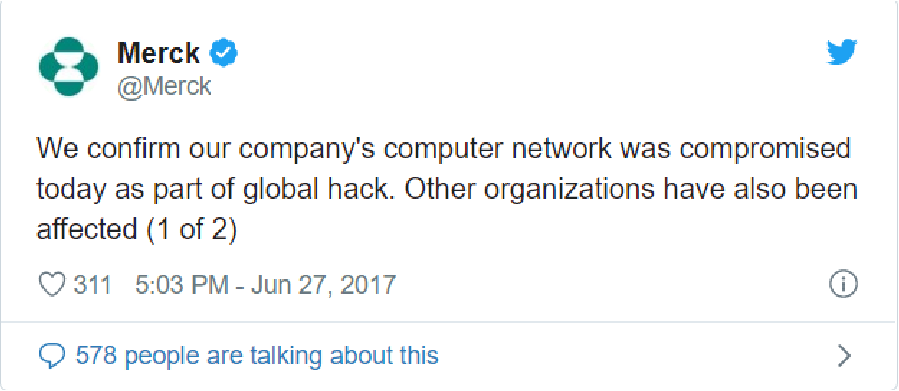
Operational phase

- Change management and configuration management
- Incident management
- Periodic review (define frequency to confirm that your system stays in validated state)
- User management (who gives the access, how training is done, what are the user levels)
- Audit trails
- Physical, logical security and data integrity (access control, virus protection etc.)

Business continuity and disaster recovery

- NHS (National Healthcare System) cyber attack in UK in 2017
  - 16 health service organisations hit by a "ransomware" WannaCry

- US pharmaceutical company MSD/Merck cyber attack in 2017



Merck
@Merck

We confirm our company's computer network was compromised today as part of global hack. Other organizations have also been affected (1 of 2)

311 5:03 PM - Jun 27, 2017

578 people are talking about this

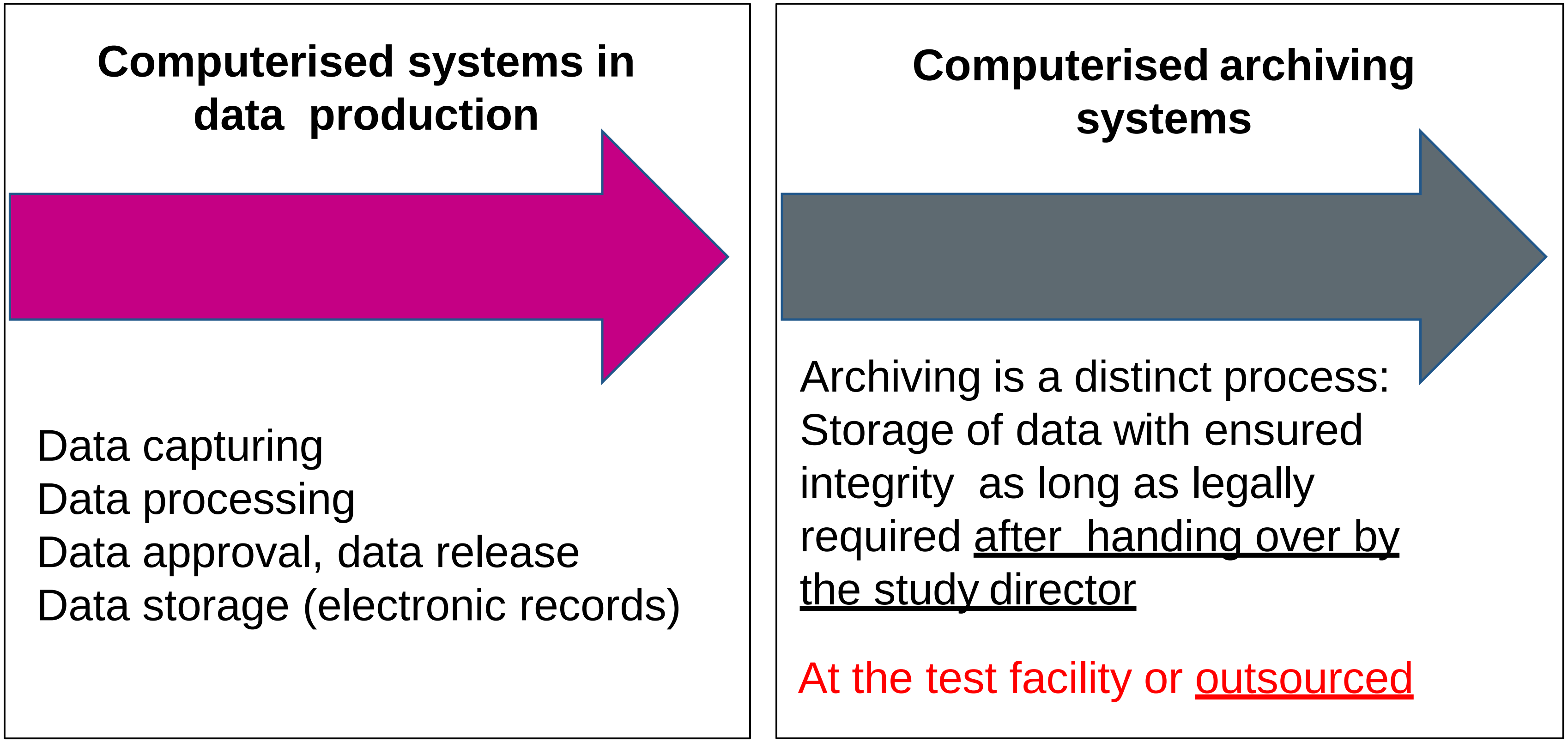
Business continuity and disaster recovery

- Original or back-up copies of all software in the version relevant for the validated computerised system are maintained, escrowed, or available by service level agreement.
- System recovery should be tested during validation and regularly during operational phase
- Procedures (SOPs) should be available

Data storage

- When data (raw data, derived data or metadata) are stored electronically, requirements for backup and archiving purposes should be defined
- Back-up of all relevant data should be carried out to
- Stored data should be verified for restorability, accessibility, readability and accuracy
- Hardware and software system changes must allow continued access to, and retention of, the data without any risk to data integrity

Electronic data



Computerised systems in data production

Data capturing
Data processing
Data approval, data release
Data storage (electronic records)

Computerised archiving systems

Archiving is a distinct process: Storage of data with ensured integrity as long as legally required after handing over by the study director

At the test facility or outsourced

Retirement phase

- System retirement should be planned and documented
- Data migration to new system or archive when needed
- Archiving of the data

Thank you!

Questions?