Data Governance for Investigator-Initiated Trials (IITs)

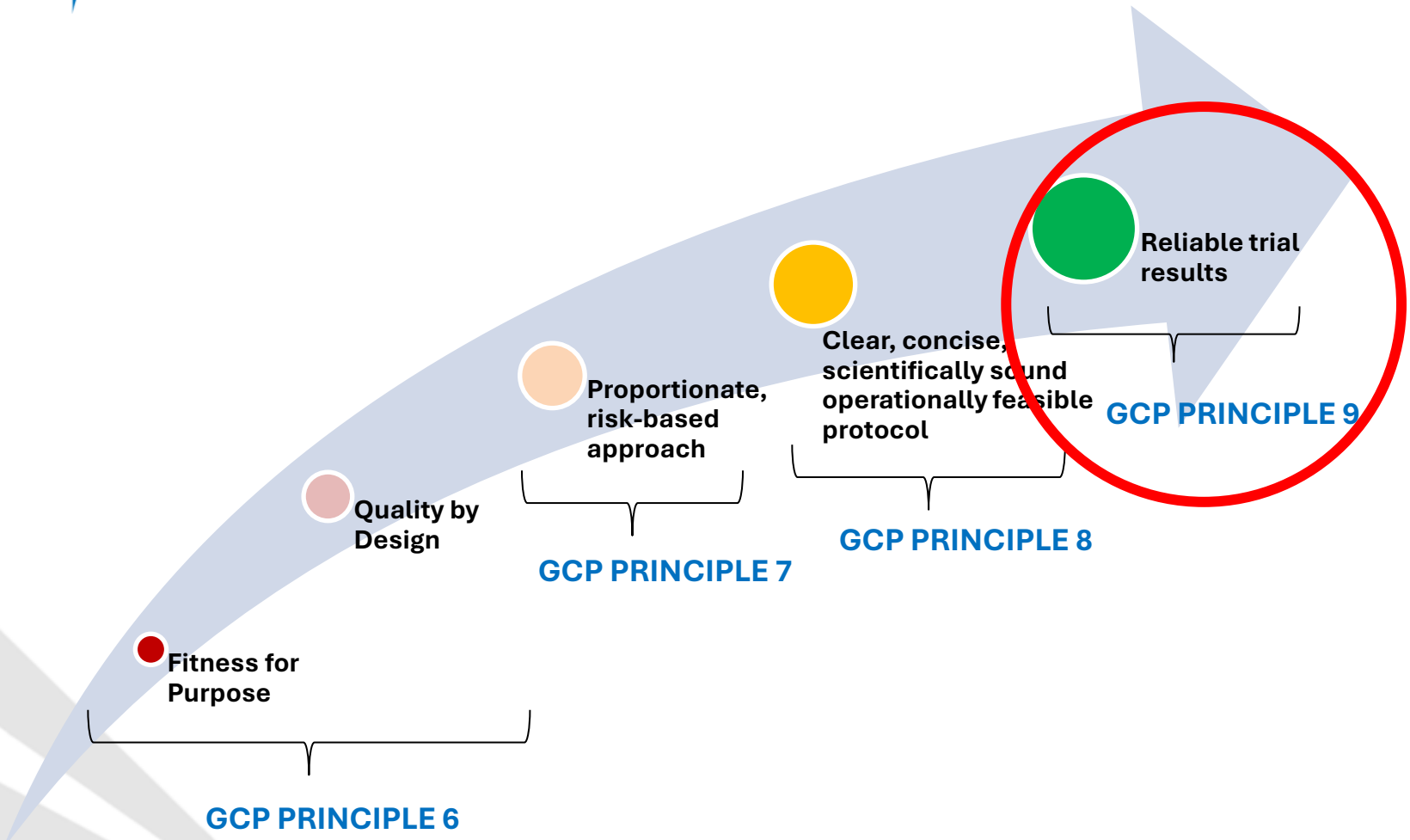
14 Nov 2025

Sumitra Sachidanandan
Regulatory Consultant
Innovation Office & Clinical Trials Branch
Health Products Regulation Group
Health Sciences Authority, Singapore

Outline

- Applying GCP Principles to Data Governance for IITs
- Documented procedures for data collection and handling for IITs
- Data Lifecycle Elements for IITs
- Computerised Systems in IITs
- Summary
- References

Applying GCP Principles to Data Governance



GCP Principle 9 – Reliable results

9. Clinical trials should generate reliable results.

9.1 The quality and amount of the information generated in a clinical trial should be fit for purpose and sufficient to provide confidence in the trial's results and support good decision making.

9.2 Systems and processes that aid in data capture, management and analyses, as well as those that help ensure the quality of the information generated from the trial, should be fit for purpose, should capture the data required by the protocol and should be implemented in a way that is proportionate to the risks to participants and the importance of acquired data.

9.3 Computerised systems used in clinical trials should be fit for purpose (e.g., through risk-based validation, if appropriate), and factors critical to their quality should be addressed in their design or adaptation for clinical trial purposes to ensure the integrity of relevant trial data.

9.4 Clinical trials should incorporate efficient and robust processes for managing records (including data) to help ensure that record integrity and traceability are maintained and that personal information is protected, thereby allowing the accurate reporting, interpretation and verification of the relevant clinical trial-related information.

Achieving Fit for Purpose Clinical Trial Quality

Trial is scientifically and operationally feasible to meet the trial objectives.

Trial is of sufficient quality to provide confidence in the trial results and to support good decision making.

Rights, safety and well-being of participants have been protected.

GCP Principle 6 – Quality by Design

6. Quality should be built into the scientific and operational design and conduct of clinical trials.

6.1 Quality of a clinical trial is considered in this guideline as fitness for purpose.

6.2 Factors critical to the quality of the trial should be identified prospectively. These factors are attributes of a trial that are fundamental to the protection of participants, the reliability and interpretability of the trial results and the decisions made based on those trial results. Quality by design involves focusing on critical to quality factors of the trial in order to maximise the likelihood of the trial meeting its objectives.

Applying QbD for Data Collection and Handling for IITs

Examples of Critical to Quality (CTQ) factors for Data Collection and Handling for IITs:

- Primary endpoints
- Secondary endpoints
- Adverse Events
- Data integrity*
- Privacy and Confidentiality

➢ **NB: Data integrity includes the degree to which data fulfil key criteria of being **attributable, legible, contemporaneous, original, accurate, complete, secure and reliable** such that data are **fit for purpose**.*

GCP Principle 7 – Risk proportionality

7. Clinical trial processes, measures and approaches should be implemented in a way that is proportionate to the risks to participants and to the importance of the data collected and that avoids unnecessary burden on participants and investigators.

7.1 Trial processes should be proportionate to the risks inherent in the trial and the importance of the information collected. Risks in this context include risks to the rights, safety and well-being of trial participants as well as risks to the reliability of the trial results.

7.2 The focus should be on the risks associated with trial participation. For clinical trials involving patients, the focus should be on risks that go beyond those associated with usual medical care. The risks relating to investigational products that have a marketing authorisation when used in the clinical trial context may differ from the usual care of patients and should be taken into consideration.

7.3 Risks to critical to quality factors should be managed proactively and adjusted when new or unanticipated issues arise once the trial has begun.

Applying RBQM for Data Collection and Handling for IITs (1)

CTQ	Risk Identification	Risk Evaluation	Risk Control
Primary Endpoint	• Use of uncalibrated thermometers	To be evaluated based on the probability, impact and detectability	• Supply calibrated thermometers
Secondary Endpoint	• Participants are unable to complete the questionnaires due to language barrier		• Use questionnaires with validated translations • Update the protocol to describe the process for completing the questionnaires with the assistance of investigator site staff if validated translations are unavailable
Adverse Events	• Underreporting of AEs • Delayed reporting of AEs		• Describe safety reporting process in protocol or protocol-related document • Train investigators on safety reporting requirements • Monitor safety reporting timelines

Applying RBQM for Data Collection and Handling for IITs (2)

CTQ	Risk Identification	Risk Evaluation	Risk Control
Data Integrity *(ALCOA, complete, secure and reliable)*	• Lack of attributability	To be evaluated based on the probability, impact and detectability	• Include initial and date fields in each section of Data Collection Form • Remind investigators to document review of test results in the EMR
	• Delays in CRF completion		• Include CRF completion timeline in CRF completion guideline • Train investigator site staff on CRF completion timeline • Monitor CRF completion timelines
	• Unauthorised access to trial data		• Ensure secure and limited access • Review audit trail regularly
	• Inconsistent trial data		• Scope of investigator site monitoring should be 100% for first 3 participants enrolled, and then 100% SDV for every alternate participant.
Privacy and confidentiality	• Data breaches		• Train staff on maintaining privacy and confidentiality

GCP Principle 8 - Protocol

8. Clinical trials should be described in a clear, concise, scientifically sound and operationally feasible protocol.

8.1 A well-designed trial protocol is fundamental to the protection of participants and for the generation of reliable results.

8.2 The scientific objectives of any trial should be clear and explicitly stated in the protocol.

8.3 The clinical trial protocol as well as the plans or documents for the protocol execution (e.g., statistical analysis plan, data management plan, monitoring plan) should be clear, concise and operationally feasible.

Protocol requirements for IITs

- **Clinical Trial Protocol**
  - ❑ **Clear, concise, scientifically sound** and **operationally feasible**
  - ❑ **Clear and explicitly stated scientific objectives**
  - ❑ **Data to be collected** and the **method of its collection**
  - ❑ Process by which the **participant's data will be handled** when a participant **withdraws or discontinues from the trial**
  - ❑ For **blinded trials** (if applicable):
    - ❑ Implement **measures to safeguard blinding**
    - ❑ Establish **procedures for unblinding**
    - ❑ Include **appropriate provisions** to ensure that **unblinded data** is **not shared with the investigator**

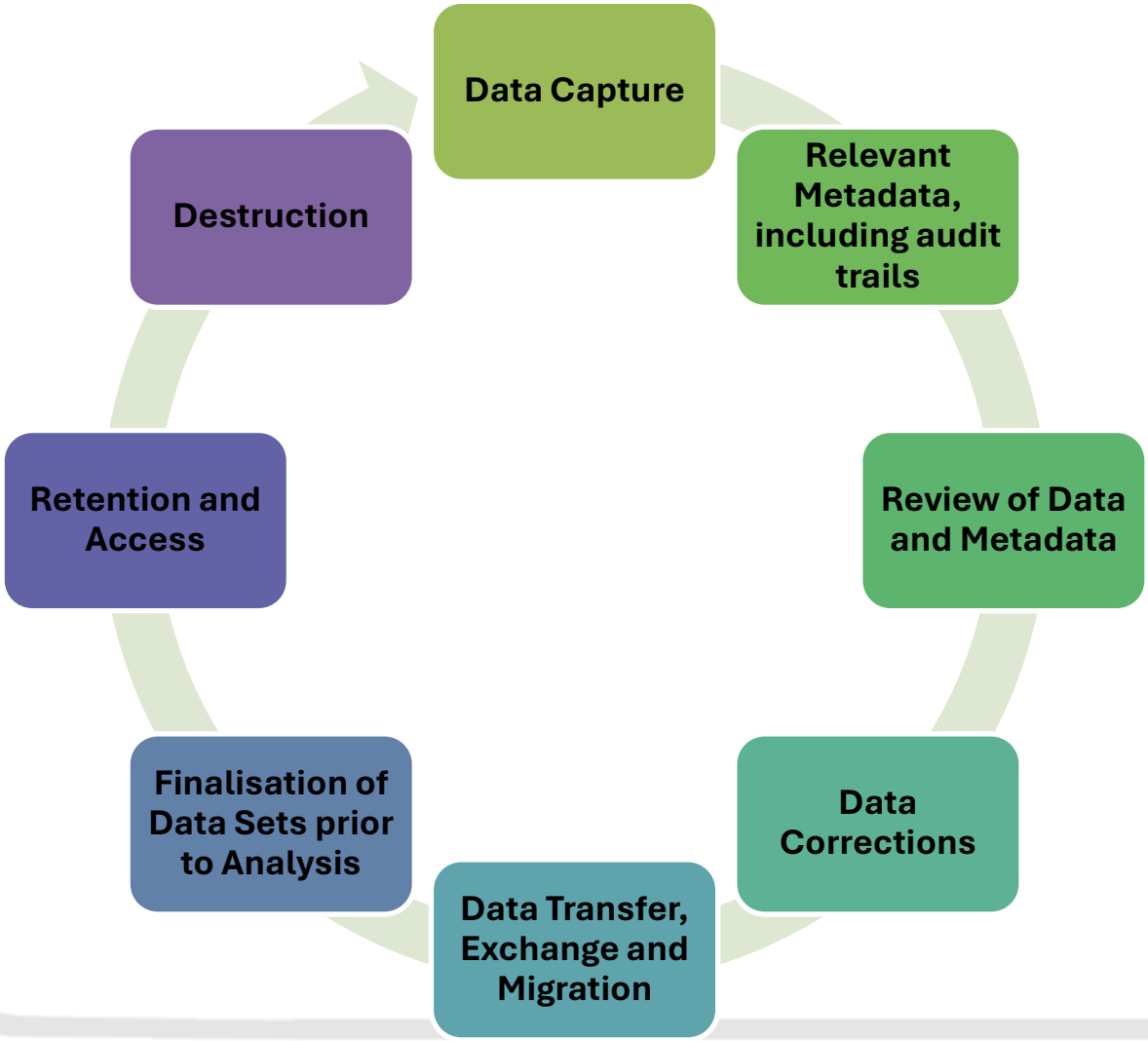
- ❑ **Protocol-related documents (e.g., plans, manuals, work instructions, workflows etc.)**
  - ❑ **Clear, concise** and **operationally feasible**
  - ❑ **Reviewed and approved** by the **sponsor or PI,** where applicable

Documented Procedures for data collection and handling

- Processes to ensure the **protection of the confidentiality of trial participants' data**
- Processes for **managing computerised systems** to ensure that they are **fit for purpose and used appropriately**
- Processes to **safeguard essential elements of the clinical trial,** such as randomisation, dose adjustments and blinding
- Processes to **support key decision making**, such as data finalisation prior to analysis, unblinding, allocation to analysis data sets, changes in clinical trial design and, where applicable, the activities of, for example, an IDMC.

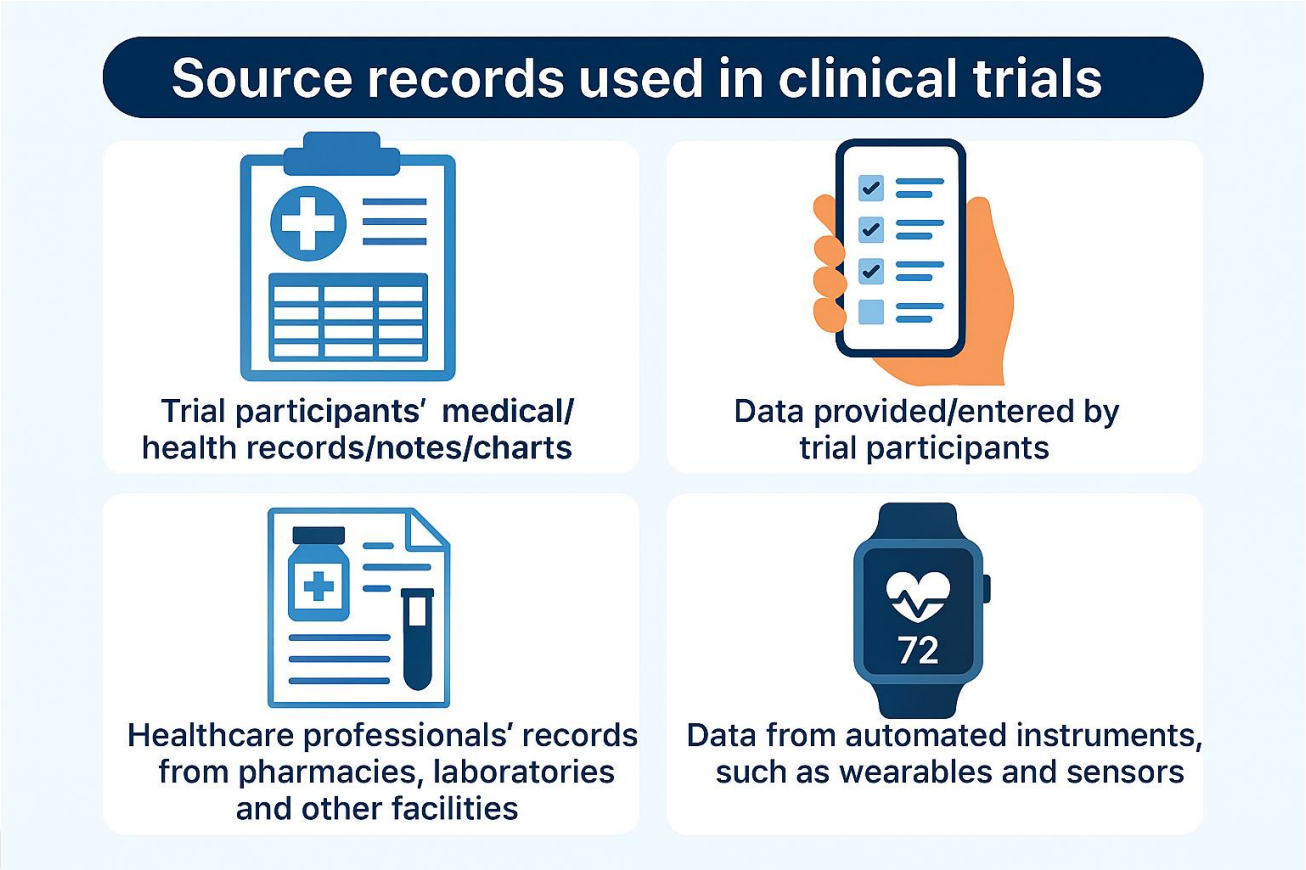
The key processes should **address the full data life cycle** with a **focus on the criticality of the data** and should be **implemented proportionately** and **documented appropriately.**

Data Lifecycle Elements



Source Records

- **Original documents or data** (which includes relevant metadata) or **certified copies of the original documents or data, irrespective of the media used.**



Case Report Forms (CRFs)

- A **data acquisition tool** designed to **record protocol-required information** to be **reported by the investigator to the sponsor** on each trial participant

How does data flow from source records?

- E.g.,
MS Excel, SPSS, R, Python, Stata, Jamovi etc.

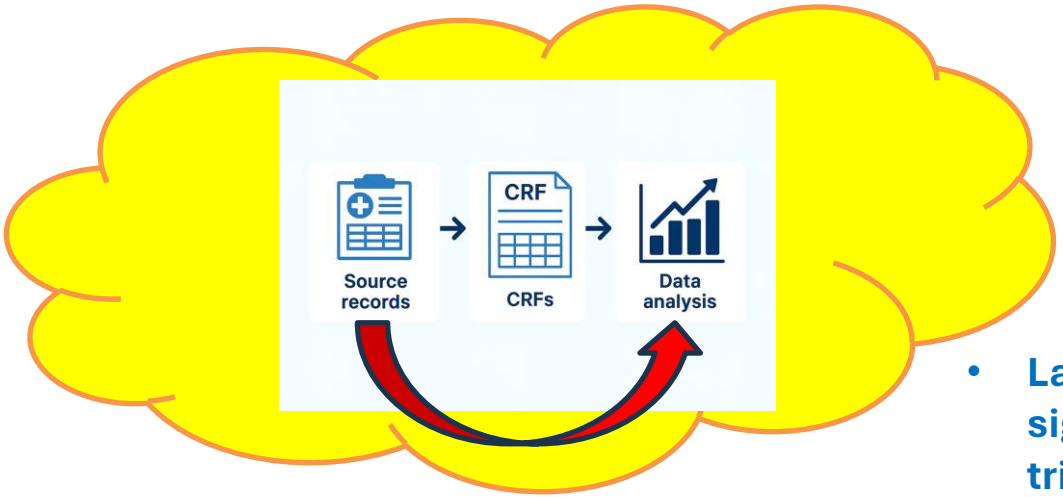
Can MS Word / MS Excel be used as electronic source records or electronic CRFs?

- **Lack of data integrity, thereby significantly impacting the reliability of trial results.**
  - Lack of audit trail will impact attributability, contemporaneousness and accuracy
  - May not be digitally signed and dated by persons entering the trial data

Are Data Collection Forms considered as Source Records or CRFs?

- **Source Record**
  - ❑ Contains **participant identifiable information** (e.g., name, DoB)
  - ❑ **Point of first capture** for trial data
- **CRF**
  - ❑ **<u>Does not</u> contain participant identifiable information**
  - ❑ Contains **trial data transcribed from source records**

Can trial data be directly transcribed from source data to data analysis software?



- **Lack of data integrity, thereby significantly impacting the reliability of trial results.**
  - Trial data may not be collected in accordance with the trial protocol.
  - Limitations with data analysis software
    - Lack of audit trail
    - Lack of computerised system validation

Data Capture for IITs

- **Investigator Responsibilities**
  - **Source Records**
    - ❑ Source Records Location List
    - ❑ Adequate source records
    - ❑ ALCOA principles
    - ❑ Changes to source records are traceable, and do not obscure the original entry and explained if necessary (via an audit trail).
    - ❑ Measures for protection of privacy of participant and confidentiality of data
  - **Case Report Forms**
    - ❑ Measures for protection of privacy of participant and confidentiality of data
    - ❑ Accuracy, completeness, legibility and timeliness of the data reported to the sponsor in the data acquisition tools
    - ❑ Data reported to the sponsor is consistent with the source records, and any discrepancies are explained.
    - ❑ Changes or corrections in the reported data should be traceable, should be explained (if necessary) and should not obscure the original entry.

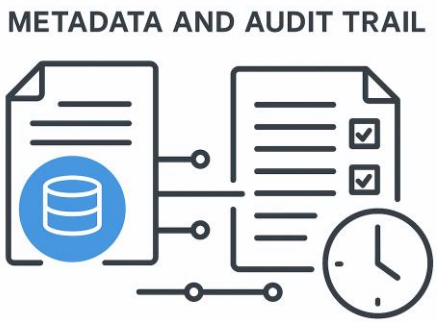
Data Capture for IITs

- **Sponsor Responsibilities**
  - **Case Report Forms**
    - ❑ Fit for purpose
    - ❑ Capture the information required by the protocol
    - ❑ Validated and ready for use prior to their required use in the trial
    - ❑ Data should be accompanied by metadata
    - ❑ Measures for protection of privacy and confidentiality
    - ❑ Data are protected from unauthorised access, disclosure, dissemination or alteration and from inappropriate destruction or accidental loss.

Relevant Metadata, including audit trails

METADATA

- The **contextual information** required to **understand a given data element** (i.e., data about data).
- Metadata is **structured information** that **describes, explains or otherwise makes it easier to retrieve, use or manage data**.
- For the purpose of this guideline, relevant metadata are those needed to **allow the appropriate evaluation of the trial conduct.**
- **Metadata should always be retained together with the trial data.**



AUDIT TRAIL

- **Metadata records** that **allow the appropriate evaluation of the course of events** by capturing details on actions (manual or automated) performed relating to information and data collection and, where applicable, to activities in computerised systems.
- The audit trail should **show activities**, **initial entry** and **changes to data fields or records**, **by whom, when and, where applicable, why.**
- In **computerised systems,** the **audit trail** should be **secure, computer-generated and time stamped**.

Example of Metadata

Metadata for Blood Pressure measurement:

1. Variable: Systolic Blood Pressure
2. Unit: mmHg
3. Type: Numeric (Integer)
4. Range: 70-250 mmHg
5. Method: Automated device, seated position
6. Frequency: 3 readings, 1 minute apart
7. Arm: Right (unless contraindicated)
8. Device: Omron HEM-907
9. Timing: Before study drug administration
10. Personnel: Research Nurse

Review of Data and Metadata

Why is it important?

- To facilitate the detection of:
  - ❑ unauthorised access
  - ❑ missing data
  - ❑ manipulated data
  - ❑ abnormal / outlier data
  - ❑ inconsistent timestamps (e.g., unusual date / timing)
  - ❑ incorrect data processing (e.g., manual calculations)
  - ❑ system / device malfunctions
  - ❑ training needs for users
  - ❑ deviations / non-compliances

How can it be performed?

- **Investigator Responsibilities**
  - ❑ **Timely review** of data
  - ❑ **Document review** of data
    - Paper source records : Initial and date
    - Electronic source records: Document review in EMR
- **Sponsor Responsibilities**
  - ❑ **Proportionate, risk-based approach** to **source data review (SDR) and source data verification (SDV)**
    - **Focus on critical data**

Data Corrections

- **Attributable**
  - Who made the correction?
  - Was the person authorised to make data corrections?
  - Did the initial / signature corroborate with the delegation log?
  - When was the correction made?
- **Justified and supported by source records around the time of original entry**
- Performed in a **timely manner**

Data transfer, exchange, migration & Finalisation of datasets

Data transfer, exchange, migration

- ❑ **Reconcile** the data to ensure that it:
  - ✓ Retains its **integrity**
    - ✓ Avoid data loss
    - ✓ Avoid unintended modifications
  - ✓ Preserves its **confidentiality**

Finalisation of datasets

- ❑ **Reconciliation** of data or datasets
- ❑ **Rectification** of data errors
- ❑ **Medical coding**
- ❑ Compilation and addressing the impact of **deviations and non-compliances.**

Retention and Access & Destruction

Retention and Access

- **Trial data and relevant metadata** are archived in a way that:
  - ✓ allows for their **retrieval and readability**
  - ✓ are **protected from unauthorised access** and **alterations** throughout the retention period.

Destruction

- **Trial data and metadata** may be **permanently destroyed** when they are **no longer required,** as determined by applicable regulatory requirements.

Computerised Systems Used in Clinical Trials

Documented Procedures for computerised systems

Documented procedures should be **proportionate to the importance of the computerised system** and the **data or activities they are expected to process**.

Record of important computerised systems used in clinical trials

- ❑ Use
- ❑ Functionality *(i.e., what the computerised system does)*
- ❑ Interfaces *(i.e., how the computerised system looks and feels to the user)*
- ❑ Validation status
- ❑ Who is responsible for its management
- ❑ Implemented access controls
- ❑ Internal and external security measures

Performing RBQM for computerised systems

CTQ	Risk Identification	Risk Evaluation	Risk Control
Data Integrity	• Lack of audit trail	To be evaluated based on the probability, impact and detectability	• Use computerised systems with audit trails • Perform Source Data Verification (SDV)
System validation	• Lack of / inadequate system validation		• Perform computerised system validation.
	• Lack of validation for system changes		• Ensure computerised system remains validated throughout the clinical trial.
User Management	• Access rights for staff was not revoked		• Review list of access rights
	• Lack of training		• Ensure staff are trained on the computerised system before granting access
	• User resistance for ePRO		• Use paper format as back-up for ePRO
	• Lack of validated translations for ePRO		• Develop alternative process for completing the questionnaires
Security, privacy and confidentiality	• Unauthorised access		• Automatically log users out after a period of inactivity • Follow institutional policy for establishing and changing passwords

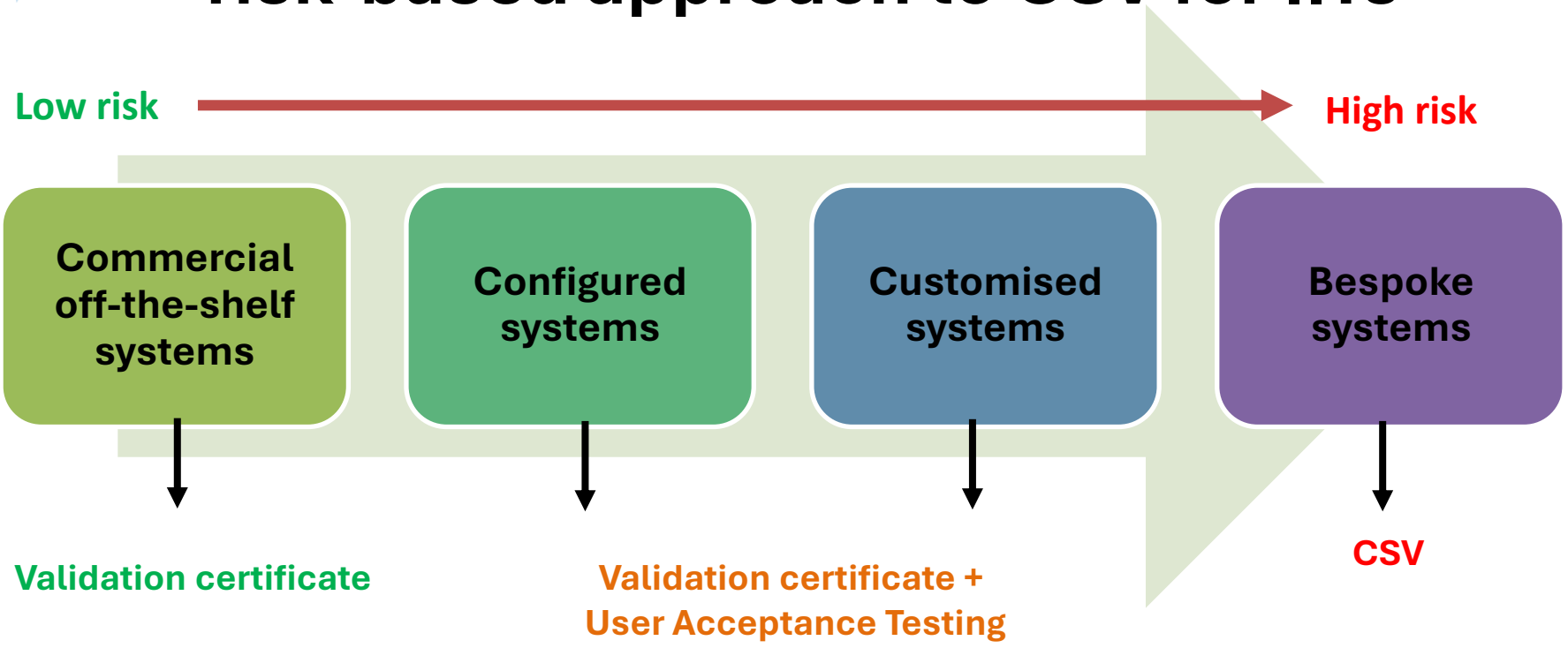
Performing RBQM for computerised systems

CTQ	Risk Identification	Risk Evaluation	Risk Control
Change control	• Uncontrolled updates	To be evaluated based on the probability, impact and detectability	• Establish change control process
System reliability	• Software bugs / glitches • Lack of system backup • Backup failures		• Ensure testing is done before update • Ensure system back-up • Test system back-up
System Integration	• Incompatibility between computerised systems		• Ensure compatibility before system integration.
Retention	• Archived data is inaccessible.		• Ensure that trial data and metadata remain complete, readable and readily available, and are directly accessible upon request by regulatory authorities, monitors, auditors and IRBs

Computerised System Validation (CSV)

- A **process** of **establishing and documenting** that the **specified requirements** of a **computerised system** can be **consistently fulfilled** from **design until decommissioning** of the system or **transition** to a new system.
- The **approach to validation** should be **based on a risk assessment** that takes into consideration the **intended use of the system** and the **potential of the system to affect trial participant protection** and the **reliability of trial results**.
  - **Focus on the important computerised systems used for the clinical trial.**
- **Comprises:**
  - User requirements and specifications
  - Validation plan
  - Test execution and reporting
  - System release
  - Periodic review
  - Change control
- The trial-specific systems (including updates resulting from protocol amendments) should only be **implemented, released or activated for individual investigator sites after all necessary approvals for the clinical trial relevant to that investigator site have been received.**

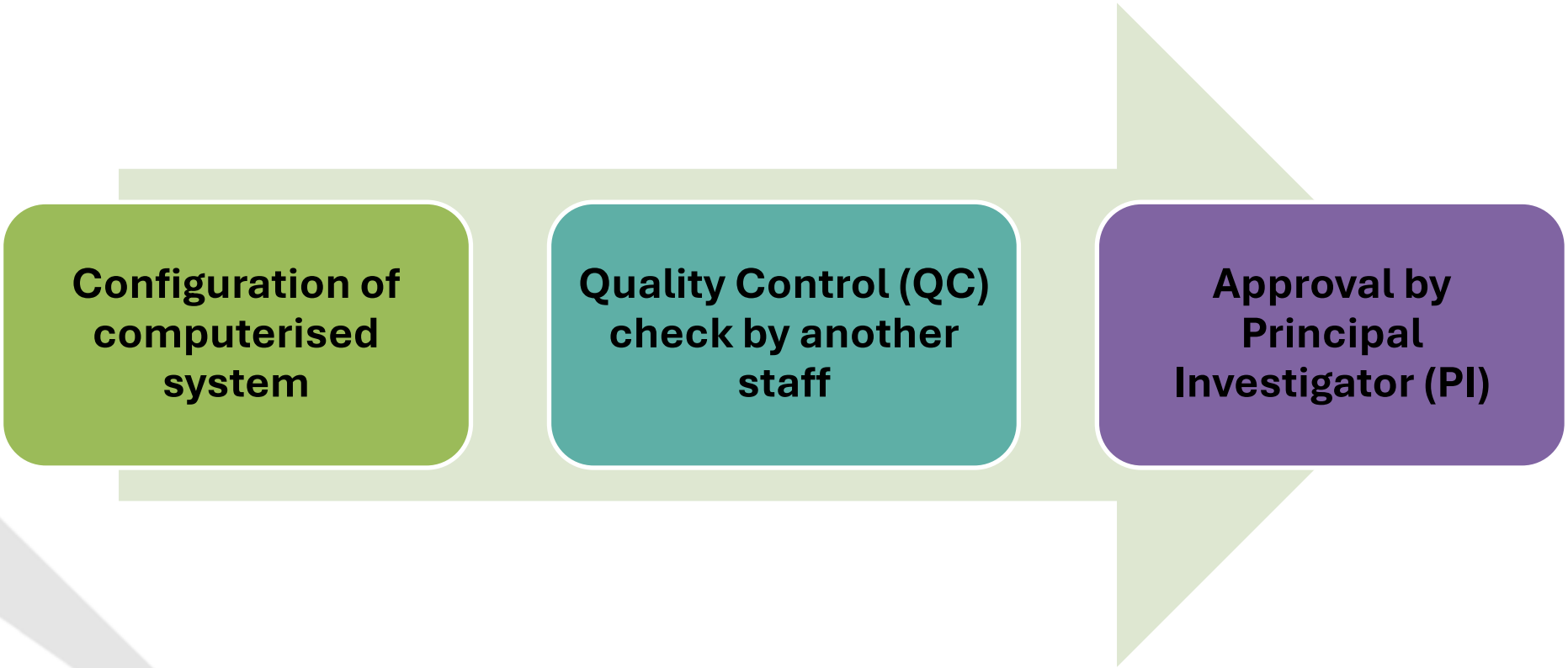
Applying a proportionate, risk-based approach to CSV for IITs



- **Configuration** sets up a system **using existing (out-of-the-box) functionality without altering the underlying code**. It **does not require programming knowledge** and **may be performed by a trained user**. For e.g., adding text fields in an eCRF (e.g., REDCap) in accordance with the trial protocol.

- **Customisation modifies and/or adds to existing functionality by custom coding.** It **requires programming knowledge**, and is **usually performed by an IT personnel**.

User Acceptance Testing (UAT) for configured computerised systems used in IITs



User Management for computerised systems

- Secure and limited access
- List of users and access permissions

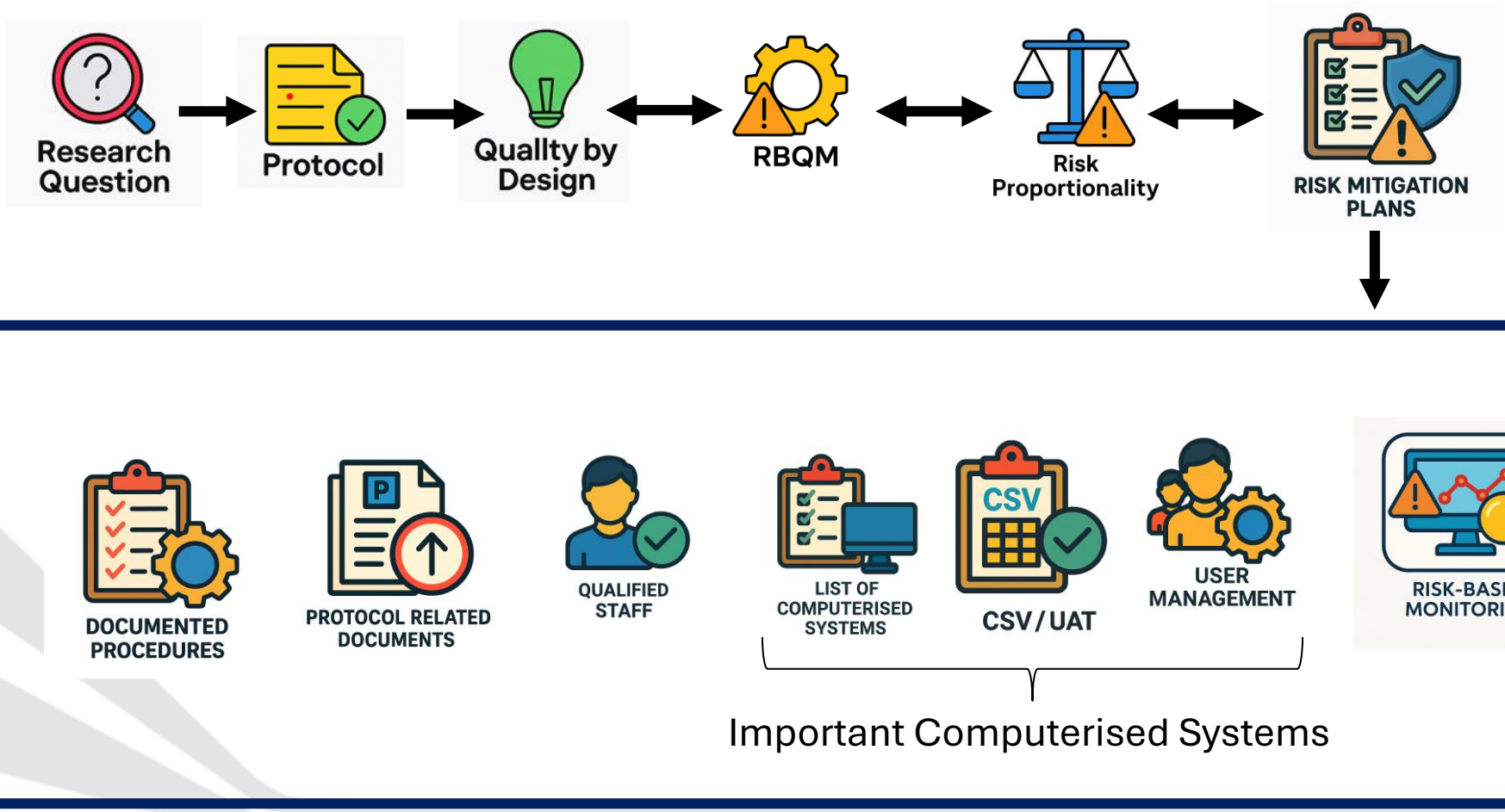
Name of staff	Role	Access permission	Start Date	End Date
	PI	Read / Write		
	Co-I	Read / Write		
	CRC	Read / Write		
	Monitor	Read		

- Access permissions should be aligned with the role and delegated tasks in delegation log.
- Users should be trained on the computerised systems, and training documented.
- List of users and access permissions should be periodically reviewed.
- Access permissions should be revoked for staff who leave the team.

Fitness for purpose assessments for computerised systems

- **System validation and maintenance**
  - Validation status, periodic review
- **User management**
  - User roles and access permissions
  - Periodic reviews
  - Provision of direct access for Monitors, Auditors, GCP Inspectors and IRBs
- **Audit trail**
  - Readable
  - Readily available
  - Indelible
  - Specifies the date, time, originator and reason for change
- **Security measures**
  - Security controls
  - Back-up
  - Incident reporting
  - Periodic review
- **Retention policy**
  - Alignment with regulatory requirements for record retention

Achieving Fit for Purpose Clinical Trial Quality



REFERENCES

- ICH E6 (R3) – Guideline for Good Clinical Practice, 6 Jan 2025

Thank You!

We welcome your queries!

HSA_CT@hsa.gov.sg