Establishing & Maintaining Data Integrity

Regulatory Requirements

Gaye Camm

Senior GMP Inspector – Technical Specialist

Inspections Section, Manufacturing Quality Branch

Medical Devices and Product Quality Division, TGA

Australian Government
Department of Health and Aged Care
Therapeutic Goods Administration

Acknowledgement of Country

I would like to acknowledge the Traditional Owners and Custodians of the lands on which we meet today and pay my respects to Elders past, present and emerging.

I would like to extend that acknowledgement and respect to any Aboriginal and Torres Strait Islander peoples here today.

Regulatory Requirements

Manufacturing principles for medicinal products

PIC/S Guide to Good Manufacturing Practice for Medicinal Products, PE009-15, 01 May 2021 (PE009-15)

Data integrity in the pharmaceutical sciences

- Computers
- Software
- Electronic data

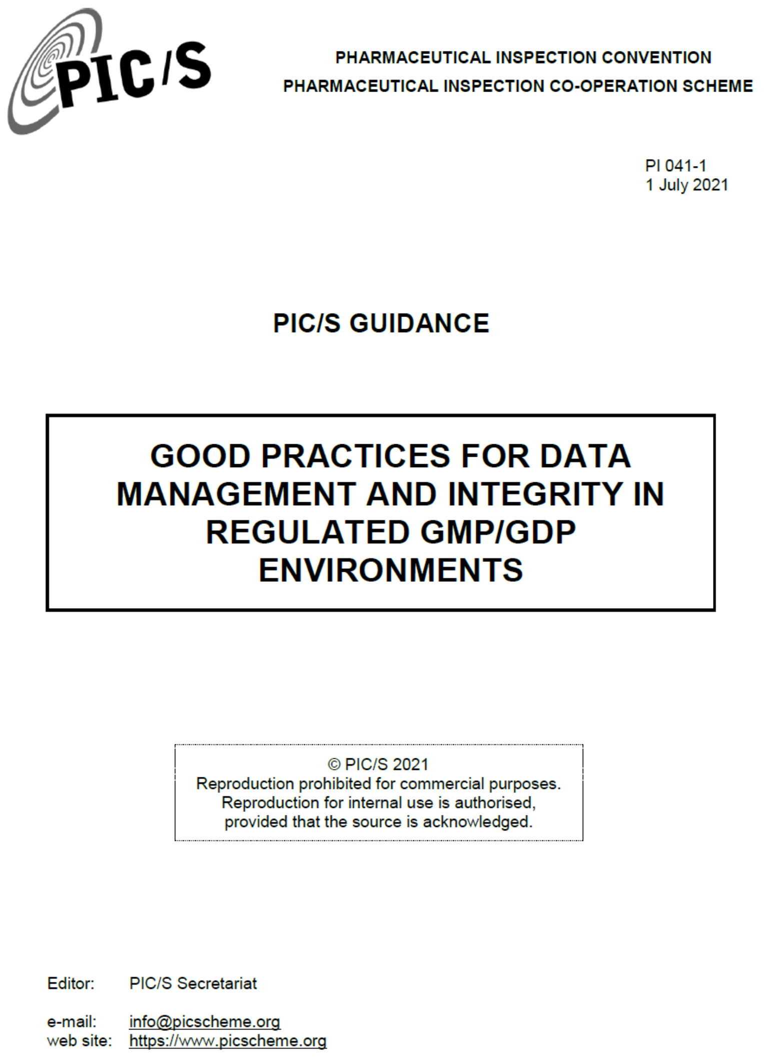
…used throughout the manufacture, testing and documentation of therapeutic goods

What is Data Integrity?

The degree to which data are

- Complete
- Consistent
- Accurate
- Trustworthy
- Reliable

…and these characteristics of the data are maintained through the data life cycle



PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 041-1
1 July 2021

PIC/S GUIDANCE

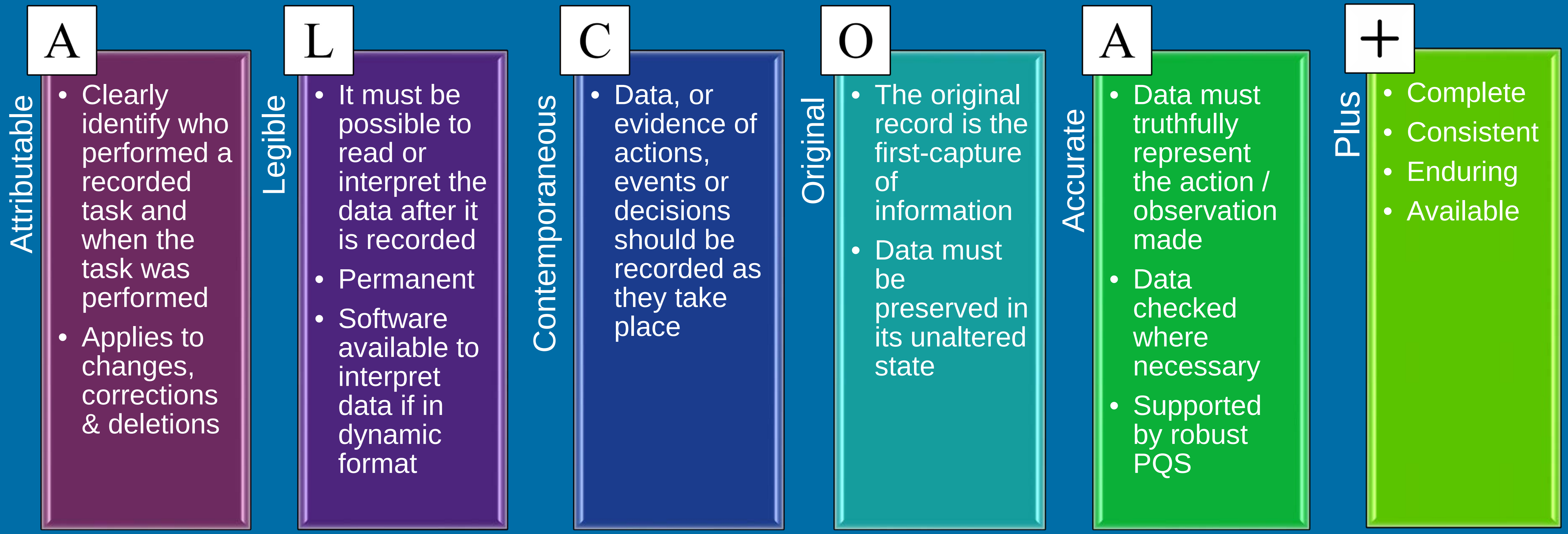
GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS

Editor: PIC/S Secretariat

e-mail: info@picscheme.org
web site: https://www.picscheme.org

https://picscheme.org/docview/4234

ALCOA+ Principles



A – Attributable

- Clearly identify who performed a recorded task and when the task was performed
- Applies to changes, corrections & deletions

L – Legible

- It must be possible to read or interpret the data after it is recorded
- Permanent
- Software available to interpret data if in dynamic format

C – Contemporaneous

- Data, or evidence of actions, events or decisions should be recorded as they take place

O – Original

- The original record is the first-capture of information
- Data must be preserved in its unaltered state

A – Accurate

- Data must truthfully represent the action / observation made
- Data checked where necessary
- Supported by robust PQS

+ – Plus

- Complete
- Consistent
- Enduring
- Available

Regulatory Requirements

ALCOA+ principles vs. PIC/S Guide to GMP

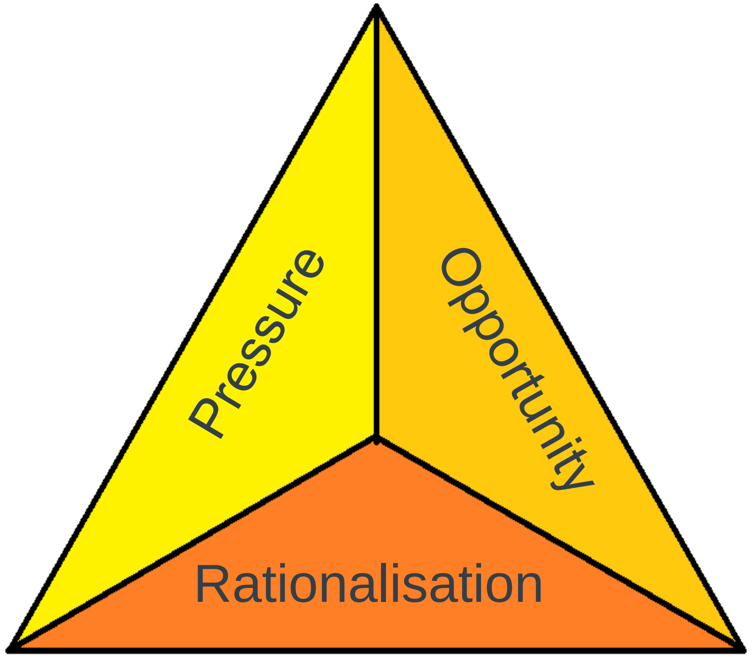
ALCOA principle	PIC/S Guide to GMP Part I	PIC/S Guide to GMP Part II	Annex 11 (Computerised Systems)
Attributable	[4.20, c & f], [4.21, c & i], [4.29 point 5]	[5.43], [6.14], [6.18], [6.52]	[2], [12.1], [12.4], [15]
Legible	[4.1], [4.2], [4.7], [4.8], [4.9], [4.10]	[6.11], [6.14], [6.15], [6.50]	[4.8], [7.1], [7.2] [8.1], [9], [10], [17]
Contemporaneous	[4.8]	[6.14]	[12.4], [14]
Original	[4.9], [4.28]	[6.14], [6.15], [6.16]	[8.2], [9]

ALCOA+ principles vs. PIC/S Guide to GMP (cont.)

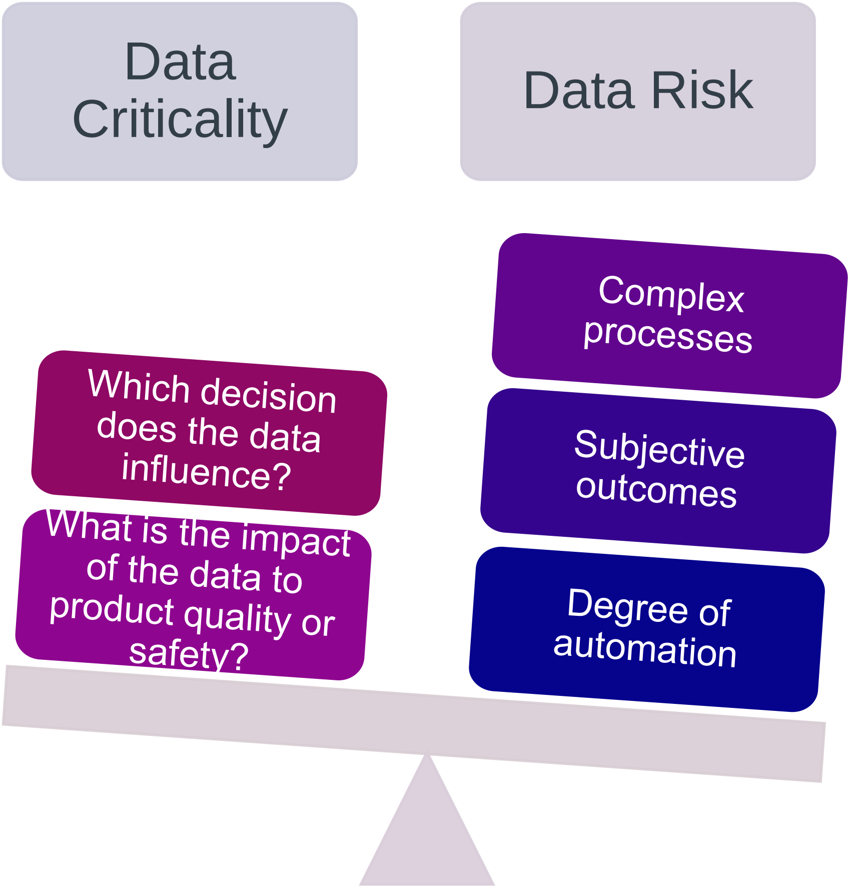
ALCOA principle	PIC/S Guide to GMP Part I	PIC/S Guide to GMP Part II	Annex 11 (Computerised Systems)
Accurate	[4.1], [6.17]	[5.40], [5.42], [5.45], [5.46], [5.47], [6.6]	[Paragraph "Principles"] [4.8], [5], [6], [7.2], [10], [11]
Complete	[4.8]	[6.16], [6.50], [6.60], [6.61]	[4.8], [7.1], [7.2], [9]
Consistent	[4.2]	[6.15], [6.50]	[4.8], [5]
Enduring	[4.1], [4.10]	[6.11], [6.12], [6.14]	[7.1], [17]
Available	[Paragraph “Principle”], [4.1]	[6.12], [6.15], [6.16]	[3.4], [7.1], [16], [17]

Creating the right environment

- Data management controls embedded in PQS
    - System design to ensure good DI practices
    - QRM approach to data integrity
    - Ongoing risk review of data criticality vs. risk
    - Robust self inspection program
- Clear understanding of importance of data integrity at all levels of the organisation
- Internal reporting encouraged & supported by Management
- Mature, open management approach to data integrity



Risk management approach to Data Integrity


Data Criticality
Data Risk
Which decision does the data influence?
What is the impact of the data to product quality or safety?
Complex processes
Subjective outcomes
Degree of automation

- Data Criticality
  - Batch release data > cleaning records
  - Data relating to product quality/safety
- Data Risk
  - Vulnerability of data to alteration, deletion, recreation, loss or deliberate falsification

Desired outcome = effective control strategy to manage identified risks

Where does it go wrong?

Data integrity issues seen during TGA inspections

Deficiencies relating to data integrity failure may have varying impact to product quality. Prevalence of the failure may also vary between the actions of a single employee to an endemic failure throughout the inspected organisation.

- PIC/S guidance - PIC/S Good Practices for Data Management and Integrity PI 041

Annex 11 §4.3 An up-to-date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems, an up-to-date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.

- No consolidated listing available
- Missing information e.g. PLC controlled equipment, simple testing instruments such as auto titrators, pH meters.
- Interfaces with other systems or processes not documented

Examples of critical systems

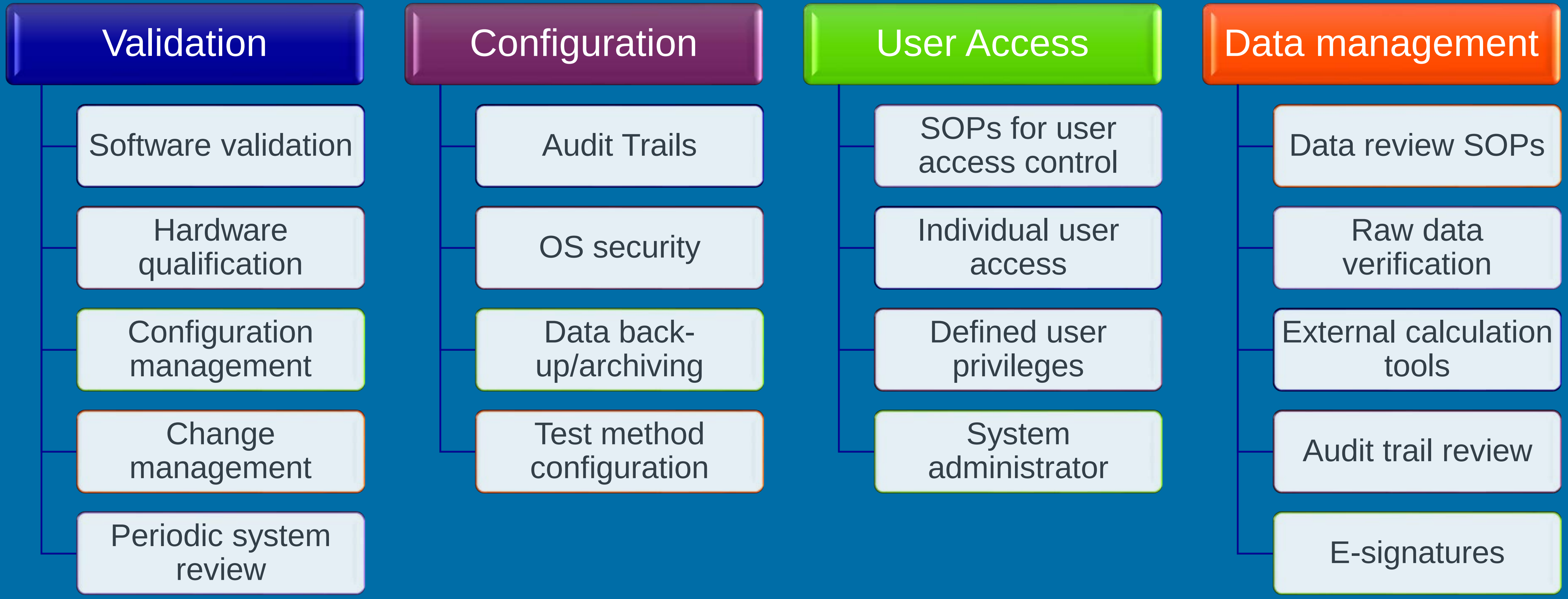
Questions to consider

- Does the system control the purchasing and/or status of products and materials?
- Is it used for the control and data acquisition for critical manufacturing processes or testing activities?
- Does the system generate, store or process data that is used to determine batch quality?
- Will the system generate data that is included in the batch processing or packaging records?
- Is the system used in the decision process for the release of products?
- Do you have simple systems that generate initial records in electronic format?

Computerised system should be verified for intended use

- No URS available for newly installed computerised systems
- Documentation supplied with commercial off-the-shelf products not reviewed to ensure user requirements are fulfilled
- Validation reports for critical system contained inadequate system descriptions:
  - ➢data flows and interfaces with other systems or processes
  - ➢hardware and software pre-requisites
  - ➢security measures required for DI

Laboratory Electronic systems



- Validation
  - Software validation
  - Hardware qualification
  - Configuration management
  - Change management
  - Periodic system review
- Configuration
  - Audit Trails
  - OS security
  - Data back-up/archiving
  - Test method configuration
- User Access
  - SOPs for user access control
  - Individual user access
  - Defined user privileges
  - System administrator
- Data management
  - Data review SOPs
  - Raw data verification
  - External calculation tools
  - Audit trail review
  - E-signatures

Control of standalone systems

- Back up of electronic data poorly administered
- Unique user logins not implemented for all staff
- Time & date on computer can be modified by user
- Data can be deleted directly from hard drives without detection

Annex 11 §9: 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 not regularly reviewed
- Audit trail review conducted on select data only
- Review requirements not formalised in procedures
- Orphan data not captured in analysis
- Reconciliation of electronic data with associated logbooks not considered

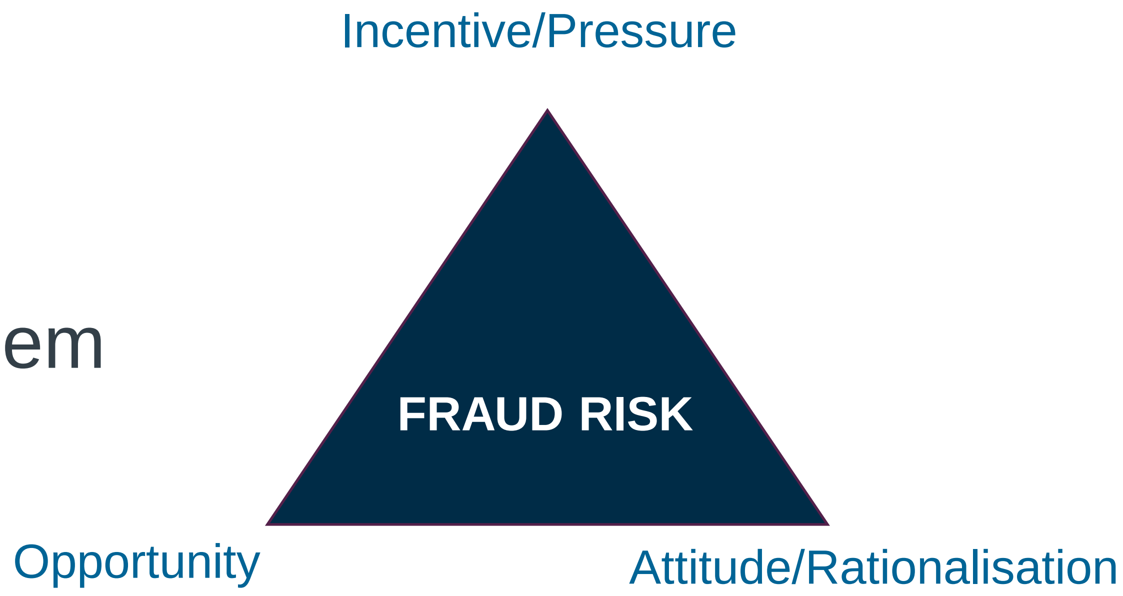
Third party suppliers of cloud services

- No risk assessment conducted to identify risk associated with using third parties who are creating, processing or storing regulated data
- No supplier assessment of cloud service providers conducted
- No formal agreement in place between the manufacturer and cloud service provider outlining GMP responsibilities

TGA expectations…understand vulnerabilities

- Design systems to prevent DI issues
- Ensure the data is authentic and retrievable
- Train staff and encourage correct behaviours and practices
- Open communication
- Encourage feedback
- System for ongoing review

- It’s not someone else’s problem



Questions?

www.tga.gov.au

Australian Government

Department of Health and Aged Care
Therapeutic Goods Administration