Record Management & Data Governance

Trev Simmons, TS CSV QA Ltd

TS CSV QA
ASSURING DATA QUALITY & INTEGRITY

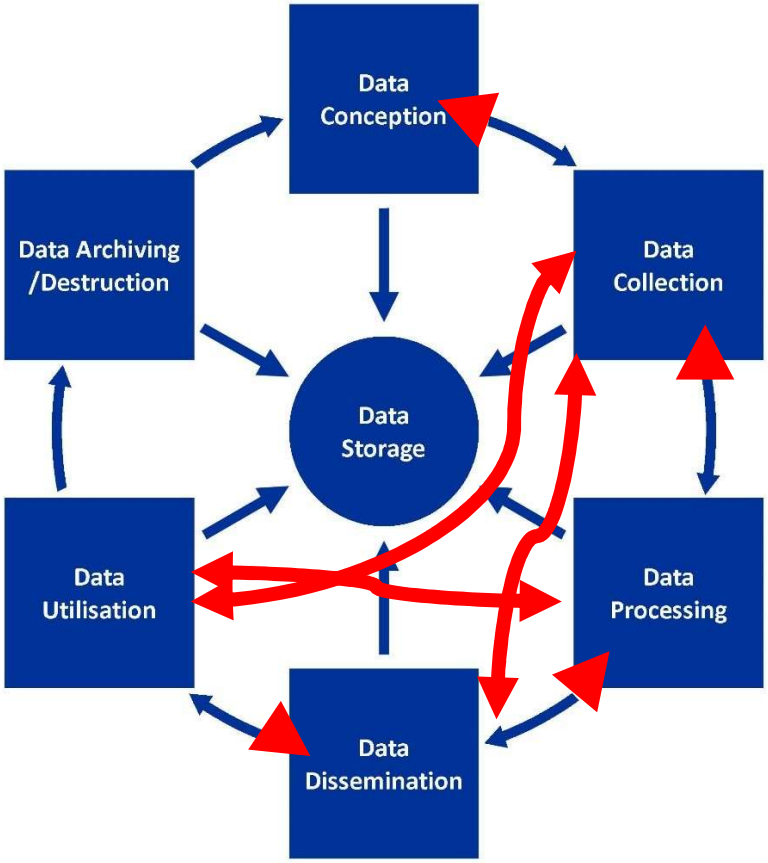
wehive
masterclasses • conferences • in-house training

Agenda

- Data Lifecycle
- Computer Systems
- Buy, Build, Configure
- SaaS / Cloud

Data Lifecycle

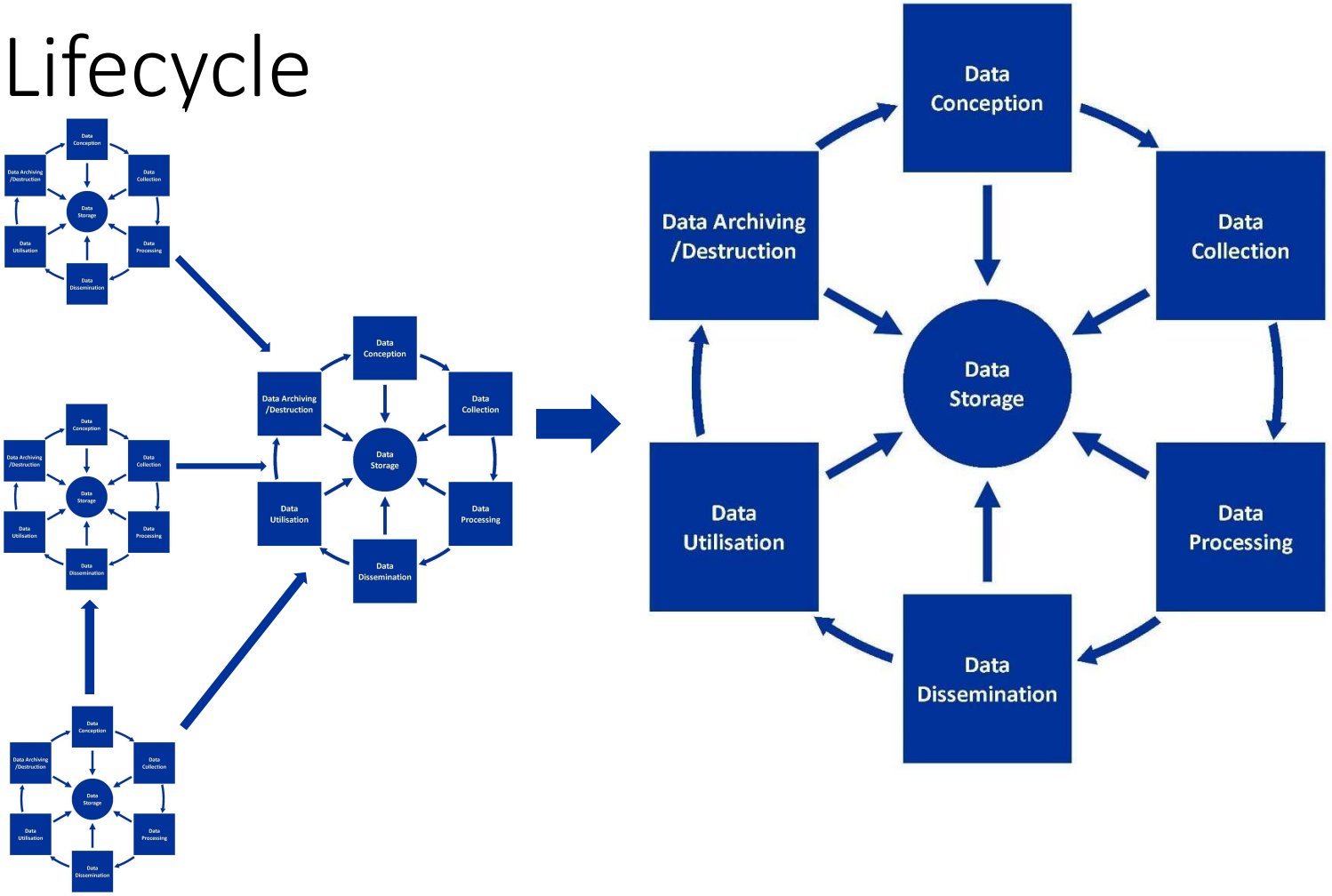
Data Lifecycle



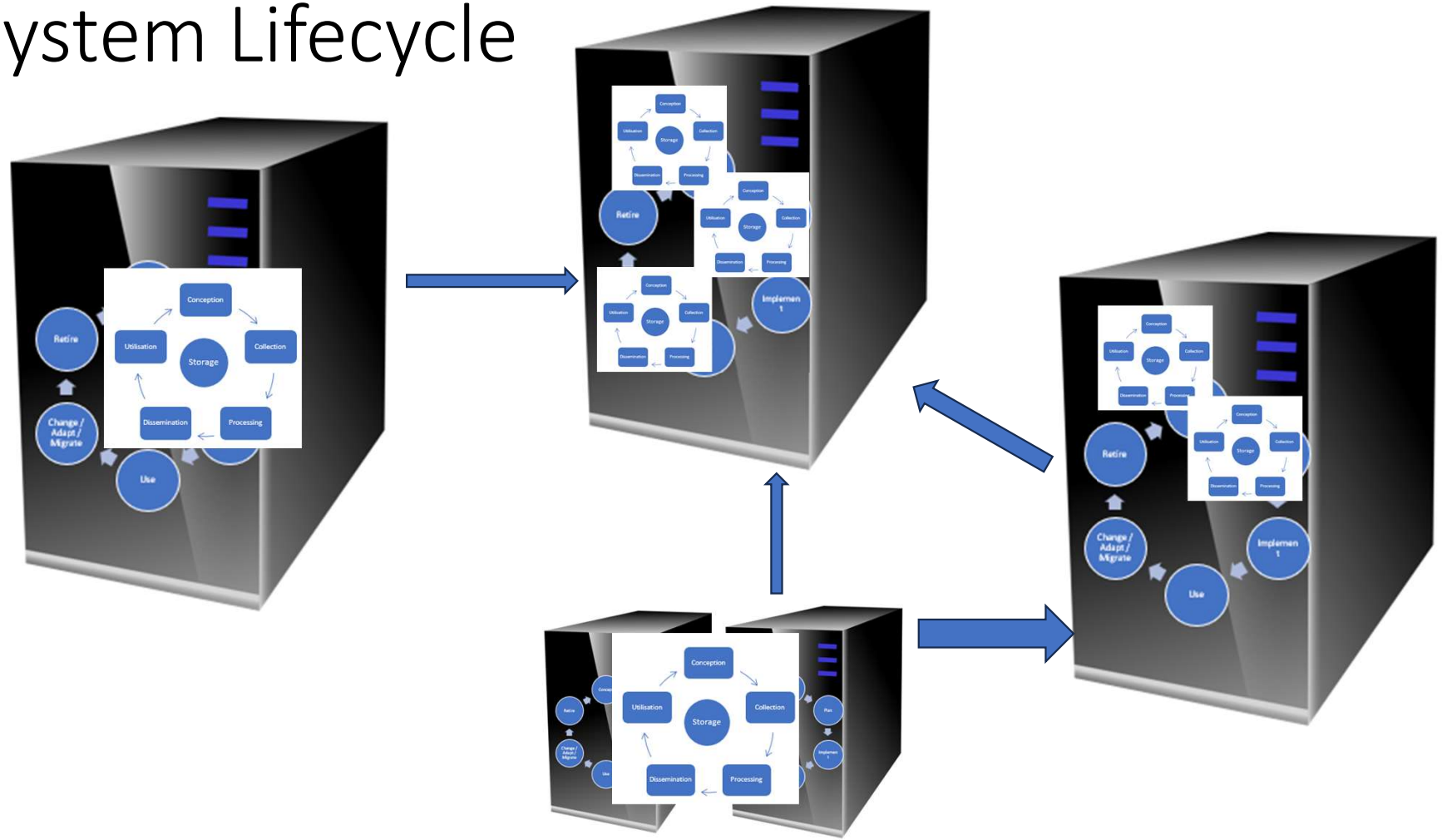
TS CSV QA
ASSURING DATA QUALITY & INTEGRITY

wehive
masterclasses • conferences • in-house training

Data Lifecycle

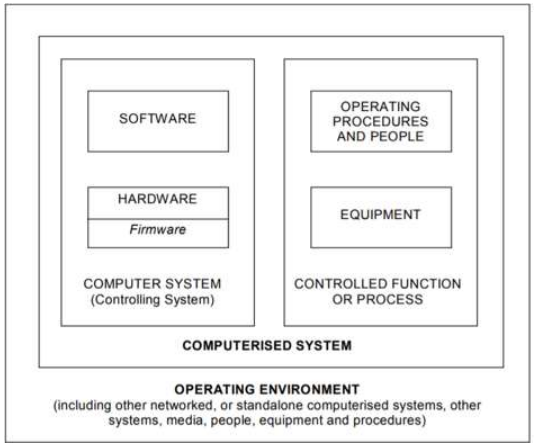


System Lifecycle



A Computerised System…

- ….is the set of hardware, software, procedures and people which together perform one or more of the data capture, processing, analysis and reporting functions, e.g. on regulatory study data
- Not just a DLL, or an Application could be an integrated collection of applications



Data Conception

Data Purpose

- System, Department, Organisation, Clients…..
- Basis of Validation Activities

Data Definition

- Data
- MetaData
- System, Department, Organisation, Client

Data Criticality

- Quality
- Safety
- Efficacy

Data Conception

- Inherent Risks
  - Alteration / Adulteration
  - Destruction
  - Suitability of System
- Data Flow throughout the lifecycle.
  - Data Flow Metadata
  - MetaData

Data Collection

Authorised Originator

- Person
- Device
- Data System

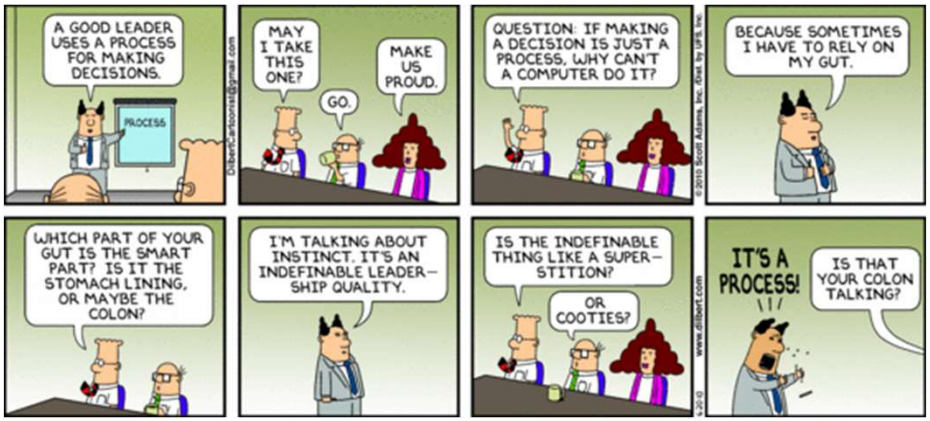
Instrument Reliability

- Error Margins
- Originator Accuracy
- Data
- MetaData
- System, Department, Organisation, Client

Storage Considerations

- Temporary vs Permanent
- Control
- True / Certified Copies

Data Processing



Acceptable and Unacceptable Alterations

- Allowed
- Disallowed
- Constructive Denial

Audit Trail of Changes (see Data Storage Logs)

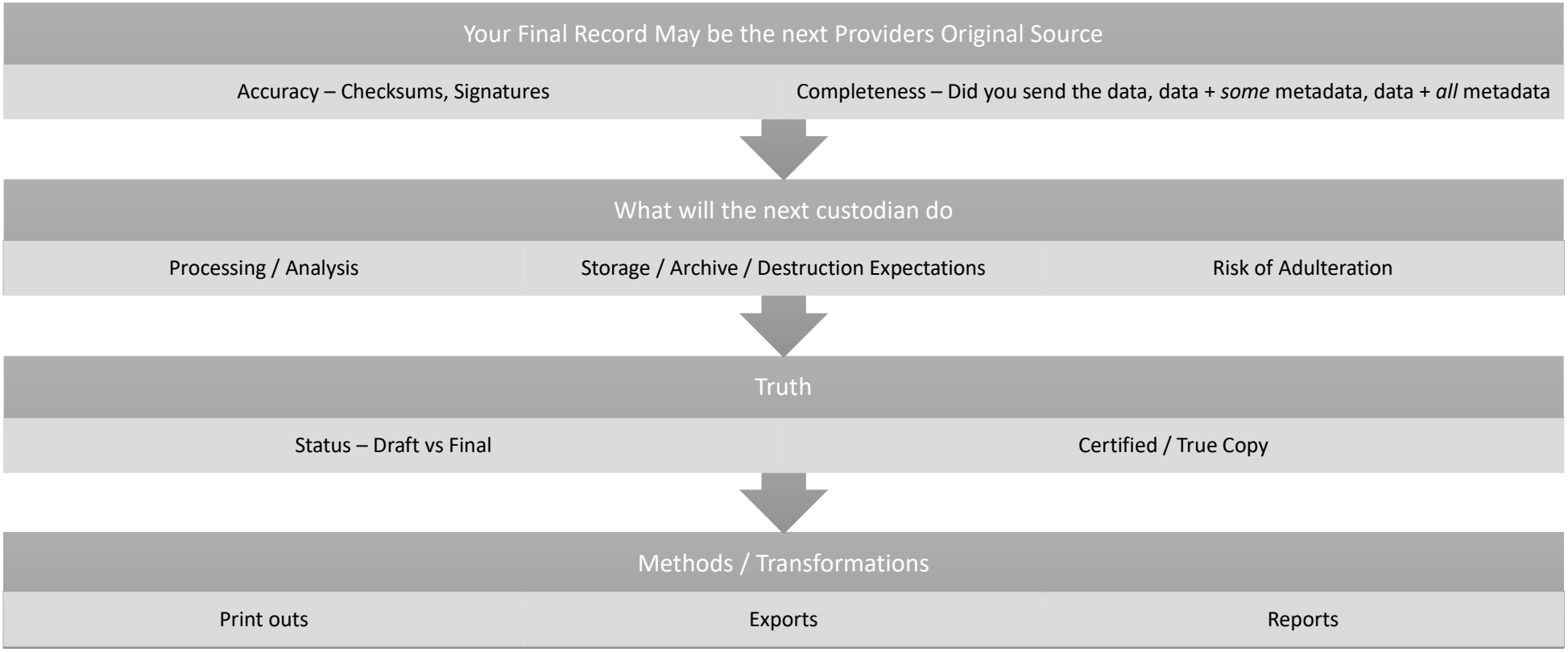
Authorised Processors

- User Access Rights
- Review / Approval
  - The Record
  - Changes

Data Processing

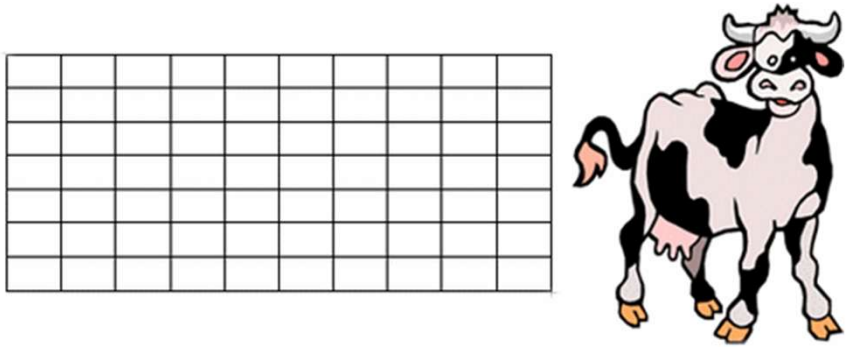
- Access / Audit Trail Review
  - Risk Based
  - Targeted or Full
  - High level or Detailed
    - 10k transactions a day in Manufacturing Plant LIMS
    - 6 Monthly Review
  - Audit Trail Data Mining
    - Keyword Search
    - Filterable
    - Old vs New Comparison
    - Paper Verification Processes

Data Dissemination



Data Utilisation

- Needs to be considered during Dissemination
- Multiple Copies & Multiple Purposes
- Access Control
  - Who can see what
  - Is its use authorised and justified
- Do you know all the ways the data is being used beyond your organisation?
- Will they tell you if that utilisation changes?
- Is the new use valid?



System / Data Re-Use

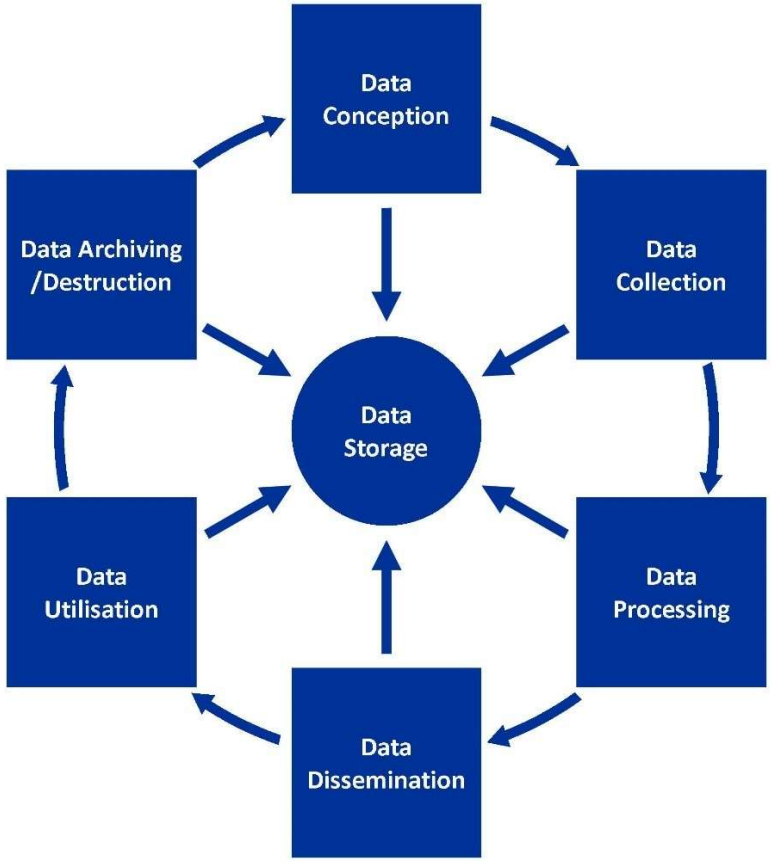
Validation of a Pilot Plant - Material Dispensary System (Inventory and Weigh-scale integration)	• Interface with Material Inventory • Confirms Material and updates for dispensed amounts • Works with 5 Balances from 2 Manufacturers • Dispense amounts 0-1kg granularity to Micrograms
Can re-use the system in Production?	• Interface with Same Material Inventory • Confirms Material and updates for dispensed amounts • Works with 2 new balances from the same supplier • Dispense amounts 0-100kg granularity to Grams

TS CSV QA
ASSURING DATA QUALITY & INTEGRITY

wehive
masterclasses • conferences • in-house training

Data Utilisation

- Are the people using the data aware of the Conception Definition?
- Is the utilisation aligned?



Data Archiving & Destruction

Are the retention requirements known	Clear Rules in Some GxPs for specific Data Usage Dependent
Format	Dynamic Usable Format Alternative Static Format •PDF •Write Once Media
Endurance	Longevity Verification
Have you destroyed the Record if there are disseminated copies?	Backups Notification to Destroy Record of the Destruction

Data Storage

Access Control

System Access
OS Access
Hardware Access
Network Exposure

Metadata / Audit Trail Components

Access Logs
System Logs
Error Logs
Application Logs
Transaction Logs

Replication

Backup Copies
Shadow / Version controls
Location (Global)

- ALCOA


Attributable
• User Identity Management
Legible
• Plain understandable Information
Contemporaneous
• As close to realtime as practicable
Original
• From the Source system
Accurate
• Subject to QC,Audit, Format Checks, Range / Value Checks

- ALCOA++

Complete

- Data and MetaData

Consistent

- Same Equipment,Settings,templates

Enduring

- Recorded and stored in a manner it can be retained ……25 years (previously 30)

Available

- Accessible whilst Enduring

Traceable

- Can Follow Data from System A to System B to C. And Requirement to Test to Evidence

So What needs to be in place?

- Attributability –Security
  - Limited, Role based Access
  - Username/Password Controls (Strong/Complex, use of Multi Factor Authentication)
- Legibility – Can still see what is deleted (Audit Trails / Logs)
- Contemporaneous
  - Reliable Date/Timestamps…..
  - System / Application Timestamp Can a PC Clock / Mobile Device Date/Time be changed
  - In the expected Time Window & Sequence
- Original
  - Source, Certified Copy, Transcribed
- Accurate
  - QC, SDV, Query Management activities

So What needs to be in place?

- Complete
  - All expected data and metadata is present (Edit Checks, Data Transfers/Truncation)
- Consistent
  - Source, Certified Copy, Transcribed
- Enduring
  - Available throughout the Trial and the expected Record Retention period (…25 years)
- Available
  - Viewable (by Sponsor, CRO, Investigators) throughout the Record Retention period
- Traceable
  - Know where the data came from (all systems/ sources)
  - Who / What created / edited

Workshop 1 – Data Flow

- Phase II Double Blind, Multicenter Study to evaluate MakeMeBetter compared to GrannyRecommends for brain cancer
- Primary End-Point – Progression-free survival (PFS) defined as the time interval form Randomisation until tumour progress according to RECIST
- Secondary End-Point – QoL based on fatigue and pain scores based on weekly at home completion via ePRO device and reviewed by Site staff during Visits
- Study and Data Management outsourced to a CRO with a 3rd part EDC system
- Centralised Medical Imaging for Tumour analysis
- eCOA solution provider
- Central & PK Laboratory
- IRT / IMP distribution provider
- Sites in EU, UK, and North Africa

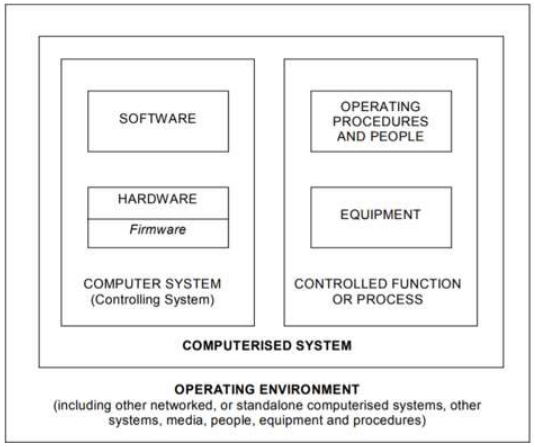
Workshop 1 – Data Flow

- Draw Up a Data Flow for the Study based on the information provided?
- Are there any gaps? (Fill them in, Be creative)
- How does this study fit with the Risks identified in Day 1 / 2 for a study?
  - Can you Link Systems / Suppliers to the Hazards / Risks?
  - Does the Data Flow give rise to any new Hazards / Risks?

Computer Systems

A Computerised System…

- ….is the set of hardware, software, procedures and people which together perform one or more of the data capture, processing, analysis and reporting functions, e.g. on regulatory study data
- Not just a DLL, or an Application could be an integrated collection of applications



So What is a System – How many systems do you have?

Business View

- EDC – Platform (cross-Project / Function)
- EDC – Project Specific Website
- eCOA Tablet used by Sites
- ePRO Device used by Subjects
- Sponsor / CRO Data Management Portal
- Manual Data Upload Portal
- eTMF
- SAS

Technical View

- Web Server
- Database Management Server
- FTP Server (Import / Export)
- File Server / Network Data Storage
- Clinical Trial VLAN
- Network Security (AV, IDS/IPS)
- Replication Services

So What is a System – How many systems do you have?

There is no right Answer, it will vary based on

- Vendor / System / Team Capabilities
- Contracts and Agreements
  - System A to System B Interface – Vendor A produced, Vendor B produced, Joint effort?
- Vendor / Team Structure
- Expertise / Availability
- Architecture / Component Design of Platforms

The critical item is to ensure a determination is made, and there are no gaps based on the data flow

eQMS & LMS

Overall Picture

- MS Sharepoint Site
  - Maintains Native QMS documentation with Version control
- QMS Administrators take ‘finalised’ documents – approved via Docusign
- Signed Documents Uploaded to Staff Viewing Portal
- Automated Workflows trigger either
  - Read and Understand
  - Competency Quiz
- Competency Quizzes Built in ‘ClassMarker’ website
  - Question Banks
  - Pass Marks
  - Re-tests
  - Certificate Generation
- Certificate Returned to Trainee and QMS Admin – Upload in to another Sharepoint Site

Systems

One System

- 2 SharePoint Sites
- 1 DocuSign Implementation,
- 1 Class Marker configuration,
- Manual processes

Two Systems

- QMS
  - 1 Sharepoint Site
  - 1 DocuSign Implementation
  - Manual processes
- LMS
  - Manual Processes
  - 1 Class Marker site
  - 1 SharePoint Site

Four Systems…..

Buy, Build, Configure

Software Categories

GAMP Category 1 – Infrastructure Software

- Established or commercially available layered software: Applications are developed to run under the control of this kind of software. This includes operating systems, database managers, programming languages, middleware, ladder logic interpreters, statistical programming tools, and spreadsheet packages (but not applications developed using these packages).
- Infrastructure software tools: This includes such tools as network monitoring software, batch job scheduling tools, security software, anti-virus, and configuration management tools. Risk assessment should, however, be carried out on tools with potential high impact, such as for password management or security management, to determine whether additional controls are appropriate.

- Layered software is not subject to specific functional verification although their features are functionally tested and challenged indirectly during testing of the application. The identity and version numbers of layered software and operation system should be documented, and verified during installation.
- Infrastructure software tools are generally highly reliable, and significantly removed from any aspect of patient risk. All infrastructure software should be controlled and managed.

GAMP Category 3 – Non-configured

This category includes off-the-shelf products used for business purposes. It includes both systems that cannot be configured to conform to business processes and systems that are configurable but for which only the default configuration is used. In both cases, configuration to run in the user's environment is possible and likely (e.g., for printer setup). Judgement based on risk and complexity should determine whether systems used with default configuration only are treated as a category 3 or category 4.

GAMP Category 3 – Non-configured

- A simplified life cycle approach may be applied to Category 3 products. Supplier assessment may not be necessary.
- The need for, and extent of, supplier assessment should be based on risk. User requirements are necessary and should focus on key aspects of use. Functional and design specifications are not expected from the user, although there should be sufficient specification to enable testing (typically covered by the User Requirements Specifications (URS) and other relevant documentation). Verification typically consists of a single test phase.
- All changes to software should be controlled, including supplier-provided patches. Standard Operating Procedures (SOPs) should be established for system use and management, and training plans implemented.
- Configuration management should be applied. For systems where the default configuration is used, configuration management demonstrates that the defaults are accurately selected.

GAMP Category 4 - Configured

- Configurable software products provide standard interfaces and functions that enable configuration of user specific business processes. This typically involves configuring predefined software modules.
- Much of the risk associated with the software is dependent upon how well the system is configured to meet the needs of user business processes. There may be some increased risk associated with new software and recent major upgrades.
- A life cycle is appropriate for configured products. Detailed URSs are necessary. The approach to assessment of the supplier and of the configurable product should be risk-based and documented. (See appendix M2 of the GAMP 5 guide).
- While Functional Specifications (FSs) may not be owned by the user, there should be adequate specification available to ensure traceability and adequate test coverage. Verification should ensure that the software product meets the user requirements with particular focus on the configured business process. Custom modules should be handled as Category 5 components.

GAMP Category 4 - Configured

- The approach should address the layers of software involved and their respective categories. The approach should reflect the outcome of the supplier assessment, GxP risk, size and complexity. It should define strategies for the mitigation of any weaknesses identified in the supplier's development process.
- Since each application of the software product is specific to the user process, support of such systems needs to be carefully managed. For example, when new versions of software products are introduced, serious problems can arise from the dependency of custom code on features of the software product which may have changed.
- Custom software components such as macros developed with internal scripting language, written or modified to satisfy specific user business requirements, should be treated as Category 5.
- In the absence of an adequate supplier Quality Management System (QMS), suppliers should be encouraged to develop such a QMS based on the principles in this Guide. Under such circumstances the software should be considered as Category 5. Regulated companies are, however, responsible for ensuring the quality of the software and hardware, and the fitness for purpose of the computerized system when used in the GxP environment.

GAMP Category 5 – Custom Application

- These systems or subsystems are developed to meet the specific needs of the regulated company. The risk inherent with custom software is high. The life cycle approach and scaling decisions should take into account this increased risk, because there is no user experience or system reliability information available.
- The life cycle approach is similar to configured products, with the addition of design. The approach to suppler assessment should be risk-based and documented. A Supplier Audit is usually required to confirm that an appropriate QMS is established to control development and ongoing support of the application. In the absence of an adequate QMS, suppliers may use this Guide to provide the foundation for managing application development and support.
- The approach should address the layers of software involved and their respective categories. It should reflect the assessment of the supplier and any audit observations, GxP risk, size, and complexity. It should define strategies for the mitigation of any weaknesses identified in the supplier's development process

Software Categories

Software Categories

- Overlapping definitions
  - Non-configured includes configuration
  - Firmware(originally category 2, now treated as 1,3,4,5 as applicable)
- Infrastructure Service have
  - Non-configured / Configurable Templates
  - Ability to write bespoke apps inside the Infrastructure
- REQUIRES CONTEXT
  - A Category 3 solution for You
  - Is a fixed solution made in a Category 4 platform from a CRO
  - Which they purchased from a Software Developer (Category 5)

Still a useful guiding principle

Build

- Expertise (In-house / Vendor)
- Resource Availability / Scalability
  - Initial Build
  - Maintenance / Operation
  - Future Adaptations
- More activities to oversee that you are Directly Responsible for
- Includes commitment across the GxP Retention Period…

- Cutting / Bleeding Edge
- Part of your Intellectual Property / USP

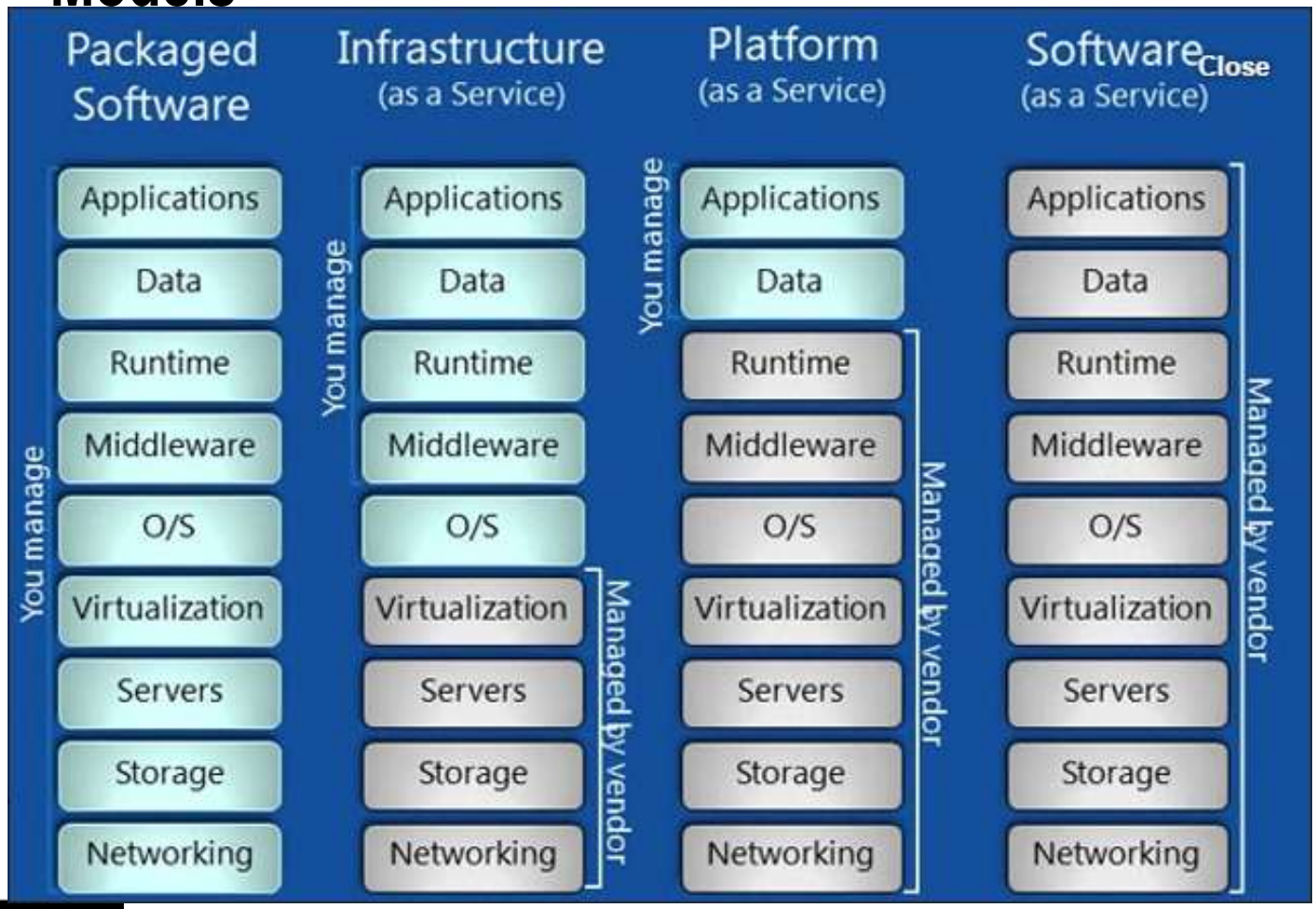
Buy (Category 3 / 4)

- A Service with Software Attached (i.e. a Full Service CRO)
- Software you can implement as your own internal service
- External Expertise / Resource Capability
- Lets your internal SMEs focus on their day jobs
- More activities to oversee that you are Directly Responsible for
- Includes commitment across the GxP Retention Period…

- Routine / More Generic processes
- Fixed Process, or Non-complex need for configuration
- Using a Risk proportionate approach you can trust / leverage supplier activities

As A Service

As a Service - Models



As a Service - Models

SaaS Provider

- Application
- Data
- Runtime

PaaS Provider

- Middeware

IaaS Provider

- O/S
- Virtualisation
- Servers
- Storage
- Networking

Service Provider (IT Vendor) Oversight

Assessment Planning Considerations

- You cannot look at all of the systems
- Risk based approach
  - Inventory / Last Validation details
    - Older Systems will have less thorough validation or may be from an older SOP
  - Validation Plan / Report
    - Level of Detail
    - Does the project appear to have had difficulties or is very complex
  - Understand the interactions with the system during the business process session

Assessment Planning Considerations

- Data Criticality
  - Yours – Your Programme / Study
  - Theirs – Is it Study Specific or One Size fits all
- Bespoke or COTS – GAMP Category
  - Bespoke – Full Lifecycle
  - COTS – Configuration
  - Pre-validated (Purpose)

As a Service Challenges

- Frequently there is no ‘Right to Audit’
- You are not in direct contract with all the providers
- The need for Security creates a shroud of mystery
  - Not listing personnel
  - Not providing Actual DC locations
- Hiding behind Privacy Laws
- Vendors not wishing to share Oversight evidence
- Reliance on Certifications SOC2, ISO27001, ISO13485, ISO9001
- Questionnaires

Audit Scopes

- Vendor
- System
- Process
- Study

Audit Planning

Core System Validation / Processes

Overall Platform – Qualification

Template / Standard Configuration Settings

Can you trust the core validation so you don't need to test at the trial level but can 'trust' the system

Trial Specific Validation / Processes

Yours – Your Programme / Study

Theirs – Is it Study Specific or One Size fits all

Audit Planning

Information Security

- Cyber Response / Incident Management
- Disaster Recovery
- Business Continuity
- The Cloud and Current Conflicts – Multi-center replication, lots of data ‘copies’ preventing loss. Loss of region unthinkable.

Bespoke or COTS – GAMP Category

- Bespoke – Full Lifecycle
- COTS – Configuration
- Pre-validated (Purpose)

Business Continuity / Disaster Recovery / Backup

Business Continuity	Disaster Recovery	Backup	Recovery Point Objective	Recovery Time Objective
•How you continue to run your CT activities WHILE the system is implementing the Disaster Recovery mechanisms •Not needed (are you sure?) / Alternative System / Manual Process •Tested	•How to get 'a' system back up and running…. Failover •Does it cover 'Failback' •Multiple Sources / Preferred source •Tested to verify Recovery Objectives •Linked to, but also separate from Backup	•Frequency •Media •Locations (Same machine, Same Cluster, Same or different Physical location •The Cloud and Current Conflicts – Multi-center replication, lots of data 'copies' preventing loss. Loss of region unthinkable.	The timepoint (in the past) to which you will have to revert in the event of a disaster •Amount of Data Loss •Context of your Trial – Realtime, 5 minutes, 1 hour, 1 day, 1 week. Is it source or can data be reconstructed from source	The expected elapsed time from the Disaster Occurring (or being discovered) to having the system (or alternate) operational •Does DR get implemented fully or partially •Often system specific – What happens of all the systems are lost at once? •Tells you how long you might need to operate your Business Continuity plans

BC /DR Spot Test

- Vendor System has an RPO of 24 hours and the system is backed up daily
- Backup Results (Success / Failure) are posted to a Slack channel monitored by the Infrastructure Team
- Incidents are logged if a backup job fails on 2 consecutive attempts
- Client is notified if 3 consecutive backup attempts fail

Are you comfortable with this approach?

BC /DR Spot Test

- Vendor System has an RTO of 24 hours and performs annual tests to verify the capability
- System Receives Blood Sugar levels in Realtime from a Subject Wearable Linke to their Mobile Device
- If the system is not available data is retained on the Mobile and Transmitted when the system is next online

Are you comfortable with this approach?

What records should you see in Audit

- Plans
  - Validation
  - Installation
  - Development
  - Testing
- Reports
  - Validation
  - Installation
  - Development
  - Testing
- Specifications
  - User Requirement Specification
  - Configuration Specification
  - Test Specification

Understandable to non-technical Personnel

What records might you see in Audit

- Agile Processes are eroding the concept of documents
- Requirements and Testing may be in the same System or Separate
  - Automated Testing may simply be code files
  - Auditor May have to rely on Comments, the number of reviewers and approvers, i.e the evidence of testing code generation controls
- Can Lead to a lot of over the shoulder auditing
- Has greater evidence of control as includes all the tasks and comments that are lost to ‘Drafting’ of documents

Don’t Forget - Data Flow / Interfaces

- The most likely risks to Data Integrity will be at the boundaries / interfaces between systems AND organisations
- Data transfer / Submissions
- Qualified Secure ‘File Upload System’ – Client Specific
- Validated eCTD / Submissions Application
- Validated Archive Repository
- Put on Global Function Fileshare (not limited to authorised study personnel) between the File Upload and eCTD tool AND between eCTD and Archive
- Automated Synchronisation (Push / Pull)

Holistic Overview

- Where is the ‘single source of truth’
- How is data moved between systems
- How does access and security profiles for data change as the data moves
- This should map / align with the Clinical Process Model (see GAMP GPG)
- Does the system support / enforce the process
- Where is data captured, transferred, processed
  - Clinical Sites
  - CROs
  - Laboratories
  - Virtualisation / Decentralisation

Workshop 2 – Scenario Reminder

- Phase II Double Blind, Multicenter Study to evaluate MakeMeBetter compared to GrannyRecommends for brain cancer
- Primary End-Point – Progression-free survival (PFS) defined as the time interval form Randomisation until tumour progress according to RECIST
- Secondary End-Point – QoL based on fatigue and pain scores based on weekly at home completion via ePRO device and reviewed by Site Staff during visits
- Study and Data Management outsourced to a CRO with a 3rd part EDC system
- Centralised Medical Imaging for Tumour analysis
- eCOA solution provider
- Central & PK Laboratory
- IRT / IMP distribution provider
- Sites in EU, UK, and North Africa

Workshop 2 – Audit / Monitoring Strategy

How does the Data Architecture and Data Flow impact your audit strategy?

- Which Systems / Vendors do you want audited?
- What type of Audit? (e.g. Vendor, System, Trial-Based)?
- Are there specific additions to Site Audits / Monitoring Plans connected to the systems?

Day 3 Summary

- The definition of a system allows for interpretation
- A cohesive IT/CSV Strategy needs to understand both Technical AND Business Risks
- CONTEXT - Technological Approaches that are Right for one Study / Programme does not mean it is right for another