



*Setting the Standard for Automation™*

# Preparing for a Data Integrity (DI) audit

Garry Wright

European Laboratory Compliance Specialist

Agilent Technologies

[garry.wright@agilent.com](mailto:garry.wright@agilent.com)

Standards  
Certification  
Education & Training  
Publishing  
Conferences & Exhibits

# Garry Wright

## European Laboratory Compliance Specialist



- 20 years of experience within an FDA / MHRA approved GMP based CMO / CRO.
- Held Laboratory Management position for last 10 years.
- Specialist interest in Instrument Management / Qualification, Compliance, GMP training and Auditing.
- First hand experience of Data Integrity (DI) audits from FDA, MHRA and Consultant auditors.
- Joined Agilent on 1<sup>st</sup> September 2015.



# New Approach to Audit

- Focus - **Potential for fraudulent activity** within your quality systems.
- Assumption - **Fraudulent activity is taking place** if they identify weaknesses in your quality systems.
- “Guilty until proven innocent” approach to auditing!
- “Data to good to be true!”.



- Electronic data (Meta data) is - preferred choice for regulatory authorities as this is the original (“official”) data.
- Meta data = data about data.
- Meta data is dynamic and can be queried / searched / trended.
- There is a much higher probability of identifying fraudulent activity within an organisation if Meta data is reviewed.
- Hard copy (Flat data – printed, pdf, photocopy) is no longer considered to be acceptable by regulatory authorities as this data is not complete and not original.
- If you state that **paper is your original raw data** in your internal procedures this will **alert an auditor** that you are **probably not managing and reviewing electronic (meta) data**.

# Key Data Integrity (DI) Questions?



- 5 key Data Integrity (DI) questions:
  - Is electronic data available?
  - Is electronic data reviewed?
  - Is meta data (audit trails) reviewed regularly?
  - Are there clear segregation of duties?
  - Has the system been validated for its intended use?
- The answers to the above questions will determine whether companies are in compliance with 21 CFR part 11 (Electronic records and signatures).
- Leave the Original Meta data in the CDS and review / approval electronically to avoid increased Data Integrity risk (the paperless lab).



- Audit Strategy:
  - Starts with a **specific result (or record)**.
  - Re-create the sequence of events that occurred at the time the result (or record) was generated **using the electronic (meta) data**.
- The auditor will want to know:
  - **WHO** performed the analysis?
  - **WHAT** equipment was used to perform the analysis?
  - **WHEN** the analysis was performed?
  - **WHY** the analysis was performed?
  - **WHERE** the electronic (meta) data is stored?
- **Answers to the above may lead to more detailed questioning / inspection.**

- The auditor will expect a suite of SOP's to be in place to support Data Integrity and minimise risk within your company.
- Examples of typical SOP's include:
  - IT policies.
  - System administration (CDS access, roles and privileges).
  - Data management and storage.
  - Data acquisition and processing.
  - Data review and approval.
  - Data archiving and back-up.

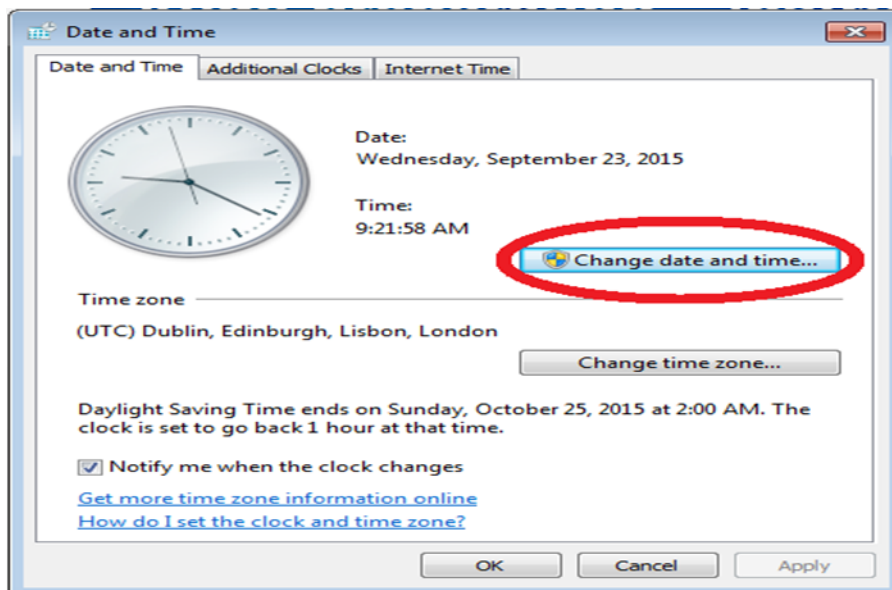


- Server room:
  - The room is secure.
  - IT access only.
  - Tidy and in good working order.
  - Has back-up and disaster recovery procedures in place.
  - Date/time functionality of servers are correct.





- The auditor will select a number of instrument controlling PC's within the lab and check:
  - Date/time functionality is correct.
  - Date/time cannot be changed by the lab personnel.



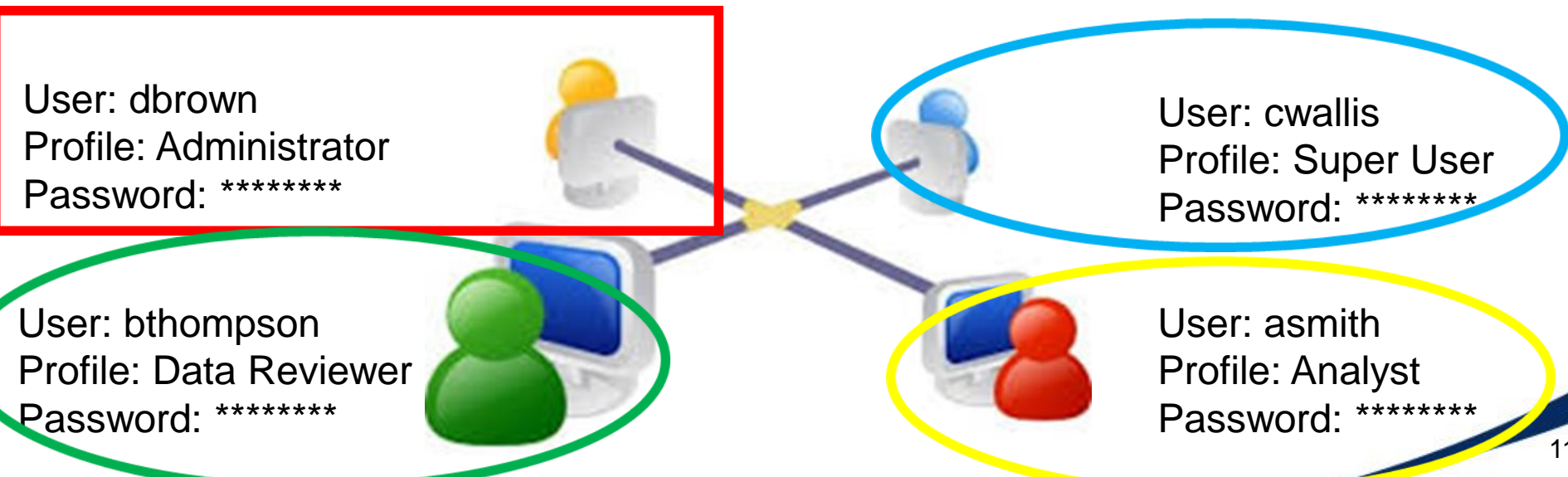
*Confirm that date/time functionality on all PC's within the lab is locked down and can only be changed by IT personnel with Administration privileges.*

- The auditor will want to understand how **access** to the Chromatography Data System (CDS) is **authorised and controlled**.
- You will need to **justify the access levels** within the CDS **and the user privileges** at each level.

## User-Access



- Specific user profiles and passwords required to access instrument software and provide audit trail traceability.
- Administration control should be independent of Analytical function to eliminate conflict of interest.
- Clear segregation of duties with no overlap of privileges.



- Reinforce – DO NOT SHARE PASSWORDS.
- Password policies - changed on a regular basis to protect your profile.
- Password strength - mix of alpha numeric characters and have a high strength.
- User policies - need to log-off the CDS immediately after use to avoid profile potentially being used by other personnel to acquire, process or manipulate data.
- User profiles - set to auto-lock after a period of inactivity to protect the user profile and data within the CDS.

A screenshot of a web-based password change form. It includes fields for "Current:" (masked with dots), "New:" (masked with dots), and "Re-type new:" (masked with dots). Below the "New:" field, it says "Password strength: Strong" in green. Below the "Re-type new:" field, it says "Passwords match" in green. At the bottom, there are "Save Changes" and "Cancel" buttons.

- The regulatory auditor will want to confirm that the **Audit Trail functionality is switched ON** within the CDS Admin console.



- The regulatory auditor may ask for Administration reports:
  - Active users
  - User privileges
  - Administration audit trail report





- Specific privileges within the **user** profile:
- They will want **assurance that data cannot be deleted** by a user once acquired.
- They will want to know if data can be moved to a different folder to potentially “**hide**” it. (e.g. **trial injections**).





- They will want to see that electronic data that has been processed **must be saved** before it can be submitted for review (or printed to hard copy).

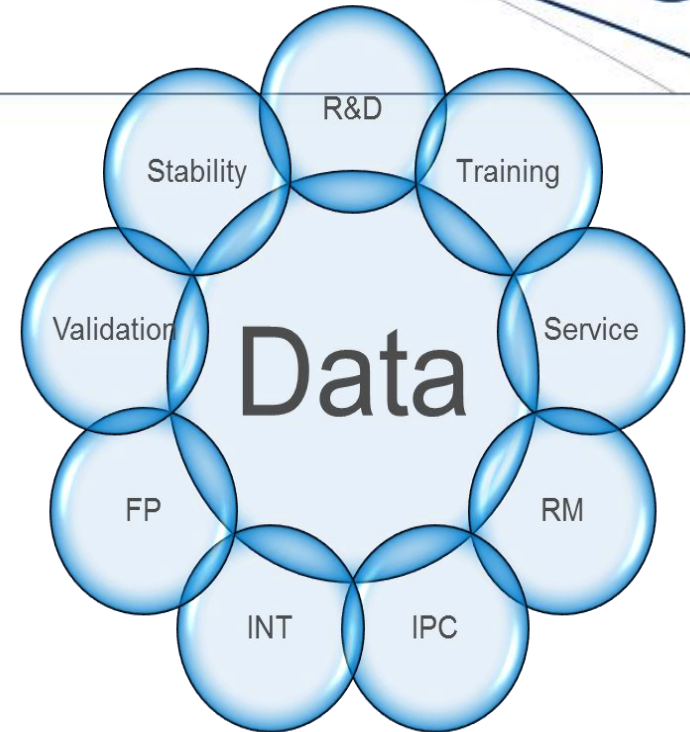


*Make sure you understand the privileges applied to each user profile and be prepared to justify to the regulatory auditor.*

# Data Management

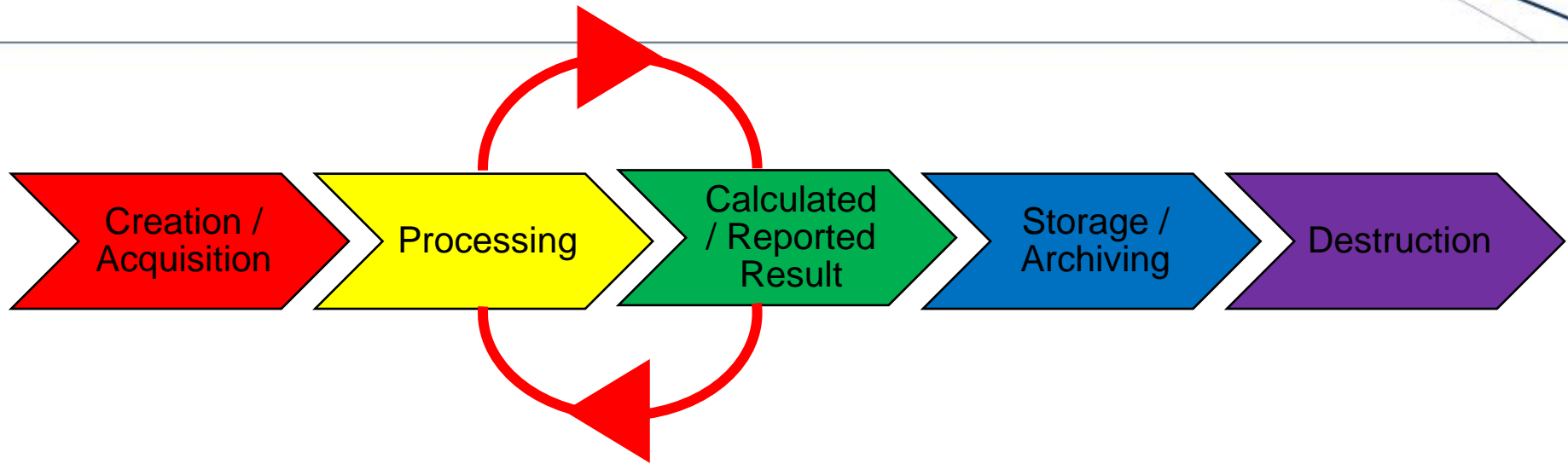
- Consider **what types of data you produce** and decide how **each type of data should be stored** within the CDS.
- **Define a data management structure** that **segregates different types of data** and enables easy retrieval during the audit.
- **Segregate GMP release data** is from **Research / Development data** if you have dual functionality within your organisation using the same CDS / Server.

*Good data management - will give the auditor confidence that you have control over your electronic (meta) data and will increase retrieval speed during the audit*



- **Periodic GMP data archiving** – make sure that data archiving is defined in your procedure and performed regularly.
- This approach **minimises the amount of “live” data** that can be accessed by users and potentially reprocessed to change previously reported results.
- The users should not have access to archive folder(s) which **adds an additional layer of protection to the electronic data.**



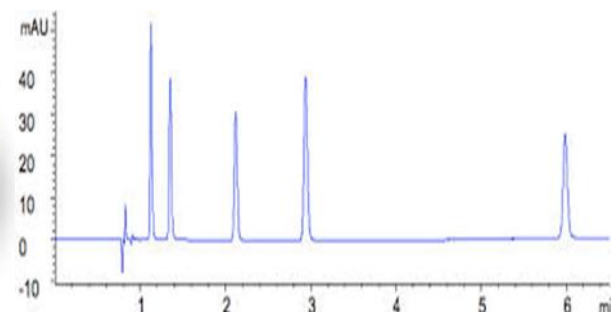


- **Data Processing Risks:**
  - Main area where results can be manipulated by human intervention.
  - Target area for auditors.
  - Controlled by procedures, user access and locked methods.
  - Avoid multiple reprocessing (if possible)!

- All data processing **should be performed within the CDS** for system suitability and batch results wherever possible.
- Move away from using validated excel spreadsheets (no longer meta data).
- For commercial release testing the auditor will **expect processing methods to be validated and locked** by the administrator.



- **Save all changes** to individual chromatograms, sequences and processing methods before submitting for review.



- Ensure that **accurate audit trail comments** are entered into the CDS when prompted to provide traceability.

Audit Trail Comment








dhsjdhsjjsjdksd

Audit Trail Comment

Integration parameters  
updated



# Auditor Checklist

- Administration control. 
- Individual user profiles and passwords. 
- Clear segregation of duties within user profiles. 
- Restricted privileges for user (cant delete / over-write / move). 
- Audit trail functionality switched ON. 
- Date / time functionality locked by IT. 
- Lab Demo – User log-on (multiple), date / time locked, cant delete data. 

# Auditor Checklist



- Data recall – Electronic sequence / data file recall in lab using staff member. **Data recall needs to be fast and efficient.**
- Data review – Chromatography scaling, integration and electronic results.
- Audit trail review – looking for suspicious activity, justification of processing.
- Training – assess staff competency with CDS in lab. Make sure staff are trained to interact with the auditor. **Have a CDS super-user present during the lab inspection.**
- Query search –assurance that batch hasn't been analysed multiple times as part of an investigation.
- Final electronic results in CDS match those reported on C of A.



FDA / MHRA inspectors have been trained by Data Integrity and CDS experts!

They have detailed knowledge of your CDS and know where to find the meta data to identify if fraudulent activity has taken place!

Thank you for  
your attention.

