GBAGROUP

Laboratory Analysis and Services for

ENVIRONMENT · FOOD · PHARMA

Welcome and Introduction

- About me:

- Peter Bäuerle working at GBA Pharma ULM
- Master Craftsman
- Bachelor of Engineering
- Data Integrity Expert
- Computer System Validation Expert
- Python, C/C++, Java, SQL, Go, Rust

Welcome and Introduction

- About us:
- GBA Group, founded in 1989, is one of Europe's leading laboratory service providers and offers an international network of companies with highly qualified specialists for customers in the Pharma, Food and Environment sectors.
- In GBA GROUP PHARMA we cover the entire value chain of drug development:
  - Preclinical Services (Pharmacelsus)
  - Clinical Trial Supply (ABF)
  - Phase I-IV Studies (LKF)
  - GxP Testing (Pharma Labs). In Ulm we do:
    - Routine analytics and validation
    - Raw material and finished drug testing
    - As well as packacking testing with ZwickRoell testing Machines

Introduction

- Why discuss user rights in software under GxP?
  - Every user needs rights, but not all needs are right.
  - The shortcut to GxP:
    - Say what you do.
    - Do what you say.
    - What's not written are rumours.
- Please take into account the requirements of 21 CFR Part 11 and EU GMP Annex 11 in your actions. A total of 10 pages of text, around 4750 words, covering comprehensive content. Also consider ALCOA+ principle.
- This talk will provide practical insights into real-life experiences, offering examples of effective and other approaches to user groups and rights during system validation. It scratches the surface of *attributable* from ALCOA+.

Introduction

- Despite the fact that there are software systems out there that lack even the basic functionality of user groups, the first rule of GxP still generates a significant workload.
- Validating a new computer system necessitates a well-defined plan to:
  - Validate the computer itself
  - Validate the software installation
  - Validate all data connections used by the software.
  - Validate the points not covered by the manufacturer's validation steps.
  - Define your user rights and groups prior to installation.
    - Sometimes just by reading the manual.
    - Other times, it requires using a demo version of the software, potentially with an active CFR21 module. If you get one.

Introduction

- Last year we validated six new computer systems.
- Including two self written support-software for data exchange between Lab equipment and LIMS.
- Each validation process produces between 70 and 125 pages of documentation due to documentation requirements and planning. Depending on how you read the current GAMP 5, additional pages quickly fill up.
- Added to this, is the manufacturer’s, sometimes excellent, documentation. Which runs between 10 and 550 pages. A little isn't always bad and a lot doesn't always help either.
- Before you can start a validation this information has to be read, understood and linked together.

User Rights and User Groups

- To meet regulatory requirements, user rights are essential.
  - In an ideal world, nobody makes mistakes, and nobody has evil intentions.
    - Unfortunately, even kids try to cheat to get a cookie.
  - Empower users to make fewer mistakes.
  - Eliminate the chance to cheat.
- A collection of rights forms a group.
  - There should only be four types of users:

Administrators	Developers
Viewers	Users

  - And perhaps Support
  - And Supervisors And Service

User Rights and User Groups

Administrators	Developers
Viewers	Users

- These four groups are usually enough, but this is the ideal scenario.
- A set of rights should be curated into a group by the company utilizing the software, rather than by the software developers.
  - There is a software from a UV spectrographic supplier with predefined groups.
    - One group cannot measure or open any measurements.
    - One group can only perform measurements without modifying templates or generating reports.
    - One group can perform almost all actions, except user management.
    - One group can perform all actions.
- Changing rights within these groups is not permitted.

User Rights and User Groups

- Some examples of rights include:
  - Manage new and existing users.
  - Manage the database and/or file handling.
  - Create templates for new measurements.
  - Configuring report settings.
  - Opening a template.
  - Opening a measurement.
  - Create a measurement
  - Print a report
  - Digitally signing documents for creation, approval, and review.
  - …

User Rights and User Groups

- How many rights are necessary?
  - There is software from a testing machine that provides you the right to set all rights.
  - ALL RIGHT!
    - Is the user allowed to use the help menu?
      - Can the user select the help option within the help menu?
        - Can the user utilize the index and content of the selected help?
        - Can the user access the About information?
        - …
  - Listing all the possible rights you can configure requires approximately 10 pages and encompasses around 300 rights.

User Rights and User Groups

- Please maintain consistency and avoid mixing up
  - Another old friend, a software for qPCR that comes from research and is now available under GxP, provides three fixed user groups.
  - Each group possesses predetermined rights; some are allowed or denied, while a few are left for personal choice.
  - An Administrator has the predetermined right to "modify or create users"
  - For a Supervisor, this is optional.
    - A Supervisor can employ an electronic signature if permitted.
      - However, this is only possible if the "modify or create users" right is enabled.
        - But, the supervisor is not able to modify or create users with this right, as the name suggests.
- Dear diary, I await the first audit with this system longingly.

Login and Credentials

- A user should be identified by their credentials.
- Usually, this involves a username and password.
- Or:
  - A User-ID from an ever-expanding list displayed upon program startup.
  - A personal USB stick created only by the microwave-manufacturer.
- How often should a user be prompted for their credentials?
- Passwords should be regularly updated.
- Passwords should not be easily guessed.

Login and Credentials

- There was once a software, for a quantitative SDS gel analyzer with camera
- 21 CFR § 11.300 Controls for identification codes/passwords: (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
- Using the same password is not allowed,
  - Not even for another user…
- The concept is simple: allow a limited number of guesses for a forgotten password before the user is locked out. Perhaps a maximum of 5 guesses is reasonable.
- Yet, the reality with this software is different: You can change your password as often as you want. Initially, it seems fine. However, the system alerts you when your new password is already in use. This opens the door to checking every user with just one attempt until you find the owner of the password.
- This is far from acceptable.

How Often Should a User Be Prompted for Credentials?

- Ever heard about ABS?
  - Action-Based Security! By a TOC analyser.
- Consider a software that can be executed by anyone with access to the computer.
- You can open a measurement, a template, or even create a new one without being prompted for a username or password.
- But if you decide to print a report, save a setting, initiate a measurement, or perform the mandatory daily water-check, you will be asked for your username and password. Every time you save. Every time you print. Every time you modify something, you will be prompted for your username and password.
- In the upcoming version, the technician proudly claimed, the last username will be remembered.
- During the validation process, he ended up typing his username and password a staggering 400 times…

Are Usernames and Passwords Enough?

- Don‘t overcomplicate! Usernames and passwords suffice in most cases.
- Alternatively, you can employ a designated user authentication system like Microsoft Active Directory (AD).
- Unfortunately, there aren't any cheering tales of successful AD misuse.
  - However, certain quirks persist:
    - Some systems automatically use the already logged-in user without requesting additional credentials.
    - Others don't even attempt to retrieve information about the active user.
    - Certain systems don't permit browsing the AD structure to locate a user by name.
- And yet you can cleverly combine these quirks with some known prior bugs to ruin your software in a big way.

How to Store Data?

- Perhaps the optimal solution is adopting a database-like structure for comprehensive data persistence.
- As an alternative, a file-based structure is maybe a secondary choice.

- There was a software for SDS from not too long ago, afflicted with a bipolar disorder.
  - In part one, it captures images from the instrument and stores them in a file folder.
    - This is necessary because this task can only be left to the user for security and data integrity reasons.
  - Part two performs calculations and requires loading images, storing them in a secure, server-sided, database-like folder.
    - This is necessary because it is not possible to leave this task to the user due to security and data integrity.

How to Store Data?

- Another software for a TOC analyzer utilizes a fully-fledged Microsoft SQL Server.
  - However, this isn't provided by the software manufacturer; you need to leverage your independent installation, as indicated in the manual. Yet, this isn't too concerning since you can use your existing substantial SQL Server structure more efficient.
    - Oddly, the installer attempts to install a free SQL Express version.
  - You're advised to establish a admin-user within the database for the software.
  - For this user, the password "softwarename2019" is required.
    - The database password is hard-coded. This detail is explicitly stated in the manual, conveniently available on our website for all to access…
- Remember: Nothing is more descriptive than a manual.

Conclusion

- In summary, the complexities of user rights, credentials and data storage in software systems subject to GxP regulations are extremely important and profound.
- Planning and managing these aspects in a clear manner is not only a legal obligation, but a crucial step in ensuring data integrity, security and compliance standards.
- Understanding the intricacies and challenges of validation related to user management, authentication and data storage can greatly improve a software system's reliability and alignment with GxP principles.

GBAGROUP

Laboratory Analysis and Services for

ENVIRONMENT · FOOD · PHARMA