C191-E048

SHIMADZU
Excellence in Science

Technical Report

Practical Procedures for Compliance with Data Integrity Requirements in Analytical Laboratories

Mamoru Kikumoto[1]

Abstract:

A recent topic related to analytical data is the lack of data integrity, due to data modification or replacement, for example. Implementing measures to ensure data integrity has become an urgent issue at analytical laboratories, but in many cases, difficulty in gaining an overall understanding of data integrity has resulted in indecision on how to proceed. Therefore, this report describes practical procedures for ensuring the data integrity for analytical instruments.

Keywords: Data integrity

1. User Roles and Responsibilities for Analytical Instruments

Compliance with data integrity requirements is a pressing issue for companies that are required to comply with GxP compliance. However, according a warning letter [1)] from the U.S. Food and Drug Administration (FDA), data integrity requires not only restricting access to laboratory analytical instruments, but also assigning user rights to analytical laboratory personnel. (Refer to the excerpt below.)

In response to this letter:

- provide a summary of your interim controls to prevent deletion and modification of data;
- define the roles and responsibilities of personnel who have access to analytical instruments and data;
- detail the associated user rights for each analytical system;
- provide a detailed summary of your procedural updates and associated training for user role assignment and controls;

2. Procedure for Assigning User Rights to Users

A typical procedure for assigning user rights is shown in Fig. 1. It shows how first (1) user rights groups are created and then (2) rights are assigned to each rights group. Next (3) users are registered and then (4) assigned to rights groups. Consequently, (5) users were successfully assigned specific user rights.

The important point, as indicated in the warning letter above, is to specify who is assigned what rights (and who is assigned to which rights group). That is because assigning inappropriate user rights creates a risk that inappropriate operations might be performed.

In that case, what measures should be taken to ensure appropriate rights are assigned to appropriate users?

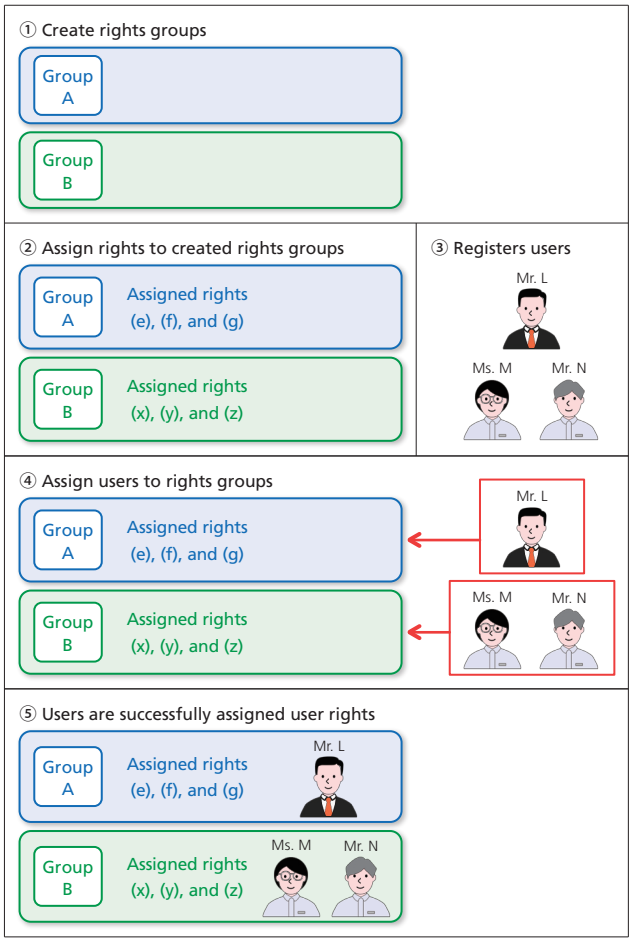

Fig. 1 Procedure for Assigning User Rights to Users

1 Analytical & Measuring Instruments Division

3. Visualizing the Workflow Using a Flow Chart

The following describes how to visualize the workflow by creating a flow chart of computer processes involved in specifying appropriate user rights settings. To make it easier to understand, this example is limited to the workflow extending from LC analysis to data approval. (Refer to Fig. 2.)

Fig. 3 shows an example of the recommended workflow involved in using LabSolutions DB/CS software. (LabSolutions DB software is used on a standalone basis, whereas LabSolutions CS is used via a network.)

In this case, the workflow is described starting with the process of specifying user rights groups, so that the overall workflow can be considered. A user rights group is like a job title, whereas a user rights group is a certain group of users that has been assigned various roles, or in other words "user rights," involved in computer work processes. Fig. 3 shows five proposed user rights groups, numbered from I to V.

It is important to confirm that user rights assignments to user rights groups are appropriate, in terms of data integrity, as the assignment process proceeds. For example, is there an excessive concentration of rights assigned to test managers? Do operators have more rights than they need? Are any users with job titles generally never involved in actually performing analysis assigned the rights for executing analyses? Ask these and other questions.

For the workflow example in Fig. 3, LabSolutions DB/CS report set functionality is used to approve data (and metadata). A report set consists of a packaged set of all information necessary for reviewing data (and metadata). Report sets are created by simply right-clicking the applicable batch file (a sequence file used to execute a continuous series of analyses) and then clicking [Create Report Set] on the right-click menu that is displayed, as shown in Fig. 4. For more details, refer to the Technical Reports [2), 3)] indicated in the References section at the end of the article.

Regarding the concepts of system owners and process owners in Fig. 3, GAMP 5 [4)] is used as reference. GAMP 5 is a material published by ISPE. GAMP 5 is known as a global standard reference document for computer system validation (CSV).

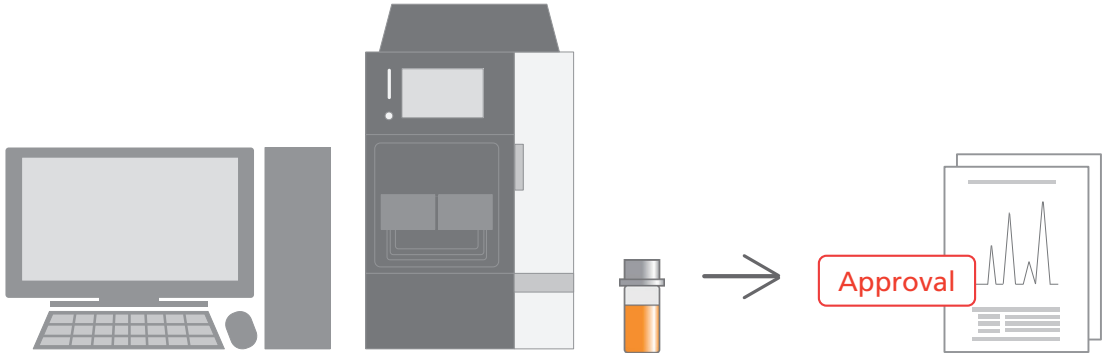

Fig. 2 LC Analysis and Data Approval

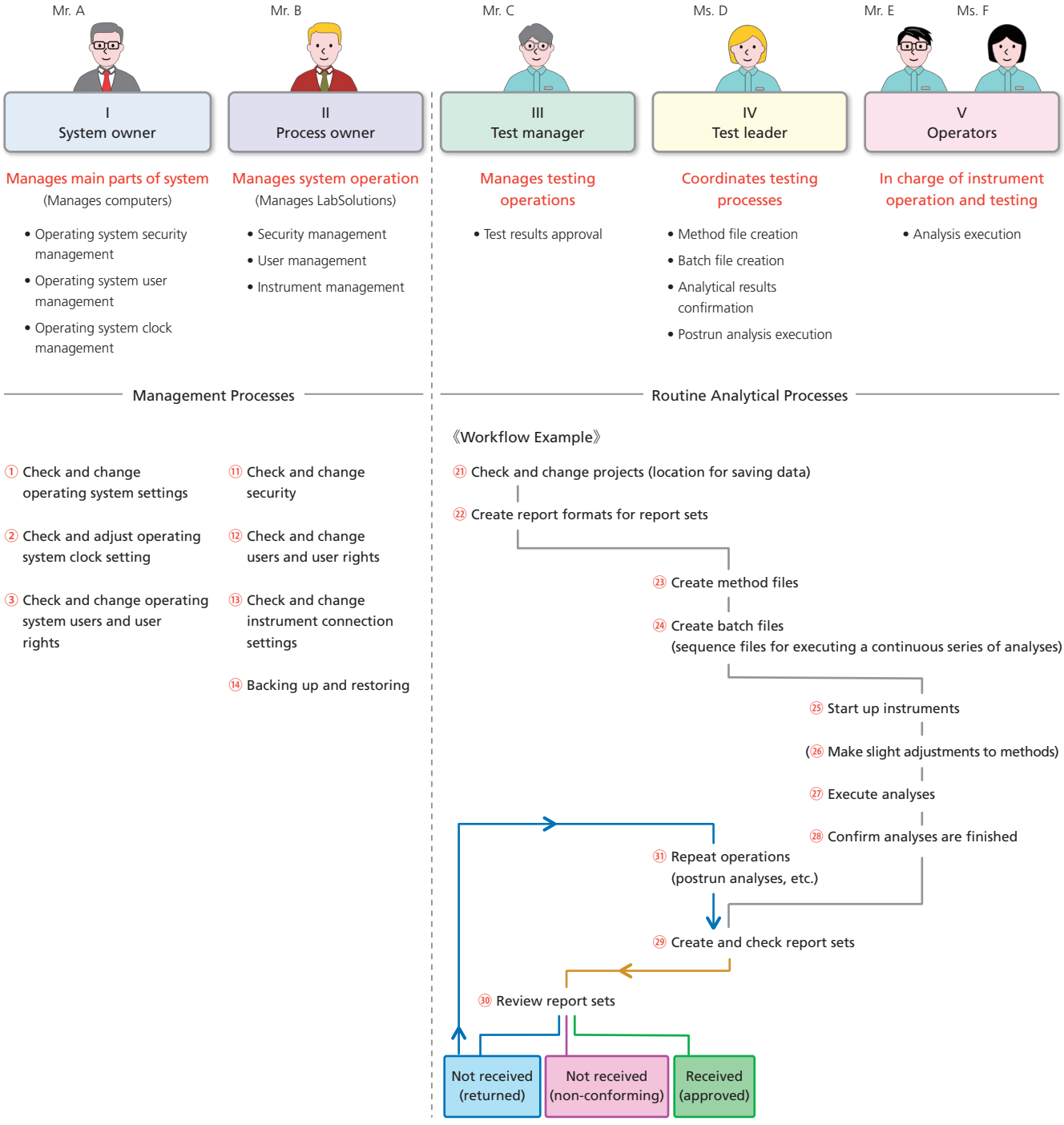

Fig. 3 Example of User Rights Groups and Workflow Recommended in Using LabSolutions DB/CS

4. Main Roles of User Rights Groups

When a flow chart is created based on Fig. 3, write out the main roles of each user rights group as shown in Fig. 5. The main roles are written out so that they can be checked for any inappropriately assigned rights that were not visible in the flow chart. The process also enables the roles of each rights group to be clearly identified.

In this case, for example, it indicates that the role of test managers is to review (approve, indicate non-conformity, or reject) test results, but not to create method files or perform analyses. Similarly, test leaders create method files and batch files (sequence files for executing a continuous series of analyses) or perform postrun analyses, as instructed by the test manager, but not perform analysis.

On the other hand, the role of operators is to perform analyses, so they are not assigned all rights for changing methods. Rather, they are only assigned rights for making slight adjustments to methods, such as changing the solvent delivery pump flowrate in accordance with the Japanese Pharmacopoeia.

In this way, creating the flow chart in Fig. 3 and listing the main roles of user rights groups in Fig. 5 help ensure a workflow with no inconsistencies in terms of data integrity.

Next, create documentation of user rights settings based on that confirmed workflow. When that is finished, apply the settings to operating system (Windows) and LabSolutions DB/CS settings.

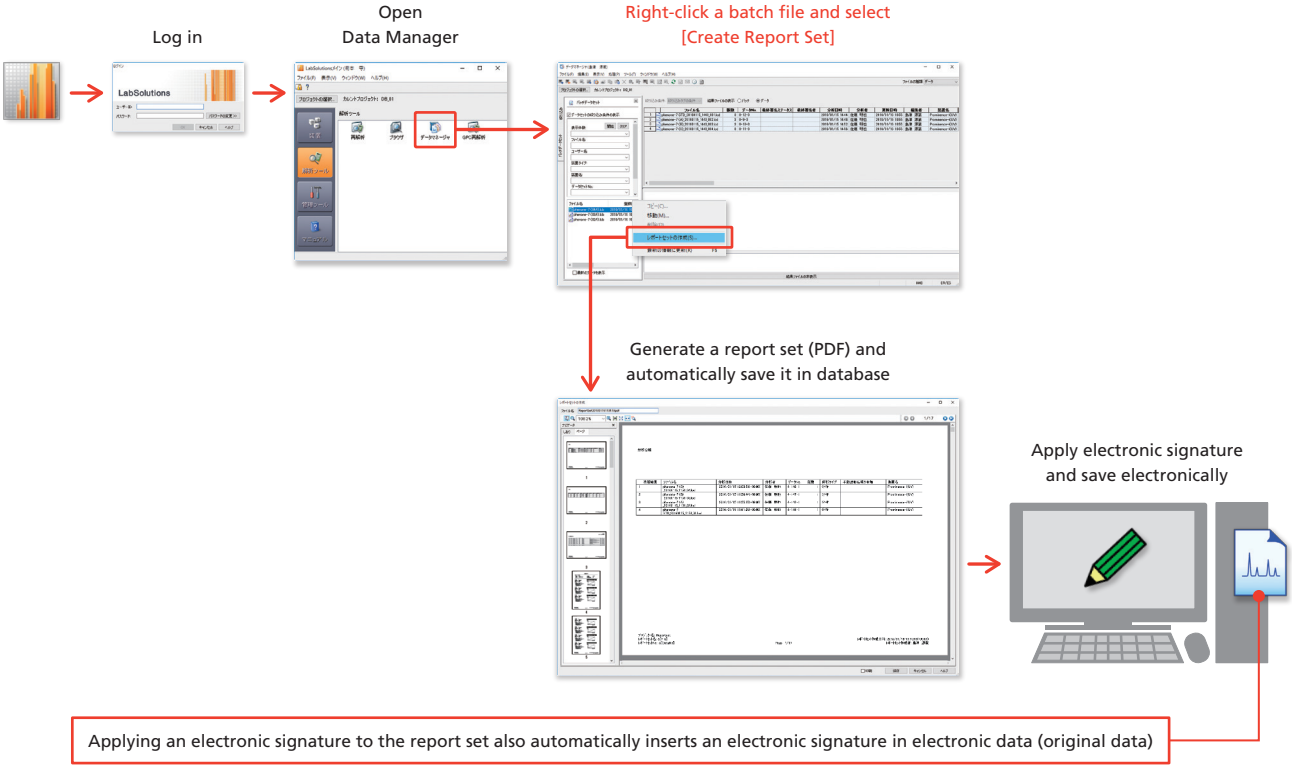

Fig. 4 Procedure for Creating a Report Set Using LabSolutions DB/CS

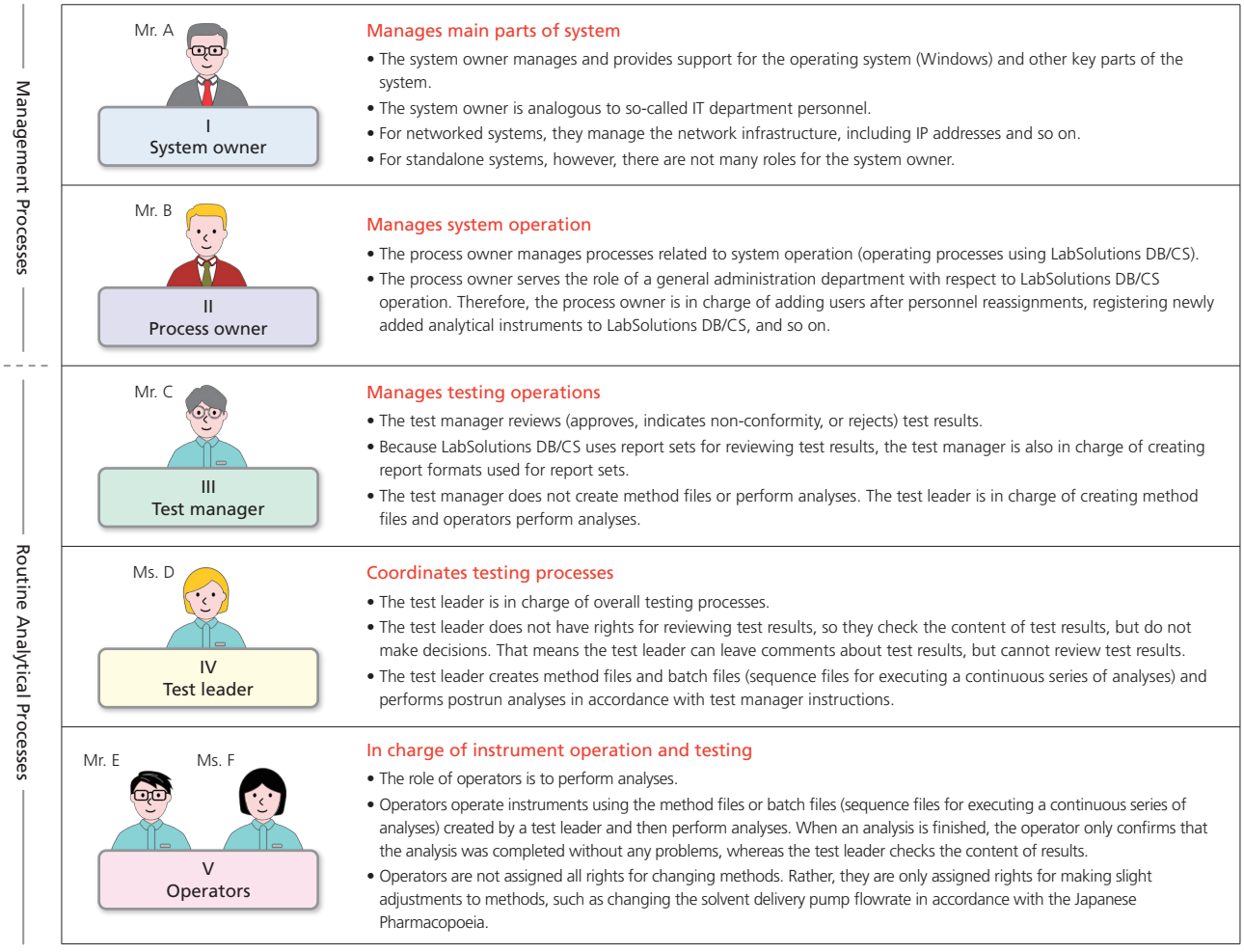

Fig. 5 Main Roles of User Rights Groups Recommended by LabSolutions DB/CS

5. Deploying User Rights for Other Instrument Types

Analytical laboratories use not only LC and GC systems, but also UV, FTIR, ICPMS, and other instrument types. In the case of LabSolutions DB/CS, the user rights specified for LC or GC systems can also be deployed for other types of instruments.

As shown in Fig. 6, user rights are specified as either common settings or instrument-specific settings. Common settings specify user rights settings used for all instrument types. In contrast, instrument-specific settings specify user rights settings for specific instrument types if the rights specified in common settings are not sufficient for that instrument. For example, they can be used as follows.

- Example of user rights with common settings: Rights to add projects
- Example of user rights with instrument-specific settings: Rights to edit methods (pump flowrate)

In this way, user rights settings in LabSolutions DB/CS can be shared, so that user rights settings can be specified based on a unified policy, even if additional standalone systems of a different instrument type are installed or a network is created.

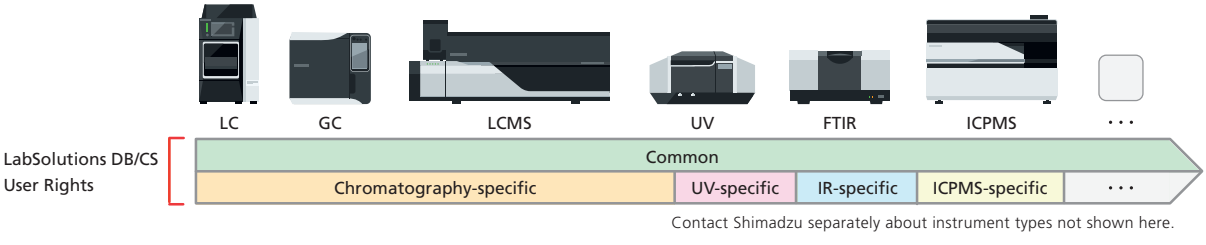

Fig. 6 LabSolutions DB/CS User Rights

6. Recommended User Rights Setting Values

The process of assigning user rights is performed by customers, because it depends significantly on the content and organization of the customer's business. However, if a customer finds it difficult to specify appropriate settings, Shimadzu now offers a paid assistance service, which is available by contacting Shimadzu as necessary. Paid assistance service from Shimadzu (Access) will also continue to be available, as usual, for setting specifications. Now paid assistance will be available for user rights settings as well. (Refer to Fig. 7.)

Recommended setting values for specifications (security policy)

No.	Item	Default Setting	Recommended Setting	Release after setting	Additional setting in Project
1	Administrate the version of data files	■	■	×	—
2	Administrate the version of method, batch, report format files	□	□	×	○
3	Synchronize with the latest version in database when opening files with instrument	□	□	○	○
4	Displayed for confirmation when files synchronize with the latest version in database	■	■	○	○
5	Administrate the version of other files	□	□	×	○
6	Prohibit rollback of files	□	■	○	○
7	Restrict operation of data files	■	■	×	—
8	Prohibit change of data information	■	■	○	○
9	Prohibit changing of files whose result files have not been confirmed	□	□	○	○
10	Prohibit deleting of method, batch and report formats files	■	■	○	○
11	Only use method, batch, and report format files from the database	□	□	○	○
12	Input reason for locking a file	□	■	○	×

Recommended setting values for user rights groups I to V

No.	Rights Name	Rights Group I	II	III	IV	V
1	System Administration	□	■	□	□	□
2	Change System Setting	□	■	□	□	□
3	Change Instrument Setting	□	■	□	□	□
4	Perform Validation Support	□	■	□	□	□
5	Register Manual Log	□	■	■	□	□
6	Edit Print Format (Data Manager)	□	■	■	□	□
7	Edit Print Format (Log Browser)	□	■	■	□	□
8	Add Project	□	□	■	□	□
9	Delete Project	□	■	□	□	□
10	Change Project Settings	□	□	■	□	□
11	Lock Project	□	■	□	□	□
12	Unlock Project	□	■	□	□	□
13	Edit Selection	□	□	■	□	□
14	Backup	□	■	□	□	□
15	Restore	□	■	□	□	□
16	Browse entire log	□	■	■	□	□

Fig. 7 LabSolutions DB/CS Setting Specifications (Security Policy) and Support for Specifying User Rights

References

[1] FDA. "Reine Lifescience 5/9/18". Warning Letter: 320-18-50. May 9, 2018. Note: The excerpt from this document is shown with some parts omitted. https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm607583.htm, (accessed August 1, 2018).

[2] Mamoru Kikumoto. "Data Integrity Compliance Using the LabSolutions Report Set". UHPLC/HPLC, LC/MS Technical Report C191-E041, Shimadzu Corporation. March 2016. http://www.an.shimadzu.co.jp/hplc/prominence/tec.htm, (accessed August 1, 2018).

[3] Mamoru Kikumoto. "Data Integrity Compliance: An Innovative Solution for Molecular Spectroscopy". UHPLC/HPLC, LC/MS Technical Report C101-E149, Shimadzu Corporation. July 2017. http://www.an.shimadzu.co.jp/hplc/prominence/tec.htm, (accessed August 1, 2018).

[4] ISPE. "GAMP Guide: A Risk-Based Approach to Compliant GxP Computerized Systems (GAMP 5)" https://www.ispe.gr.jp/ISPE/07_public/07_01_19.htm, (accessed August 1, 2018).

First Edition: April, 2020

Shimadzu Corporation

www.shimadzu.com/an/

3655-02916-ODPIT