Technical Note

OpenLAB ECM

OpenLAB ECM and Microsoft Excel: Managing Spreadsheets in a Regulated Environment

Introduction

Microsoft Excel is powerful spreadsheet software used by labs for calculations, analytics, and tracking to monitor product quality and improve efficiencies. Due to its flexibility, Microsoft Excel has become popular among scientists and laboratory technicians.

In regulated environments such as the pharmaceutical industry, it is necessary to manage the risks associated with spreadsheets that contain data that are generated during a regulated product's lifecycle. Regulatory requirements such as US FDA 21 CFR Part 11 and EU Annex 11, demand that access control and full traceability of changes (recorded in an audit trail) are applied to spreadsheets containing data regarding regulated products.

Agilent OpenLAB ECM is a secure central data repository deployed by most leading pharmaceutical companies. OpenLAB ECM protects files and metadata from unauthorized modification or deletion. This technical note describes how to control and monitor changes to Microsoft Excel spreadsheets stored in the OpenLAB ECM environment without special modifications or add-on packages. Users can directly access data stored in OpenLAB ECM,

Note: This technical note applies to spreadsheets stored in OpenLAB ECM. It is not for spreadsheets under continuous use or databases.

Agilent

Trusted Answers

Electronic records requirements

To comply with regulatory requirements such as FDA 21 CFR Part 11, spreadsheets containing regulated records must include the following characteristics:

- Access control with various user access levels
- Revision storage and version control
- Secure storage (protection from any unauthorized change or deletion)
- Audit trail for the file, and each of its cells
- Protection of sheet, rows, and cells

In addition, spreadsheets containing regulated records must be:

- Validated to ensure they perform calculations and reports correctly and as intended
- Archived and backed up to ensure they are protected for the required retention time

Overview: OpenLAB ECM with Microsoft Excel spreadsheet compliance

Managing controlled Microsoft Excel spreadsheets with OpenLAB ECM is based on the three building blocks shown in Figure 1. OpenLAB ECM is the foundation that provides a secure repository to store and archive data. User access is restricted by password protection and a fine granularity of user privileges determining who can do what with data. OpenLAB ECM also provides revision control of all files stored within it.

OpenLAB ECM desktop integration allows users to open files and access data in OpenLAB ECM directly from desktop applications such as Microsoft Office.

The Microsoft Excel spreadsheet audit trail captures cell-by-cell changes. Restricted user access to its functionality is available to prevent unauthorized users from changing spreadsheets or parts of spreadsheets.

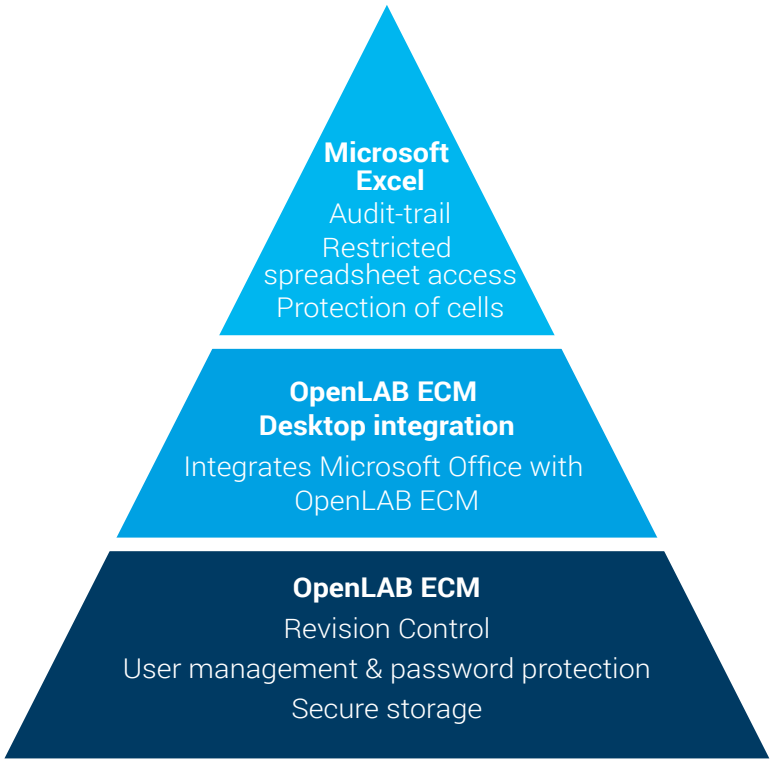

Figure 1: Spreadsheet compliance building blocks.

Configuring Microsoft Excel spreadsheets

Controlling access

Access to templates and data-containing files must be restricted to authorized users. There are two levels of protection for Microsoft Excel spreadsheets stored in OpenLAB ECM: file-level protection in OpenLAB ECM and cell-level protection in Microsoft Excel. As shown in figure 2, Microsoft Excel templates and data-containing files can be protected from unauthorized access and modification by storing them in OpenLAB ECM folders with controlled access. A password is used to allow specific users to develop, modify, and save spreadsheet templates.

To establish ***file-level protection***, set the folder security in OpenLAB ECM as follows:

- For templates under development and validation, set access to be restricted only to authorized developers and not users.
- For released templates, set access to be read-only for all users.
- For folders with data-containing files, set contributor access to the users who perform calculations.

Cell-level protection involves password-protecting cells within the Microsoft Excel file to prevent modification of their contents. Protection must be enabled on all cells that contain formulas, constants, or other data not intended to be modified by users. The Microsoft Excel cell-locking feature prevents users from modifying or deleting values. In addition, when the tab key is used to move between fields, the cursor will only advance to unprotected cells. Data entry fields can be color coded, for example with a green outline, to make them easy for users to locate. When spreadsheet protection is enabled, all cells are protected by default. Only authorized users can unprotect data entry cells.

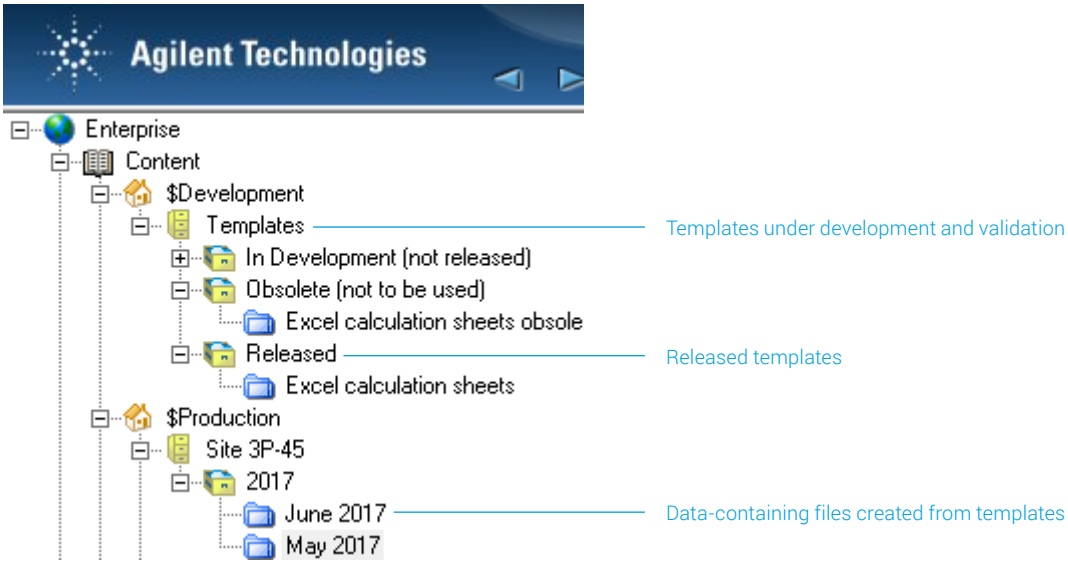

Figure 2. Example OpenLAB ECM folder structure for controlling access to Microsoft Excel files.

Tracking and controlling changes (audit trail)

In addition to actions taken on the spreadsheet file itself, it is important to be able audit the actions taken within the file. Microsoft Excel contains automatic audit trailing called "change history" that is activated using an Excel configuration option. Turning on the audit trail includes setting the audit trail duration. When a spreadsheet template is configured with password-protected access control, users cannot turn off or modify the audit trail.

When the audit trail is enabled, Microsoft Excel requires the user to save the modified file to another folder in OpenLAB ECM with a unique file name, and the audit trail is created. The Microsoft Excel audit trail automatically records all data entered or modified in the new file. Each time the user saves the modified file the audit trial will be updated. The audit trail cannot be modified or deleted by the user. Once saved, the file can be accessed, but not deleted without file-delete permission.

To set up the Microsoft Excel audit trail choose the "Review" tab, click "Share Workbook," choose the "Editing" tab in the pop-up window, and turn on (select) "Allow changes" (Figure 3).

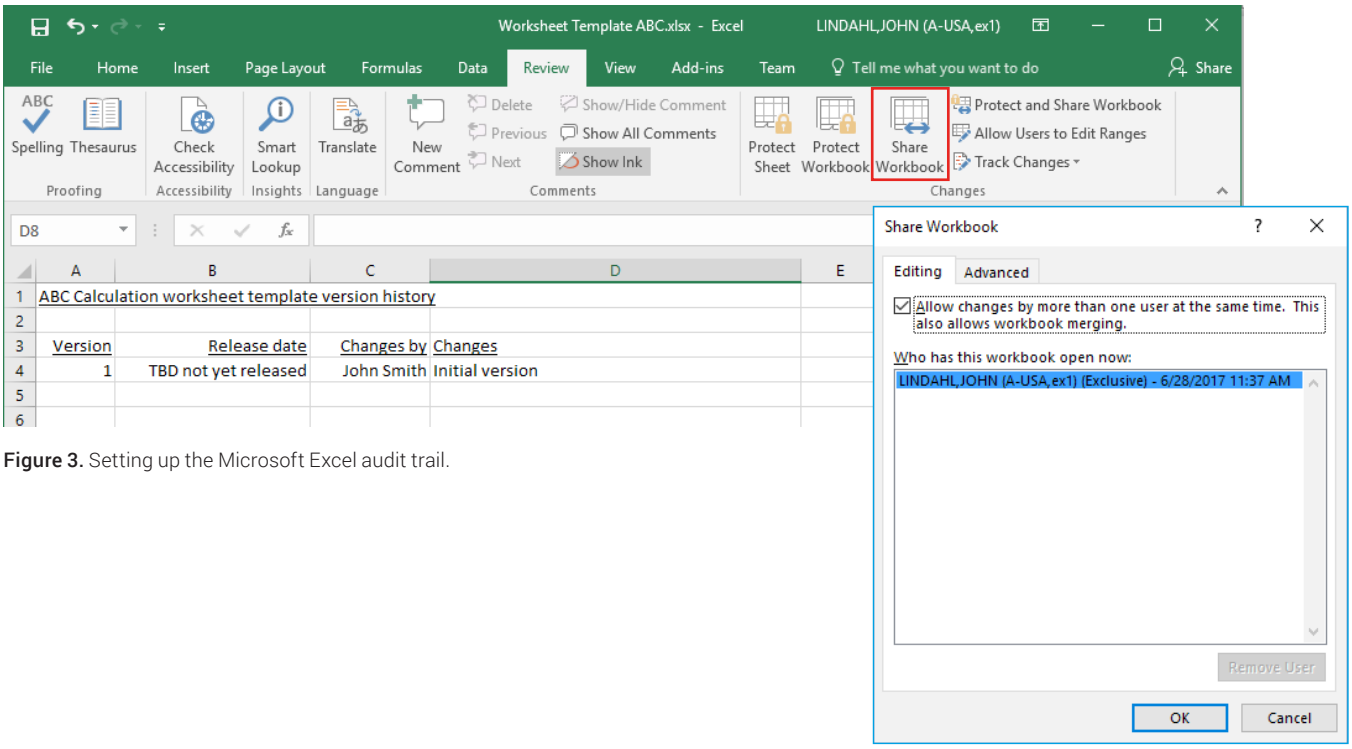

Figure 3. Setting up the Microsoft Excel audit trail.

Next, switch to the "Advanced" tab (Figure 4A). Under the "Track Changes" section, choose "Keep change history for:" and specify 32767 days (which is about 89 years) or other value that best reflects the applicable retention policy. Switch back to the "Editing" tab, and turn off (unselect) "Allow changes…" (Figure 4B). It was only turned on to choose the duration setting.

To complete audit trail setup, choose the "Review" tab, click "Protect and Share Workbook," select "Sharing with track changes," and enter a password (Figure 5).

Tip: Complete configuration of all other spreadsheet functionality and remove any test data before turning on the audit trail.

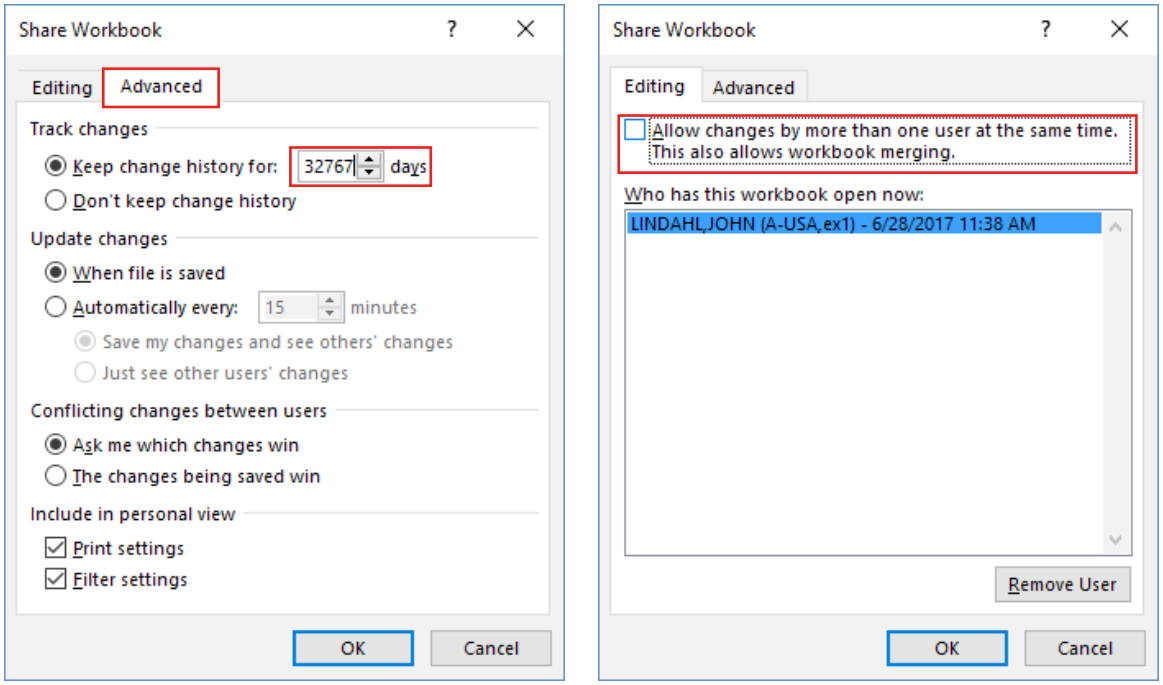

Figure 4A and B. Setting the audit trail duration.

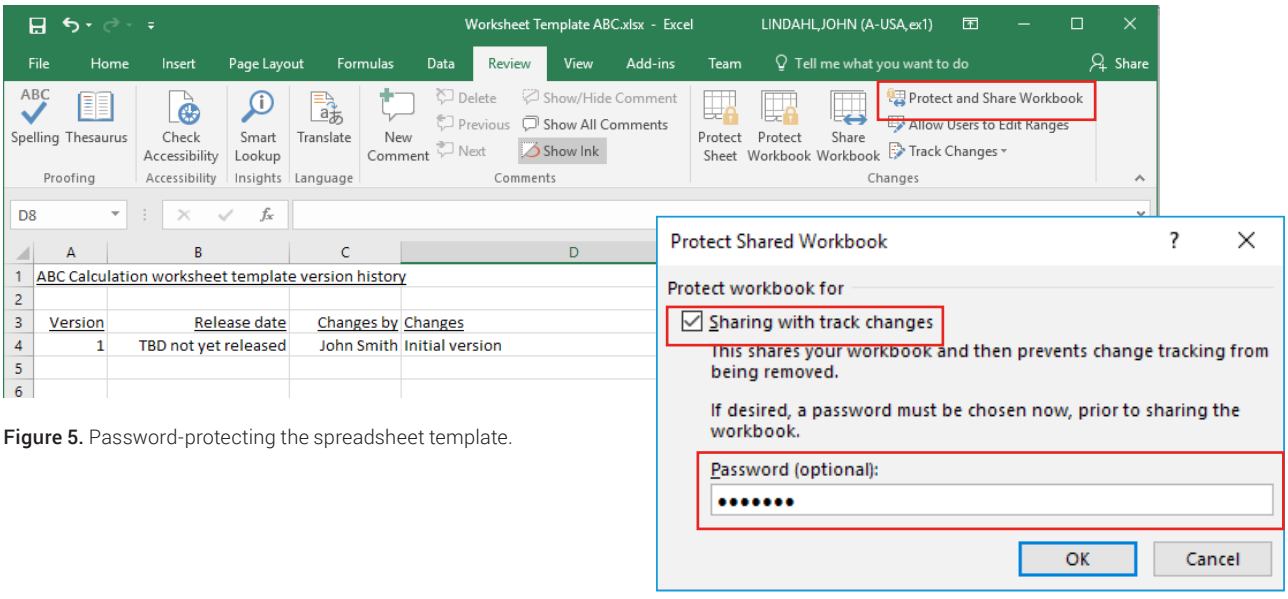

Figure 5. Password-protecting the spreadsheet template.

Creating templates: best practices

Ideally, the spreadsheet template should format data outputs to meet organizational requirements and conventions including significant digits, rounding, units of measure, and warning messages. Outputs can also be formatted with highlights, text colors, or other cosmetic attributes to quickly attract and guide users' attention.

To ensure users use the correct version, the spreadsheet template should contain a version designation that appears on all displays and printed outputs. A version designation is simply text that indicates the name of the spreadsheet template and its version. The version designation is often placed in a protected cell--usually cell A1.

The spreadsheet template should include data entry checks for data entry cells. Data entry checks can restrict the type of data entered to text, numbers, or dates. For easy selection, a drop-down list of pre-established valid entries can be created. For example, a standard list for "Severity" could contain only the values "Major," "Moderate," and "Minor." Another type of data entry check specifies the allowed range of values entered. For example, the data entry could be restricted to a value greater than or equal to 18.

Securing templates

As shown in Figure 6, when the spreadsheet template is ready for use, it must be stored in a secure read-only OpenLAB ECM folder.

Note: The password used to protect spreadsheet templates should not be given to users.

Validating templates

In regulated environments, spreadsheets must be validated for intended use in the same manner as other Commercial/Configurable Off-The-Shelf (COTS) products. Once the validated spreadsheet is in production use, its validated state must be maintained with change control.

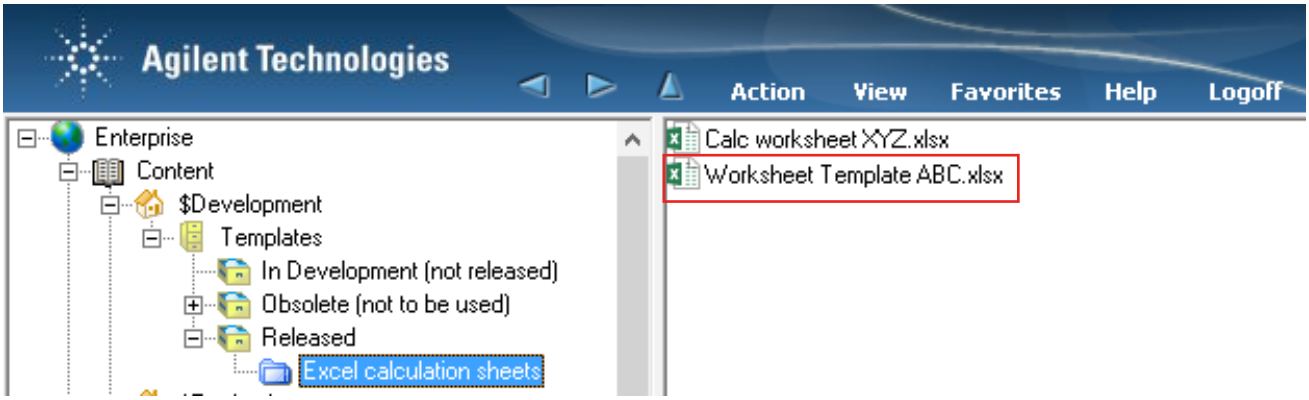

Figure 6. Storing the template in a secure folder in OpenLAB ECM.

Using templates

Users access spreadsheets by opening the template file from the read-only location in OpenLAB ECM (Figure 7).

After entering the required data, the user saves the worksheet to a data folder where the record of the calculation and reason is stored (Figure 8). The saved user file provides an electronic record that contains the application, data, and audit trail.

The spreadsheet can be reviewed and approved via electronic signature using OpenLAB ECM (Figure 9).

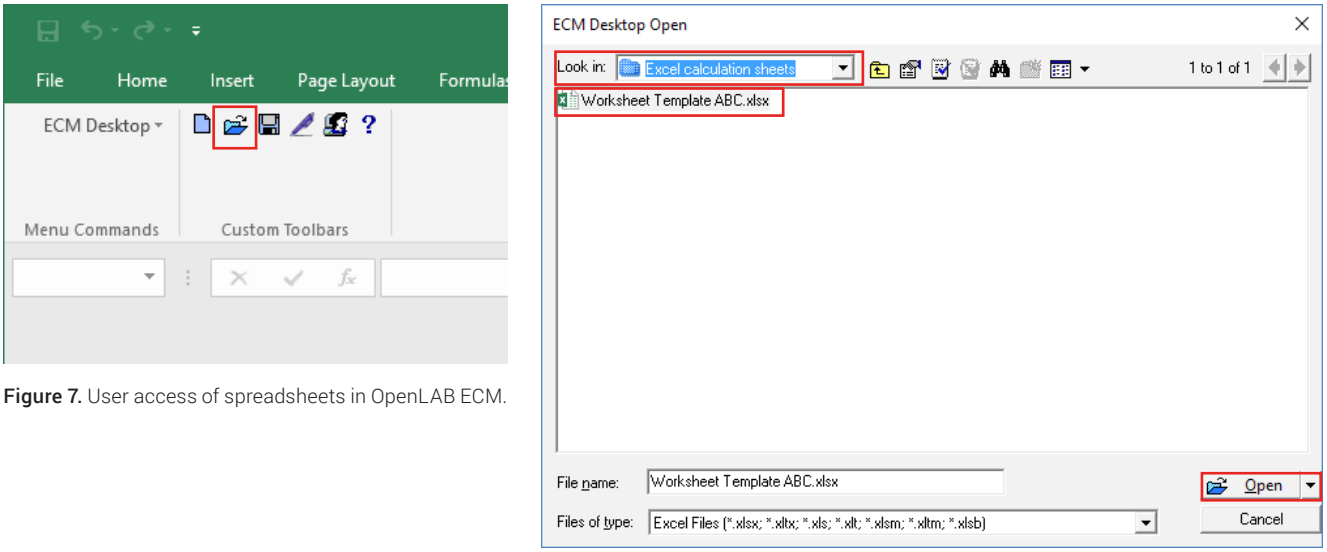

Figure 7. User access of spreadsheets in OpenLAB ECM.

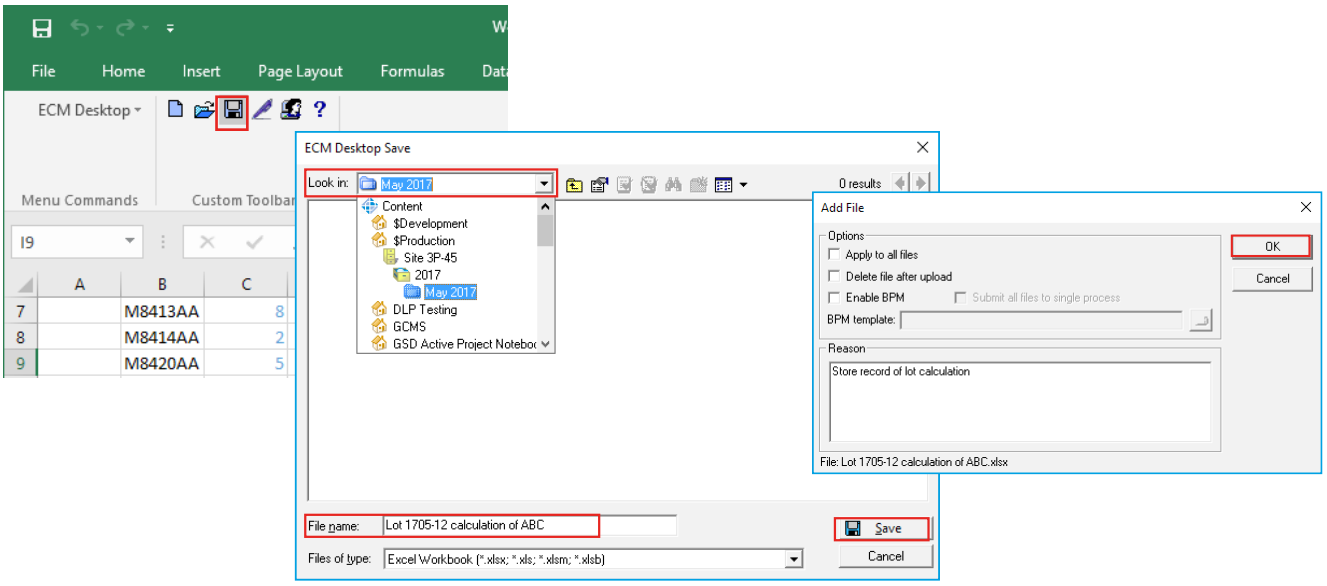

Figure 8. Saving the spreadsheet with the record of the calculation and reason.

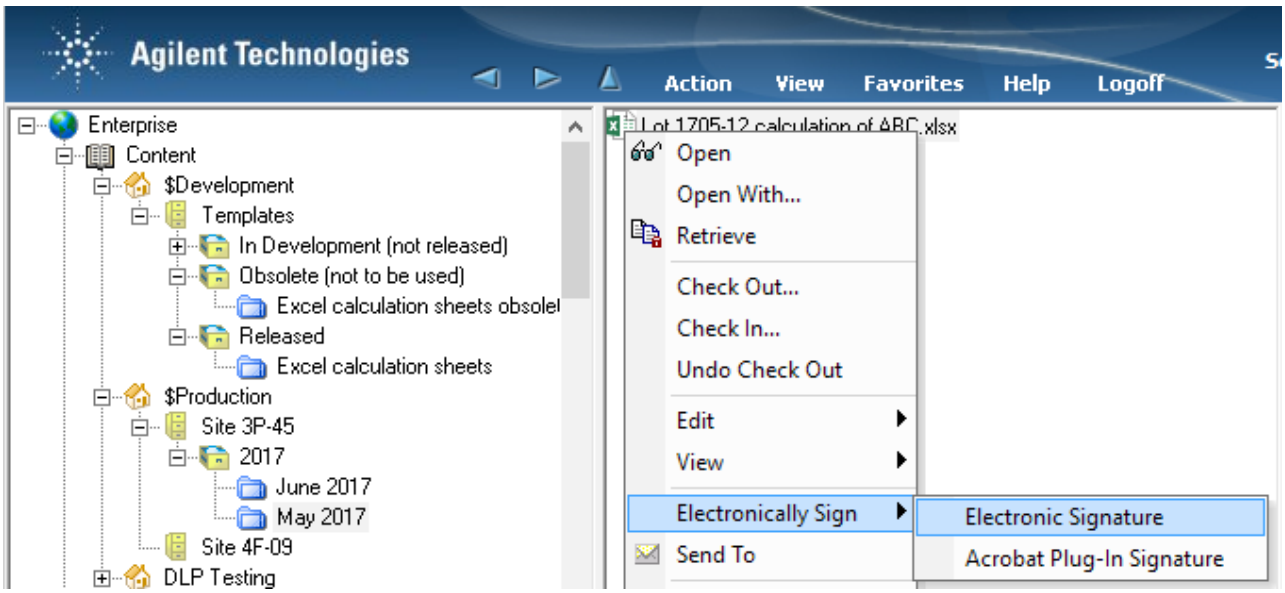

Figure 9. Spreadsheet review and approval using OpenLAB ECM.

Reviewing Microsoft Excel audit trails

The Microsoft Excel audit trial can be viewed at any time by choosing the "Review" tab and clicking "Track Changes" (Figure 10). Next, in the "Highlight Changes" window, turn off (unselect) everything except "List changes on a new sheet."

As shown in Figure 11, the Microsoft Excel audit trail is displayed in a new worksheet. The user name is based on the name of the Microsoft Windows logged in user.

Note: If users are allowed to work from a shared PC with a shared logon, users will not be uniquely identified, and thus the audit trail will not meet regulatory requirements.

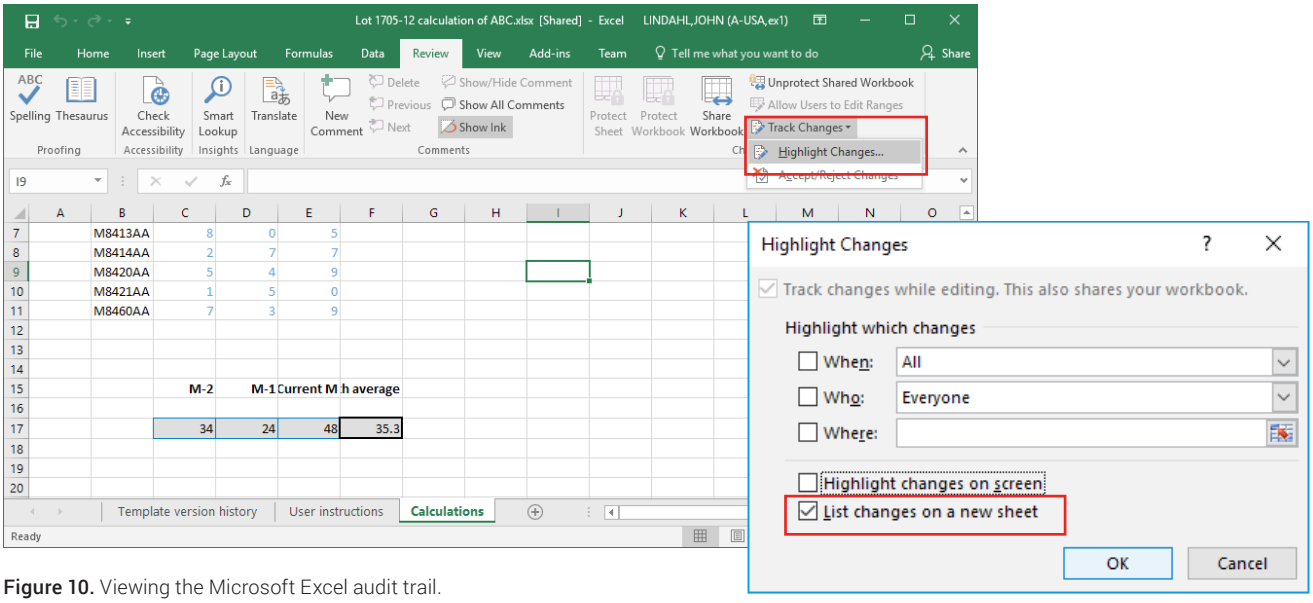

Figure 10. Viewing the Microsoft Excel audit trail.

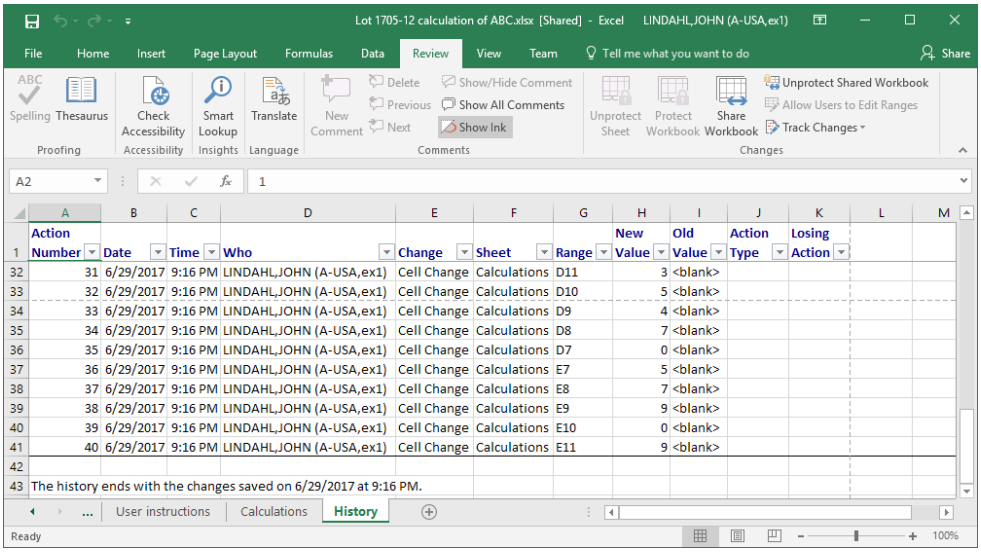

Figure 11. Example of a Microsoft Excel audit trail.

Summary

Regulatory requirements specify strict controls for secure data access, full revision control, and audit trail for spreadsheets containing regulated data; that is data created during drug/device development and/or manufacturing, and/or data generated in support of drug/device development and/or manufacturing. As summarized in Table 1, when used with OpenLAB ECM, Microsoft Excel spreadsheets can be managed in a way that complies with US FDA 21 CFR Part 11 and EU Annex 11, without special modifications or add-on packages.

Table 1. Summary: Managing spreadsheets in a regulated environment using OpenLAB ECM and Microsoft Excel.

Requirement	Implementation with OpenLAB ECM
Access control	OpenLAB ECM logon required to access files
Various user access levels	OpenLAB ECM folder access permissions
Revision storage and version control for data integrity	Microsoft Excel desktop integration for revision controlled file storage (in OpenLAB ECM)
Secure storage (protected from any unauthorized change)	OpenLAB ECM stores files in a protected location and metadata in a secure database
Archive and backup	Performed by the OpenLAB ECM administrator
Audit trail for each cell	Microsoft Excel audit trail (track changes)
Protection of sheet, rows, or cells	Microsoft Excel feature
Validation of OpenLAB ECM	IQ/OQ provided by Agilent; DQ/PQ is users responsibility.
Validation of MS Excel Application	User responsibility; can use standard COTS validation approach

Appendix: Satisfying the requirements set forth in US FDA Title 21 CFR Part 11 and related global regulations using OpenLAB ECM and Microsoft Excel.

Column 1: The table addresses 21 CFR Part 11 requirements in the order that they are presented in the US FDA reference document. Related requirements such as those found in EU Annex 11 follow each section of Part 11.

Column 2: For completeness, column 2 lists all requirements of 21 CFR Part 11 and other related global requirements. "System" refers to the analytical system used to acquire and process data. Most requirements are fulfilled by either technical controls (i.e., software functionality) or procedural controls (i.e., SOPs). Technical controls are controls provided by the software and hence the software supplier, while procedural controls are the responsibility of the user organization. 21 CFR Part 11 requirements listed in bold are requirements addressed by technical controls. Other global requirements are listed in regular font. Requirements that must be addressed by procedural controls are listed in blue.

Column 3: Some requirements involve both technical and procedural controls. Responsibilities for each requirement are listed in column three. "S" refers to analytical system supplier. "U" refers to the user organization. Rows containing requirements that must be exclusively addressed by the user organization are shown in blue. Blue may also be technical controls the user will be responsible to implement.

Column 4: If available and where appropriate, related global requirements and comments are provided in column four.

Column 5: Column 5 indicates with a "yes" or "no" whether the requirement can be satisfied using the technical controls provided in Microsoft Excel and/or OpenLAB ECM. N/A is not applicable.

Column 6: Column 6 explains how the regulatory requirement can be satisfied using the technical controls provided by Microsoft Excel and/or OpenLAB ECM. Column six also provides additional recommendations for the user organization when relevant.

1. Validation

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation?
Part 11 11.10(a)	1.1 Is the system validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?	S, U	Required by all regulations. This is a typical example of shared responsibility between the system supplier and the user organization. While the user organization has ultimate responsibility for validation, some tasks can only be done and must be delivered by the software supplier, e.g., validation activities during development and related documentation.	Yes	Agilent Technologies has extensively verified the performance of OpenLAB ECM using tests that evaluate the accuracy and security of stored files and metadata. However, the user organization is required to validate their spreadsheet applications, processes, and systems according to regulatory expectations.
Annex 11	1.2 Is infrastructure qualified?	U	Annex 11.Principle B Brazil GMP 577	N/A	Qualification of infrastructures, such as servers and networks, is the responsibility of the user organization.

2. Accurate Copies and Secure Retention and Retrieval of Records

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.10(b)	2.1 Is the system capable of generating accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the FDA?	S		Yes	Records are available printed on paper or electronically as a PDF file.
Annex 11	2.2 Is it possible to obtain clear printed copies of electronically stored e-records?	S	Annex 11.8.1 Brazil GMP 583	Yes	Records are available printed on paper or electronically as a PDF file.
Brazil	2.3 Are there controls to make sure that the data back up, retrieval and maintenance process is duly carried out?	S, U	Brazil 585.2	Yes	While backing up data is the responsibility of the user organization, OpenLAB ECM is designed to allow back up of all relevant files.
Part 11 11.10(c)	2.4 Does the system protect records to enable their accurate and ready retrieval throughout the records retention period?	S, U	China GMP 163	Yes	All files in OpenLAB ECM are stored in a protected location. Physical security (control of physical access to workstations and servers) is the responsibility of the user organization.
Annex 11	2.5 Are data checked during the archiving period for accessibility, readability, and integrity?	U	Annex 11.17	N/A	It is the responsibility of the user organization to ensure data are checked during archival for accessibility, readability, and integrity.
Annex 11	2.6 If relevant changes are made to the system (e.g., computer equipment or programs), is then the ability to retrieve the data ensured and tested?	S, U	Annex 11.17	Yes	The system is designed to read data from earlier versions of OpenLAB ECM. The user organization is responsible for ensuring readability of this data during their implementation and validation processes.
Annex 11	2.7 Are data secured by both physical and electronic means against damage?	S, U	Annex 11.7.1 Brazil GMP 584	Yes	All files are stored in a protected location. Physical security is the responsibility of the user organization.
Clinical guide	2.8 Are there controls implemented that allow the reconstruction of the electronic source/raw documentation for FDA's review of the (clinical) study and laboratory test results?	S	Clinical Computer Guide F2 FDA Q&As	Yes	All files and metadata in OpenLAB ECM are maintained in secure storage to allow reconstruction of laboratory test results as needed.

2. Accurate Copies and Secure Retention and Retrieval of Records *continued*

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Clinical guide	2.9 Does the information provided to FDA fully describe and explain how source/raw data were obtained and managed, and how electronic records were used to capture data?	U	Clinical Computer Guide F2 FDA Q&As	N/A	It is the responsibility of the user organization to describe how source/raw data were obtained and managed, and how electronic records were used to capture data.
Annex 11	2.10 Does the system allow performing regular back ups of all relevant data?	S	Annex 11.7.1 China GMP 163 Brazil GMP 585 Part 211, 68 b	Yes	While backing up data is the responsibility of the user organization, OpenLAB ECM is designed to allow back up of all relevant files.
Annex 11	2.11 Is the integrity and accuracy of backed-up data and the ability to restore the data, checked, validated, and monitored periodically?	U	Annex 11.7.2 China GMP 163 Brazil GMP 585 Part 211, 68 b	N/A	It is the responsibility of the user organization to ensure the integrity and accuracy of backed-up data, and to check, validate and monitor restored data periodically.
Clinical Computer Guide	2.12 Are procedures and controls in place to prevent the altering, browsing, querying, or reporting of data via external software applications that do not enter through the protective system software?	S, U	Clinical Computer Guide E	Yes	OpenLAB ECM can only be accessed through the web or Desktop interfaces with privileged user credentials.
Clinical Computer Guide	2.13 Are there controls implemented to prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software?	S, U	Clinical Computer Guide F	Yes	Agilent has tested OpenLAB ECM in conjunction with industry standard anti-virus applications. However, it is the responsibility of the user organization to implement anti- virus software.

3. Authorized Access to Systems, Functions, and Data

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.10(d)	**3.1 Is system access limited to authorized persons?**	S, U	China GMP 183 163 Brazil GMP 579, ICH Q7.5.43	Yes	Access to Excel applications and their data-specific application files are managed via OpenLAB ECM.
	3.2 Is each user clearly identified, e.g., though his/her own user ID and Password?	S, U	Several Warning Letters	Yes	OpenLAB ECM provides secure access.
Clinical	3.3 Are there controls to maintain a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges?	S, U	Clinical Computer Guide 4	Yes	OpenLAB ECM authenticates users via either the Windows Domain or locally in the application itself. Access privileges are set in the application and any changes are recorded in the activity log

4. Electronic Audit Trail

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM with Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.10(e)	**4.1 Is there a secure, computer-generated, time-stamped audit trail to independently record the date and time of operator entries and actions that create, modify, or delete electronic records?**	S	China GMP 163	Yes	Microsoft Excel provides a full audit trail of all data entry additions, changes, and deletions in spreadsheets. OpenLAB ECM provides an audit trail of all actions performed on the Excel template and data files. All user activities are recorded in secure, computer generated, time-stamped audit trails.
FDA GLP	4.2 Does the audit trail record who has made which changes, when and why?	S	FDA 21 CFF 58.130 e Clinical Computer Guide 2 Clinical Source Data 3	Yes	Provided by the Microsoft Excel audit trail that includes the user ID, date and time of the change, and the before and after values. The OpenLAB ECM audit trail lists modifications, date and time of the change, the use ID and reason for the change.
Annex 11	4.3 Can the system generate printouts indicating if any of the e-records have been changed since the original entry?	S	Annex 11, 8.2	Yes	Provided by the Microsoft Excel audit trail.

4. Electronic Audit Trail *continued*

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM with Microsoft Excel? If no, what is the recommendation to customers?
FDA GMP	4.4 Does the audit trail include any modifications to an established method employed in testing? 4.5 Do such records include the reason for the modification?	S	Part 211.194 8b	N/A	OpenLAB ECM does not control test equipment.
	4.6 Is the audit trail function configured to be always on and can it not be switched off by system users?	S, U		Yes	Provided by the Microsoft Excel audit trail that is protected by a password. Entries in the OpenLAB ECM audit trail cannot be switched off, altered, or deleted by any user
Annex 11	4.7 Is audit trail available in a generally intelligible form for regular review?	S	Annex 11, 9	Yes	Provided by the Microsoft Excel audit trail that is viewable from the application. The OpenLAB ECM audit trail can be reviewed by filtering on user, dates, and other criteria. It can be printed to paper or PDF as required.
	4.8 Can audit trail contents be configured such that only relevant activities are recorded for realistic and meaningful review of audit trail information?	S	Implicitly required by Annex 11 with many warning letters related to review of audit trail.	Yes	Provided by the Microsoft Excel audit trail. OpenLAB ECM allows the audit trail to be filtered prior to displaying its contents to address user preferences for reviewing the information it contains.
Part 11 11.10(e)	**4.9 Is previously recorded information left unchanged when records are changed?**	S		Yes	The Microsoft Excel audit trail records all data entry additions, changes, and deletes. Changes to a spreadsheet file stored in OpenLAB ECM are saved as new revisions of the original, which is left unchanged. When opening files for further processing or reporting, the user chooses the version of the file used (based on their permissions.)
Part 11 11.10(e)	**4.10 Is audit trail documentation retained for a period at least as long as that required for the subject electronic record?**	S, U		Yes	The Microsoft Excel audit trail is included with the data-specific application file. Audit trail information for files stored in OpenLAB ECM is linked to the electronic record and cannot be separated from it.
Part 11 11.10(e)	**4.11 Is audit trail available for review and copying by the FDA?**	S		Yes	Audit trails can be viewed, filtered, and printed.
Annex 11	4.12 Is it possible to obtain clear printed copies of electronically stored e-records (e.g., e-audit trail).	S	Annex 11, 8.1	Yes	Provided by Microsoft Excel software in general. Audit trails can be viewed and printed.

5. Operational and Device Checks

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.10(f)	**5.1 Are there operational system checks to enforce permitted sequencing of steps and events, if required?**	S		Yes	Microsoft Excel can be configured to provide sequencing by configuration checks on prerequisite data entry values.
Part 11 11.10(g)	**5.2 Are there authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand?**	S	Part 211, 68 b	Yes	OpenLAB ECM provides secure access to Microsoft Excel templates and data-specific files.
	5.3 Is the system designed to record the identity of operators entering, changing, confirming or deleting data including date and time?	S	Annex 11, 12.4	Yes	The identity of operators taking action in the application is recorded in the Microsoft Excel audit trail. Actions taken on spreadsheet files are stored in the OpenLAB ECM audit trail.
Part 11 11.10(h)	**5.4 Does the system allow use of device checks to determine, as appropriate, the validity of the source of data input or operational instruction?**	S	There are two equally valid interpretations of this requirement. Systems should be designed such that: 1. Proper communication is confirmed between the computer and the "source" of data input (i.e., the instrument) prior to transmission of instructions to or data from the "source." 2. Regulated records created by the system must unambiguously indicate the "source" of the data (i.e., which instrument or component generated the data.)	N/A	Microsoft Excel software does not directly interface with equipment or instruments providing source data.
Part 11 11.10(i)	5.5 Is there documented evidence that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks?	U	China GMP 18 Brazil 571	N/A	It is the responsibility of the user organization to maintain documented evidence that the persons who develop, maintain, or use electronic record and electronic signature systems have the education, training, and experience needed to perform these tasks Agilent software professionals involved in development of OpenLAB ECM have received training in relevant aspects of data integrity.

5. Operational and Device Checks *continued*

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.10(j)	5.6 Is there a written policy that holds individuals accountable and responsible for actions initiated under their electronic signatures, in order to determine record and signature falsification?	U		N/A	It is the responsibility of the user organization to establish a written policy (SOP) that holds staff responsible for the actions initiated under their electronic signatures.
	5.7 Have employees been trained on this procedure?	U	Implied requirement of Part 11 11.10(j)	N/A	It is the responsibility of the user organization to train their staff.
Part 11 11.10(k)	5.8 Are there appropriate controls over systems documentation including: Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance? Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	U	China GMP 161	N/A	It is the responsibility of the user organization to establish systems documentation. Each Microsoft Excel file contains a version that shows the evolution of modifications to the application.
Part 11 11.10(i)	**5.9 Are there revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of system documentation?**	S, U		Yes	Agilent maintains development and testing documentation for OpenLAB ECM. Upon request, this documentation is available for user review. The user organization is expected to maintain documentation of their system and associated changes in situ. Each Microsoft Excel file contains a version that shows the evolution of modifications to the application, and each version is validated by the users.

6. Data Integrity, Date and Time Accuracy

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Annex 11	6.1 Do computerized systems that exchange data electronically with other systems include appropriate built-in checks for the correct and secure entry and processing of data?	S	Annex 11.5	N/A	Microsoft Excel does not directly interface with equipment or instruments providing source data. Microsoft Excel files can be configured to contain data entry checks for manual data entry.
Annex 11	6.2 Is there an additional check on the accuracy of the data? This check may be done by a second operator or by validated electronic means.	S, U	Annex 11-6 Brazil GMP 580 ICHQ7-5.45	Yes	Representatives of the users of Microsoft Excel applications validate the process of using the application, which may include checks by a second person.
Clinical Computer Guide	6.3 Are controls established to ensure that the system's date and time are correct?	S, U	Clinical Computer Guide D.3	N/A	Agilent recommends that the system be configured to reference a timeserver to ensure accuracy of the system date and time. This is configured in and controlled by the operating system. Microsoft Excel uses the operating system time.
Clinical Computer Guide	6.4 Can date or time only be changed by authorized personnel, and is such personnel notified if a system date or time discrepancy is detected?	S	Clinical Computer Guide D.3	N/A	This is usually limited to the System Administrator. This is configured in and controlled by the operating system. Microsoft Excel uses the operating system time.
Clinical Computer Guide l	6.5 Are timestamps with a clear understanding of the time zone reference used implemented for systems that span different time zones?	S, U	Clinical Computer Guide D.3	Yes	Microsoft Excel uses the operating system time that identifies local time.

7. Control for Open Systems (Only Applicable for Open Systems)

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.30	7.1 Are there procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt?	S, U		N/A	OpenLAB ECM is not intended to be deployed as "open" system as per 21 CFR Part 11.3(b) (9).
Part 11 11.30	7.2 Are there additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality?	S		N/A	OpenLAB ECM is not intended to be deployed as "open" system as per 21 CFR Part 11.3(b) (9).

8. Electronic Signatures – Signature Manifestation and Signature/Record Linking

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Annex 11	8.1 When electronic signatures are used, Do they have the same impact as hand-written signatures within the boundaries of the company? Are they permanently linked to their respective record? Do they include the time and date that they were applied?	S, U	Annex 11.14 ICH Q7.6.18	Yes	Microsoft Excel does not support electronic signatures, but OpenLAB ECM can be used to perform electronic signatures. The user organization must establish the legal impact of electronic signatures. Signatures are permanently linked to their respective records.
Part 11 11.50 (a)	**8.2 Do signed electronic records contain information associated with the signing that clearly indicates all of the following: The printed name of the signer? The date and time when the signature was executed? and The meaning (such as review, approval, responsibility, or authorship) associated with the signature?**	S		Yes	OpenLAB ECM can be used to provide electronic signatures. Signed electronic records show the name of the signer, and date and time the signature was executed, and the meaning of the signature.

8. Electronic Signatures – Signature Manifestation and Signature/Record Linking *continued*

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.50 (b)	**8.3 Are the items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section subject to the same controls as for electronic records and are they included as part of any human readable form of the electronic record (such as electronic display or printout)?**	S		Yes	OpenLAB ECM can be used to provide electronic signatures. All electronic signature components are displayed and printed.
Part 11 11.70	**8.4 Are electronic signatures and handwritten signatures linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?**	S		Yes	OpenLAB ECM can be used to provide electronic signatures.
Part 11 Preamble	8.5 Is there a user-specific automatic inactivity disconnect measure that would "de-log" the user if no entries or actions were taken within a fixed short timeframe?	S	Part 11 Preamble section 124	N/A	Microsoft Excel does not support inactivity timeout but this functionality can be provided by the operating system.

9. Electronic Signatures General Requirements and Signature Components and Controls

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.100(a)	9.1 Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	S, U		Yes	OpenLAB ECM can be used to provide electronic signatures. Each user has a unique login and thus a unique signature that cannot be used by another user.
Part 11 11.100(b)	9.2 Does the organization verify the identity of the individual before the organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature?	U		N/A	It is the responsibility of the user organization to verify the identify of staff before it establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature.

9. Electronic Signatures General Requirements and Signature Components and Controls *continued*

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.100 (c)	9.3 Are persons using electronic signatures, prior to or at the time of such use, certified to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures? Do persons using electronic signatures, upon agency request provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature?	U		N/A	It is the responsibility of the user organization to verify that staff using electronic signatures meet these requirements.
Part 11 11.200(a) (1)	**9.5 Do electronic signatures that are not based upon biometrics employ at least two distinct identification components such as an identification code and password?**	S, U		Yes	OpenLAB ECM can be used to provide electronic signatures that require a unique username and password.
Part 11 11.200(a) (1) (i)	**9.6 When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all electronic signature components?**	S		Yes	OpenLAB ECM can be used to provide electronic signatures.
Part 11 11.200(a) (1) (i)	**9.7 When an individual executes a series of signings during a single, continuous period of controlled system access, are subsequent signings executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual?**	S		Yes	OpenLAB ECM can be used to provide electronic signatures that require the user to re-enter their password within a specified period of continuous system access.

9. Electronic Signatures General Requirements and Signature Components and Controls *continued*

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.200(a) (1) (ii)	**9.8 When an individual executes one or more signings not performed during a single, continuous period of controlled system access, is each signing executed using all of the electronic signature components?**	S		Yes	OpenLAB ECM requires all signature components for each signature performed outside the specified period of continuous system access.
Part 11 11.200(a) (2)	**9.9 Are controls in place to ensure that electronic signatures that are not based upon biometrics are used only by their genuine owners?**	S		Yes	OpenLAB ECM can be used to provide electronic signatures that require a unique username and private password.
Part 11 11.200(a) (3)	**9.10 Are the electronic signatures administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals?**	S, U		Yes	Misuse of electronic signatures by anyone other than the owner requires intentional co-operation of a user and the System Administrator.
Part 11 11.200(b)	**9.11 Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners?**	S		N/A	Biometric authentication is not supported in OpenLAB ECM.

10. Controls for Identification Codes and Passwords

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Part 11 11.300(a)	10.1 Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?	S, U		Yes	OpenLAB ECM can be used to provide electronic signatures that require a unique username and private password. OpenLAB CDS does not allow duplicate user IDs so each electronic signature is unique.
Part 11 11.300(b)	10.2 Are controls in place to ensure that identification code and password issuance are periodically checked, recalled, or revised (e.g., to cover such events as password aging)?	S, U		N/A	It is the responsibility of the user organization to verify that staff using electronic signatures meet these requirements.
Part 11 11.300(c)	10.3 Are there procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromise tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls?	U		N/A	It is the responsibility of the user organization to establish these procedures.
Part 11 11.300(d)	10.4 Are there transaction safeguards in place to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts of their unauthorized use to the system security unit, and, as appropriate, to organizational management?	U		N/A	It is the responsibility of the user organization to establish these transaction safeguards.
Part 11 11.300(e)	10.5 Are there controls for initial and periodic testing of devices, such as tokens or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner?	U		N/A	It is the responsibility of the user organization to establish controls to test devices initially as well as periodically to ensure they function properly and have not been altered in an unauthorized manner.

11. System Development and Support

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using OpenLAB ECM and Microsoft Excel? If no, what is the recommendation to customers?
Annex 11	11.1 Has the software or system been developed in accordance with an appropriate quality management system?	S, U	Annex 11 4.5 Brazil GMP 577 GAMP This is a shared responsibility between the system supplier and the user organization. The user should require the supplier to provide documented evidence that software is developed within the framework of a quality management system (QMS).	Yes	OpenLAB ECM is developed within the ISO 9001 Quality Management Standard.
Brazil	11.2 Is there a formal agreement when the software supplier subcontracts software and maintenance services. Does the agreement include the contractor's responsibilities?	S, U	Brazil GMP 589 This is a shared responsibility between the system supplier and the user organization. The supplier must have such an agreement with the subcontractor, and the user must verify that the agreement is in place.	Yes	Agilent requires formal agreements with all suppliers.
ICH Q10	11.3 For outsourced (development and support) activities, is there a written agreement between the contract giver and contract acceptor?	S, U	ICHQ10, 2.7 c	Yes	Agilent requires formal agreements with all suppliers.
ICH Q10	11.4 Are the responsibilities and communication processes for quality related activities of the involved parties (contractors) defined?	S, U	ICHQ10, 2.7 c	Yes	Agilent defines responsibilities of all suppliers.
Part 11 11.10(i)	11.5 Is personnel developing and supporting software trained?	S, U	This is a shared responsibility between the system supplier and the user organization. The supplier must ensure its staff is trained, and the user should have assurance, e.g., through audits that SW developers are trained and that this training is documented.	Yes	All Agilent personnel are required to be trained.

www.agilent.com/openlab

Printed in the USA, August 17, 2017
5991-8294EN

Agilent
Trusted Answers